I manuali SIFO

Linee guida per la sicurezza delle Farmacie Ospedaliere

SIFO Società Italiana di Farmacia Ospedaliera
e dei Servizi Farmaceutici delle Aziende Sanitarie

Società Italiana di Farmacia Ospedaliera
e dei Servizi Farmaceutici delle Aziende Sanitarie

I manuali SIFO

Linee guida per la sicurezza delle Farmacie Ospedaliere

CAMPANO
EDIZIONI

Volume a cura di
Lidio Brasola
Fulvio La Bella
Marcello Pani
Ettore Rossi
Giuseppe Turchetti

Hanno collaborato
Andrea Antonel
Andrea Cammilli
Sara Cannizzo
Barbara Meini

Revisione e validazione
Domenico Di Giorgio (Aifa)
Maria Grazia Chimenti (Farmindustria)
Giuseppe Naso (AIBA)
Romina Ronchi (Ania)

ISBN 978-8-86528-438-4

© 2018 by Edizioni Il Campano
Via Cavalca, 67, 56126 Pisa
Tel. 050 580722
info@edizioniilcampano.it
www.edizioniilcampano.it

Sommario

LA SICUREZZA DEL FARMACO DOPO LE AZIONI DEL CONGRESSO SIFO 2014 7

PRESENTAZIONE 9

RAZIONALE DEL DOCUMENTO 13

LINEE GUIDA PER LA SICUREZZA DELLA FO 11

1. Panoramica generale 17
2. Il concetto di "Sicurezza" 19
3. Concetti sui sistemi 20
4. Gestione dei rischi 25
   - 4.1 Modelli normativi di gestione del rischio 26
   - 4.2 Cenni sugli strumenti del Risk Management 28
   - 4.3 Strumenti per la gestione del Security Risk 29
   - 4.4 Elementi per la riduzione dell'impatto di rischio residuo da coprire attraverso gli strumenti assicurativi 32
   - 4.5 Risk Assessment 34
5. Progettazione del sistema per la gestione della sicurezza 37
   - 5.1 Disegno architetturale del sistema 38
   - 5.2 Disegno dei sottosistemi 44
   - 5.3 Validazione del sistema 48
   - 5.4 Modifiche alla progettazione 49
   - 5.5 Specifiche per i Security Services 50
   - 5.6 Requisiti di gestione dei fornitori 50
   - 5.7 Requisiti infrastrutturali generali 52

6. Sotto-sistemi e servizi tecnici 54
6.1 Misure fisiche 54
6.2 Sistema di controllo degli accessi 61
6.3 Sistemi intelligenti 66
6.4 Controllo delle consegne 67
6.5 Sistema di allarme 68
6.6 Gestione del personale 74
6.7 Sicurezza della documentazione 78
7. Gestione delle attività esternalizzate (Outsourced activities) 79
7.1 Azioni pre-contrattuali 80
7.2 Esecuzione del contratto 82
7.3 Auditing 84
7.4 Azioni post-contrattuali 85
7.5 Outsourcing: Elementi generali per la riduzione dei rischi per la sicurezza 85
8. Intelligence 88
9. Miglioramento 89
10. Gestione delle modifiche al sistema 91
11. Manutenzione 93
12. Bibliografia e riferimenti sitografici 94
13. Appendice: Resilienza Organizzativa: concetti e modelli 105
13.1 Resilienza Organizzativa: alcuni modelli 108
14. Allegato 1: Questionario base per lo strumento di calcolo del LMS 114
15. Allegato 2: Esempio specifiche telecamera professionale top level 120
16. Allegato 3: Esempio specifiche sensore volumetrico professionale top level 122
17. Allegato 4: Esempio specifiche sistema di controllo accessi a lettura della retina professionale top level 123

La sicurezza del farmaco dopo le azioni del Congresso SIFO 2014

Al fine di presentare una proposta per affrontare a livello Nazionale il problema della sicurezza del farmaco è stato lanciato nel 2014 il progetto Padlock (Progetto di Adeguamento Dei Livelli di sicurezza delle farmacie Ospedaliere contro il rischio di furti e definizione di standard tecnici) istituendo un Gruppo di Studio con l'obiettivo di portare al Congresso lo stato dell'arte delle soluzioni in materia.

Il Gruppo ha assegnato un'attività di auditing a un partner industriale del Gruppo di Lavoro esperto di sicurezza definendo un panel significativo di Farmacie Ospedaliere per avere una panoramica dello stato di sicurezza attuale e definire il punto di partenza o "as is".

È stata prodotta quindi una linea guida per le Farmacie Ospedaliere che consentisse loro di operare la valutazione del livello di dimensionamento dei propri sistemi di sicurezza.

È stato costruito un sito internet che potesse essere un luogo di condivisione dei risultati delle attività del progetto e che ospitasse un tool informatico per facilitare la valutazione dello stato di sicurezza della Farmacia Ospedaliera in remoto.

Dai dati raccolti nel progetto è emersa la necessità di dotare le Direzioni di uno strumento che fosse di supporto per la corretta adozione di sistemi di sicurezza adeguati alle differenti situazioni e ai diversi scenari in cui si trovano ad operare le singole Farmacie Ospedaliere Italiane.

Presentazione

Questo documento nasce nell'ambito del progetto Padlock, una collaborazione tra SIFO Area Logistica e Roche SpA per la prevenzione dei furti e la messa in sicurezza delle farmacie ospedaliere.

Rimane importante aumentare i livelli di sicurezza nelle strutture pubbliche al fine di limitare accessi non autorizzati ai farmaci e la distribuzione illecita su canali esteri o nazionali, con innumerevoli e conseguenti rischi connessi per la salute (mancato rispetto degli standard di conservazione, contraffazione, ecc.).

La sicurezza è un problema complesso e deve essere affrontato in logica sistemica.

Dopo l'emissione della prima linea guida (Novembre 2015), che sensibilizzava le Direzioni sulla problematica della sicurezza della Farmacia Ospedaliera e la messa in opera del *tool* informatico per l'autovalutazione dello stato di sicurezza della Farmacia sul sito dedicato al progetto Padlock, è il momento di fissare le minime regole progettuali per garantire la messa in opera di sistemi di sicurezza coerenti ed adeguati alle problematiche delle singole realtà sul territorio.

Queste sono le esigenze a cui la presente Linea Guida vuole trovare risposta.

La forma di Linea Guida è stata scelta in quanto più adatta allo scopo di indirizzare e fornire conoscenze che possano essere efficacemente applicate nelle diverse situazioni, piuttosto che una serie di prescrizioni che possono di volta in volta essere eccessive o insufficienti.

Il presente documento vuole essere il punto di partenza per un percorso che porti le Farmacie Ospedaliere a definire la specifica architetturale del sistema di gestione per la sicurezza scegliendo la composizione più adatta di componenti e pratiche per garantire il livello di sicurezza desiderato e per contrastare in modo efficace il problema dei furti di medicinali.

Si tratta di una guida per il disegno del sistema di gestione per la sicurezza e il suo controllo nel tempo, uno strumento efficace ed aggiornato, validato da AIFA, FARMINDUSTRIA, ANIA, AIBA, realizzato in collaborazione con la Scuola Superiore Sant'Anna di Pisa.

Razionale del Documento

Il presente documento rappresenta il risultato del lavoro di ricerca comparata su differenti schemi di implementazione dei sistemi di garanzia per la sicurezza esistenti nei maggiori Paesi.

La proposta di un determinato approccio al disegno e alla valutazione dei sistemi per la sicurezza della Farmacia Ospedaliera descritta nel documento è il risultato delle valutazioni di un campione rappresentativo di Farmacie Ospedaliere italiane svolte all'interno del progetto Padlock di SIFO tra il 2014 e il 2016.

L'analisi complessiva dell'approccio normativo alla sicurezza da una parte e della situazione effettiva della Farmacia Ospedaliera dall'altra ha portato alla comprensione della realtà degli ospedali italiani come unica in termini di connotazione logistica, organizzativa e umana.

Data la premessa si è ritenuto necessario sviluppare un sistema dedicato alla tipologia logistica "Farmacia Ospedaliera" in tutta la sua peculiare complessità che – facendo tesoro dell'esperienza normativa mondiale – consentisse l'efficace ed efficiente applicazione di soluzioni tecniche ed organizzative per la concreta protezione dei siti.

L'elaborato ha previsto di includere due elementi di straordinaria importanza e cioè l'approccio generale al rischio per la sicurezza nella prospettiva delle assicurazioni (attraverso la collaborazione ANIA/AIBA) e il sistema di intelligence per l'analisi e la condivisione degli scenari di minaccia alla sicurezza della Farmacia Ospedaliera (che si ispirerà al lavoro svolto da AIFA) – al momento solo abbozzato che sarà oggetto di sviluppo delle prossime revisioni.

L'ambito di applicazione delle regole espresse nel documento è la Farmacia Ospedaliera nelle sue differenti forme presenti sul territorio italiano.

La presente pubblicazione – che rappresenta la finalizzazione di una linea guida per il disegno e la valutazione del sistema di sicurezza della Farmacia Ospedaliera Italiana – chiude i lavori di revisione del Comitato Tecnico istituito da SIFO che ne ha approvato i contenuti.

Linee guida per la sicurezza della FO

La presente linea guida costituisce l'insieme organico delle best practices alle quali la Farmacia Ospedaliera dovrebbe fare riferimento per disegnare e verificare la corretta messa in opera di un sistema di gestione per la garanzia della sicurezza del farmaco.

Lo stesso documento viene utilizzato come riferimento per l'attività di audit finalizzata al rilascio del sigillo SIFO Padlock al sito interessato.

Il concetto principale – filo conduttore di tutta l'architettura del presente standard – è quello di "resilienza" applicato al sistema di gestione per la garanzia della sicurezza del farmaco.

Con la terminologia "resilienza del sistema" si intende la capacità dello stesso di rispondere in modo adeguato agli scopi per cui viene messo in opera di fronte a future sollecitazioni sia dovute ai processi interni che provenienti da cambiamenti dell'ambiente esterno.

Più in generale il termine "resilienza" indica la capacità di un sistema di adattarsi al cambiamento.

Questo principio guida va inteso come l'ago di una bussola da utilizzare per navigare tutta la linea guida fornendo un'interpretazione coerente all'implementazione delle best practices descritte, tenendo conto dello specifico contesto ambientale, organizzativo, culturale, finanziario del sito.

La linea guida sviluppa diversi momenti per la messa in opera di un coerente sistema di gestione per la garanzia della sicurezza del farmaco. La coerenza dimensionale del sistema viene garantita attraverso l'adozione di un approccio "risk based" nella fase iniziale di dimensionamento e pianificazione del sistema, nonché nelle fasi di gestione del cambiamento e miglioramento del sistema.

Le specifiche realtà delle Farmacie Ospedaliere, parti integranti dei sistemi "ospedale", non consentono l'adozione *tout court* di alcuno degli standard di sicurezza oggi disponibili in ambito normativo. L'esperienza fatta negli ultimi anni con il progetto Padlock di SIFO ha portato all'unica linea guida specificamente orientata alla realtà della Farmacia Ospedaliera italiana che, per motivi progettuali, è soprattutto dedicata alla diffusione di un concetto di "sicurezza del farmaco" in ambito ospedaliero

per poter ottenere un cosiddetto "livello minimo accettabile di sicurezza", concentrando necessariamente l'azione solo su un sottoinsieme del mondo dei requisiti per la sicurezza effettivamente applicabili.

Il suddetto sottoinsieme – rappresentando il risultato di oltre quaranta audit presso FO italiane – è stato considerato rappresentativo della realtà attuale della FO italiana per la definizione del LMS o "Livello Minimo di Sicurezza".

Per dotare la FO italiana di uno strumento per la rapida valutazione del proprio livello di sicurezza rispetto al LMS è stato sviluppato – sempre all'interno degli scopi del progetto Padlock di SIFO – uno specifico strumento accessibile informaticamente previa registrazione sul sito internet del progetto Padlock.

Lo strumento di valutazione è culminato nella definizione della "Scala Lockpill" che descrive lo stato generale di sicurezza del sito derivante dall'uso dello strumento e le azioni di follow up che andrebbero intraprese al fine di ottenere almeno il LMS.

L'allegato "questionario base per lo strumento di calcolo del LMS", riporta i quesiti utilizzati per popolare il database necessario per valorizzare l'indice di sicurezza secondo la scala Lockpill.

Nelle parti tecniche della presente linea guida saranno illustrate alcune delle motivazioni alla base dello strumento di valutazione per le dimensioni utili al fine di determinare il valore del LMS.

Il presente documento inoltre – ancora sviluppato all'interno degli scopi del progetto Padlock di SIFO – ha l'ulteriore ambizione di costruire una guida alla progettazione dedicata a un sistema di gestione per la garanzia della sicurezza del farmaco completa, verificabile e valutabile che possa costituire elemento di linguaggio comune per tutti gli oltre 1.000 siti pubblici e privati italiani – visti in logica di rete – per farmacie veramente "sicure".

Nello studio delle differenti fasi della linea guida sono stati presi a riferimento alcuni standard normativi che oggi costituiscono lo stato dell'arte e cioè:

- ISO 31000 assieme alla ISO 14971 come schema generale di riferimento procedurale nel complesso percorso che porta all'emergenza dei rischi effettivamente da considerare in una logica di costo efficacia del sistema. A queste si affianca il contributo della ICH Q9 utilizzata soprattutto in quanto riferimento principale per il mondo del farmaco.

- ISO 28000 e ISO 9000 come basi di riferimento per l'approccio sistemico all'organizzazione e l'approccio per processi nella messa in opera del sistema di gestione per la garanzia della sicurezza del farmaco, in quanto sono considerate a livello mondiale lo stato dell'arte per le realtà organizzative.

- TAPA FSR e TSR in quanto stato dell'arte per quanto concerne le applicazioni operative, dovute soprattutto alla grande esperienza sul campo dei soggetti che costituiscono l'associazione a livello mondiale (Transported Assets Protection Association).

È stato inoltre preso in considerazione il "The Drug Quality and Security Act (DQSA), signed into law by President Obama on November 27, 2013", per le sue implicazioni sulla sicurezza del farmaco e i problemi legati alla contraffazione.

Si sono inoltre considerati i dettami della direttiva anti contraffazione 2011/62/UE e relativi decreti di recepimento in Italia.

Tutto l'impianto del documento tiene conto inoltre del Regolamento Europeo sulle nuove Buone Pratiche di Distribuzione (Linee guida del 7 marzo 2013 sulle buone pratiche di distribuzione dei medicinali per uso umano 2013/C 68/01).

Considerata la pervasività dell'informatica e la crescente importanza della gestione delle informazioni e dei dati nel più generale scenario dell'Internet delle Cose (IOT – Internet Of Things), la linea guida inizia in questa prima stesura a integrare alcuni processi di controllo dei dati facendo riferimento a due linee guida principali:

- ISO/IEC 27000 è la famiglia di standard internazionali che delineano il Sistema di Gestione della Sicurezza delle Informazioni. Il Sistema di Gestione delle Informazioni protegge infatti: la riservatezza, l'integrità e la disponibilità dei dati dell'organizzazione.

- 21 CFR part 11 (Electronic Record: Electronic Signatures final rule) definisce i criteri di accettazione del FDA delle registrazioni elettroniche e delle firme su record elettronici come equivalenti alle registrazioni cartacee e firme manuali. La norma richiede l'implementazione di controlli, tracciati di audit, validazioni, firme elettroniche e la documentazione dei sistemi elettronici utilizzati per processare i dati in forma elettronica.

Analogamente è stata valutata la norma della Commissione Europea per i sistemi computerizzati: Annex 11(computerized systems) to Volume 4 of GMP for the European market.

1. PANORAMICA GENERALE

I magazzini che trattano merci in grandi volumi e ad alto valore sono particolarmente a rischio di furto con scasso. Ad esempio risulta che nel solo Regno Unito questo tipo di reato rappresenti il 20% di tutti i crimini registrati contro le imprese.

In Italia i furti di farmaco ammontano a oltre 20 milioni Euro di danno – dati rapporto Medicrime – ma, soprattutto, introducono rischi di indisponibilità delle cure per i cittadini e – anche dove riutilizzati – diventano pericolosi a causa dell'uscita dal controllo della corretta conservazione. Infatti i prodotti più "appetibili" spesso devono essere movimentati rispettando le regole della "catena del freddo" senza interruzioni.

Con queste cifre in gioco, è di vitale importanza prendere misure significative per proteggere il farmaco e quindi la salute dei cittadini. Installare sistemi di videosorveglianza (CCTV) – anche a tecnologia avanzata – è una soluzione che può fungere da deterrente ma da sola non è sufficiente a scoraggiare i ladri.

Nel prendere provvedimenti contro potenziali furti esiste una serie di fattori che è necessario prendere in considerazione.

Innanzitutto è opportuno procedere a una prima valutazione dei rischi connessi alla natura ed estensione delle infrastrutture, ma soprattutto è necessario comprendere che non esistono misure in grado singolarmente di eliminare il rischio di furti. Un buon risultato può essere ottenuto solo attraverso una combinazione di processi, prodotti di alta qualità, e opportune standardizzazioni delle pratiche di controllo delle operazioni.

Questa linea guida nasce come evoluzione del lavoro svolto con il progetto Padlock di SIFO aspirando a diventare il riferimento per la sicurezza del complesso mondo della Farmacia Ospedaliera Italiana.

Lo scopo della Linea Guida è di dare tutte le indicazioni necessarie per progettare e valutare il sistema di gestione per la garanzia della sicurezza del farmaco nella Farmacia Ospedaliera, consentendo agli agenti delle amministrazioni di controllare la corretta implementazione e gestione del sistema messo in opera.

Il documento si snoda attraverso un percorso che parte dalla definizione dei concetti di base che si vogliono assicurare attraverso l'implementazione del sistema. Viene quindi messo in evidenza l'approccio preventivo basato sull'analisi dei rischi e vengono trattati i modelli di riferimento per

la gestione dei rischi a cui ci si è ispirati. In questa parte viene integrata la prospettiva di valutazione dell'efficacia dei sistemi di sicurezza delle assicurazioni attraverso la collaborazione con gli enti di rappresentanza delle stesse e dei broker assicurativi.

La guida continua successivamente illustrando tutti i processi necessari per disegnare l'architettura del sistema in modo che sia coerente con i rischi effettivi del sito in questione e alle sue reali dimensioni. Vengono quindi evidenziati i sotto-sistemi operativi che sarà necessario mettere in opera secondo applicabilità in armonia ai dettami del disegno architetturale per ottenere le necessarie garanzie di sicurezza. I sotto-sistemi vengono trattati in modo da suggerire elementi di valutazione utili per poter comprendere la coerenza delle scelte progettuali con gli obiettivi di sicurezza.

La guida si conclude quindi con i processi di continuo adeguamento di quanto messo in opera attraverso la reiterazione del cammino progettuale, necessario per garantire la resilienza del sistema. Non viene tralasciato il processo di gestione dei dati di intelligence anche alla luce della disponibilità di strumenti messi in opera per monitorare l'evoluzione degli scenari di minaccia da AIFA, Farmindustria, ASSORAM e Carabinieri NAS con il supporto del Ministero della Salute, che hanno creato una banca dati dei furti, un archivio costantemente aggiornato con le segnalazioni inviate dalle oltre trenta aziende che aderiscono al progetto.

Allegato alla guida è stato inserito un breve studio sui concetti e i modelli della Resilienza Organizzativa che si applicano al mondo delle organizzazioni industriali e che costituiscono parte del perimetro di riferimento di questo stesso documento.

2. IL CONCETTO DI "SICUREZZA"

Sicurezza: definizione

(http://www.garzantilinguistica.it/ricerca/?q=sicurezza)

pl. -e

1. condizione di ciò che è sicuro, di ciò che consente di prevenire o attenuare rischi: la sicurezza di un edificio, di un mezzo di trasporto; fare qualcosa per maggior sicurezza, per essere più sicuro, per tutelarsi da imprevisti;
2. certezza: *devo avere la sicurezza di trovarlo; non ho la sicurezza di riuscire*;
3. qualità di chi è sicuro di sé e delle proprie azioni: sicurezza di modi, di giudizio; *guidare con sicurezza; la sicurezza del candidato sorprese gli esaminatori*;
4. l'insieme del personale specializzato che ha il compito di intervenire in situazioni di emergenza in una struttura complessa quale una banca, un albergo, un luogo dove si svolge un evento: chiamare la sicurezza.

Etimologia: ← deriv. di sicuro.

Per gli scopi del presente documento utilizzeremo la definizione data dal Comitato Tecnico competente dell'ISO e riportata al paragrafo 3.2 della norma ISO 28000:

Security: resistance to intentional, unauthorized act(s) designed to cause harm or damage to, or by, the supply chain.

Nel nostro caso considereremo i furti di medicinali come gli "*unauthorized act(s)*" a cui la definizione riferisce.

L'obiettivo del Sistema di Gestione oggetto della presente guida è quello di essere capace di garantire il livello di sicurezza voluto in relazione alla continua evoluzione nel tempo degli scenari di minaccia intesi come le modalità con cui avvengono gli "*unauthorized act(s)*" di cui sopra.

La dinamicità dell'enunciato precedente diventa a sua volta la definizione del moderno concetto di "resilienza" che evidenzia come scopo ultimo del sistema di Gestione per la garanzia di sicurezza la capacità – da ritenersi intrinseca al suo disegno progettuale – di *mantenere la sua efficacia nel tempo*.

3. CONCETTI SUI SISTEMI

Per sistema – ai fini del presente documento – si intende un insieme interconnesso di processi che condividono dati e generano informazioni per l'azione.

Un'attività – che utilizza risorse ed è gestita con il fine di trasformare elementi al suo ingresso in elementi in uscita – può essere considerata un processo.

Accade tipicamente che – all'interno del sistema considerato – l'elemento in uscita da un processo costituisca direttamente l'elemento in ingresso del processo successivo.

La norma ISO 9000 – base per tutti i sistemi di gestione – definisce tecnicamente il processo come un "*insieme di attività correlate o interagenti che trasformano elementi in entrata in elementi in uscita*".

Si definisce invece approccio per processi il modo di affrontare la realtà organizzativa individuando e gestendo le numerose attività tra loro collegate che la costituiscono.

Si definisce quindi prodotto il risultato di un processo e – ai fini organizzativi – esistono quattro categorie di prodotti:

- servizi – es. il trasporto di merci;
- software – es. un programma per computer, il contenuto di un dizionario;
- hardware – es. la parte meccanica di un motore;
- materiali da processo continuo – es. il carburante.

Dato che si interfacciano con i sistemi aziendali che per loro natura sono dinamici e aperti – cioè evolvono nel tempo e comunicano con l'ambiente circostante – i Sistemi di Gestione per la Sicurezza sono strutture necessariamente dinamiche possono essere adattati coerentemente con l'evoluzione degli scenari di minaccia ambientali e i cambiamenti dell'organizzazione in cui operano.

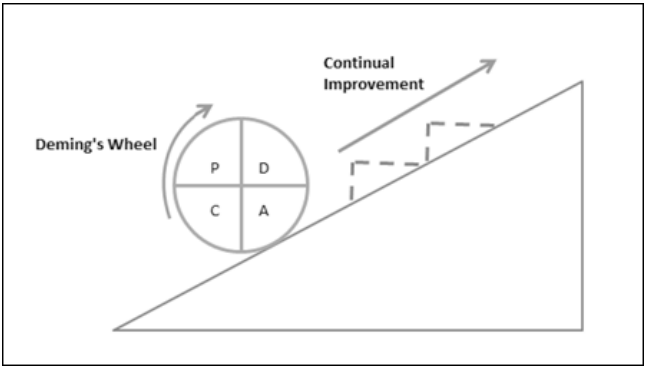
Così, qualsiasi soluzione efficace per la sicurezza deve essere pensata, sviluppata, implementata e gestita come un sistema.

La base concettuale del livello gestionale dei sistemi è lo sviluppo della capacità dei sistemi di adattarsi al proprio ambiente. Questo approccio è noto come "Ciclo di Deming" o PDCA (acronimo inglese di Plan Do Check Act).

Il Ciclo di Deming è un modello di gestione del cambiamento in quattro fasi utilizzato in ambito aziendale per il miglioramento continuo del business e il problem solving incrementale.

Questo modello fornisce un approccio sistematico al miglioramento il cui obiettivo è progredire attraverso le differenti fasi per ottenere una migliore qualità dell'output così come definito dal cliente in termini di qualità dei prodotti e dei servizi.

La figura seguente riassume le quattro fasi della metodologia che dovrebbe essere applicata dalle organizzazioni senza soluzione di continuità.



Approfondimento metodologico

Di seguito vengono esaminate le differenti fasi del modello PDCA per spiegarne nel dettaglio il funzionamento applicativo e i relativi limiti.

PLAN: Pianificare (la fase iniziale e successivamente il miglioramento)

L'obiettivo di questa fase è decidere cosa è necessario fare e come si possa farlo al meglio. Questo obiettivo va raggiunto attraverso la revisione e lo studio degli attuali processi di lavoro e dei dati disponibili. Questa fase richiede di esaminare approfonditamente i modi correnti di agire o le aree problematiche. Gli strumenti di gestione del cambiamento in questa fase includono il seguente elenco:

- Analisi della relazione Cliente/fornitore;
- Flowcharting – la mappatura dei processi del business;

- Pareto Analysis;
- Brainstorming – per la generazione di idee;
- Albero del valore;
- Matrici di Assessment;
- Analisi delle cause primarie e degli effetti.

DO: eseguire le attività pianificate

Si tratta di implementare il piano di azione o di problem-solving eseguendolo. In questa fase il piano è effettivamente messo in opera nel contesto reale. Le persone responsabili per le attività devono essere coerentemente formate e dotate delle risorse necessarie per completare i compiti assegnati. Via via che i problemi emergono, può essere necessario applicare in forma ridotta dei nuovi cicli PDCA per risolverli e attuare le nuove soluzioni. Risorse e competenze includono:

- Team Leader e supervisori leadership;
- Basi di progettazione;
- Competenze per la gestione dei problemi operativi;
- Competenze di gestione dei conflitti;
- On-the-job training.

CHECK: verificare e valutare i risultati

Le nuove soluzioni vanno valutate per verificare che abbiano ottenuto i risultati voluti. Strumenti di questa fase possono essere i seguenti:

- Fogli di raccolta dati;
- Carte di controllo;
- Key Performance Indicators.

ACT: agire rispetto ai risultati

Questa fase in stretta relazione con la precedente: se i risultati dell'implementazione hanno ottenuto i risultati attesi, la risposta è la standardizzazione dei relativi processi. In caso contrario, si deve imparare da ciò che è accaduto, decidere i necessari correttivi e formalizzare il tutto prima di iniziare un nuovo ciclo PDCA.

Ricominciando daccapo si mettono in atto tutte le azioni correttive richieste, si fissano i risultati corretti e si riprende il ciclo a partire dalla nuova pianificazione. La documentazione può includere:

- Mappa dei processi di Business e procedure operative standard;
- Aggiornamento controllato delle informazioni di riferimento;
- Formazione sui nuovi processi standard.

Punti chiave del ciclo di Deming

Laddove i processi sono automatizzati, la possibilità di fare cambiamenti da parte degli operatori è limitata, pertanto la responsabilità è dei progettisti e dei manager. Invece, dove il processo è manuale o focalizzato sul servizio – come la consegna merci – la possibilità e la responsabilità del vettore nella relazione con i destinatari è fondamentale per capire se le reali esigenze dei clienti sono soddisfatte.

Questo è un punto fondamentale da legare ai processi di cambiamento organizzativo in quanto fa emergere la necessità di coinvolgere la front line quando si considerano cambiamenti e miglioramenti perché lì si opera il processo e si mettono in atto le competenze particolari che possono influenzare i risultati del progetto. Il modello PDCA lo riconosce.

Limiti e insidie del ciclo di Deming

I seguenti punti devono essere considerati per evitare che le attività del PDCA siano slegate dalle attività strategiche del business.

- Il modello non tiene conto con la parte "umana" del cambiamento, tralasciando i concetti di resistenza e motivazione.
- Gli stili di leadership da adottare nelle differenti fasi del modello sono trascurati.
- Non vengono considerati i metodi di comunicazione tra il management e gli operativi.
- Il ciclo PDCA implica che il miglioramento divenga parte del lavoro di ogni persona, sebbene questi possano non essere competenti o sufficientemente addestrati.

- L'effettivo processo di lavoro potrebbe non essere progettato per ottenere i risultati attesi nel piano, perciò la qualità deve essere costruita in ogni elemento del processo prima di delegarne il miglioramento alle persone.
- Tutti i responsabili dell'implementazione del ciclo PDCA devono avere buona conoscenza e controllo del processo e delle iniziative di miglioramento per accettarle e renderle efficaci.
- Il ciclo PDCA è limitato nello scopo. È soprattutto orientato a migliorare singoli processi che a gestire grandi cambiamenti organizzativi: non tiene conto degli obiettivi strategici del business e può diventare un processo isolato dall'insieme delle iniziative di modifica delle strategie.

W. E. Deming

William Edwards Deming (14 ottobre 1900 – 20 dicembre 1993) è stato un professore e uno statistico americano. È conosciuto per il suo lavoro in Giappone, dove ha aiutato le aziende giapponesi ad avere successo mediante l'attuazione di misure di miglioramento continuo utilizzando metodi statistici incentrati sulla qualità.

Deming ha dato un contributo significativo alla reputazione del Giappone per l'innovazione e prodotti di alta qualità, insegnando al top management come migliorare la progettazione, il servizio, la qualità del prodotto, e il testing. Egli è famoso soprattutto per il suo modello Plan-Do-Check- Act e oggi il premio principale per la qualità in Giappone porta il suo nome.

4. GESTIONE DEI RISCHI

Gli ultimi approcci normativi antepongono al ciclo PDCA una logica di gestione del rischio. Questo tipo di approccio si pone come una ulteriore sovrastruttura concettuale che incorpora la dinamica del ciclo PDCA rinforzando la caratterizzazione applicativa rispetto al soggetto.

Ogni realtà organizzativa è differente dalle altre. Persone differenti, modelli di business diversi, disponibilità finanziaria, accesso a risorse relazionali, respiro locale o globale, prodotti e servizi variegati e così via.

Il ciclo PDCA ha inizio con la fase di "pianificazione" dove si decide che cosa è necessario fare e come farlo, quali risorse dedicargli e come dislocarle eccetera. Dopo il momento dell'azione le fasi di verifica e correzione richiedono ancora di ripartire con una nuova pianificazione.

Ai fini della massima efficienza ed efficacia – trovandosi l'azione diretta a sistemi economici cioè a sistemi con risorse limitate – il successo applicativo si massimizza se viene data la giusta priorità di intervento alle cose da fare. Questo significa scegliere tra le diverse opzioni possibili quelle con il miglior rapporto costo/efficacia.

Il processo di gestione del rischio consente di ottenere questo risultato.

Il processo di gestione del rischio soprassiede tutti i momenti del ciclo PDCA di pianificazione, esecuzione, controllo e correzione del sistema consentendo di mantenere il focus su una implementazione sempre efficace ed efficiente delle azioni necessarie.

Le principali normative internazionali sui sistemi organizzativi in generale (ISO 31000), sui dispositivi medici e sul farmaco in particolare (ISO 14971 e ICH 09), sono abbastanza concordi a suddividere il ciclo di gestione del rischio in alcuni momenti fondamentali che integrano il ciclo PDCA in perfetta logica di ottimizzazione.

L'attività di gestione del rischio è un approccio qualitativo. Attraverso tecniche di valutazione viene dotato di una componente quantitativa che ne consente una gestione più efficace. La fase di risk assessment – che dà inizio all'intero processo – prevede la catalogazione dei rischi secondo due dimensioni: la magnitudo e la probabilità di accadimento. Alle due dimensioni possono essere associati valori numerici o semantici per giungere a una matrice finale dove i rischi rilevati possono essere catalogati sulle due dimensioni ed essere associati a un "livello di accettabilità" che dipenderà dalle politiche di sistema definite nelle fasi iniziali di progettazione della sicurezza.

4.1 Modelli normativi di gestione del rischio

Di seguito si riassumono brevemente gli orientamenti delle normative citate rispetto agli Enti di emissione.

International Conference for Harmonization: ICH Q9 Quality Risk Management

È il riferimento per la gestione del rischio nell'Industria farmaceutica. Stabilisce come principio la protezione della salute del paziente e il riferimento alla conoscenza scientifica per stabilire il rischio per la qualità. La guida fornisce anche raccomandazioni per l'implementazione e sancisce che il livello di copertura, formalismo e documentazione del processo di quality risk management deve essere commisurato al livello effettivo del rischio.

La norma stabilisce inoltre come non sia sempre appropriato o necessario utilizzare un processo formale di gestione del rischio: l'utilizzo di processi informali può essere considerato accettabile.

La norma ICH Q9 è stata adottata dall'Unione Europea (European Union Annex 20 of the EU and PIC/S GMP Guides).

International Standards Organization ISO 14971 – Application of Risk Management to Medical Devices

Questo documento è stato sviluppato per le industrie dei dispositivi medici ma è stato anche raccomandato dal FDA americano per l'industria farmaceutica.

Tale standard internazionale specifica un processo per identificare i pericoli associati ai dispositivi medici per stimare e valutare i rischi associati, per controllare tali rischi e monitorare l'efficacia dei controlli.

I requisiti di questo standard sono applicabili a tutte le fasi di vita di un dispositivo medico. Lo standard non si applica alle decisioni cliniche e non stabilisce livelli di rischio accettabili.

Lo standard non richiede la presenza di un sistema di qualità residente ma ne può essere parte (la ISO 13485 sui sistemi di qualità per i dispositivi medici infatti la richiama espressamente come la nuova normativa sulle Good Distribution Practices).

International Standards Organization ISO 31000 – Risk Management – Principles and Guidelines

Questo standard internazionale fornisce principi e linee guida generiche sul risk management. Può essere utilizzato da qualsiasi soggetto pubblico, privato, associazione, gruppo o individuo, pertanto non specifica alcuna industria o settore.

Questo standard internazionale può essere applicato in tutta la vita di una organizzazione e a un'ampia gamma di attività incluse strategie e decisioni, operazioni, processi, funzioni, progetti, prodotti, servizi e risorse.

Questo standard internazionale può applicarsi a qualsiasi tipologia di rischio, di qualsiasi natura, che abbia conseguenze positive o negative.

Sebbene questo standard internazionale fornisca indicazioni generiche, non intende promuovere uniformità nei modi di gestione del rischio all'interno delle organizzazioni. Il progetto e l'implementazione dei piani di gestione del rischio e il quadro di riferimento devono considerare i diversi bisogni della specifica organizzazione, i particolari obiettivi, contesto, struttura, operazioni, processi, progetti, prodotti, servizi, risorse e pratiche impiegate.

Questo standard internazionale ha anche lo scopo di poter essere utilizzato come armonizzatore del processo di risk management in tutti gli standard presenti e futuri. Infatti fornisce un approccio comune a supporto di standard per settori specifici integrandoli senza cancellarli.

International Standards Organization ISO 31010 – Risk Assessment Techniques

Questo standard internazionale fa da supporto alla ISO 31000 e fornisce alcuni elementi guida sulla selezione e l'applicazione di tecniche per il risk assessment.

La valutazione dei rischi effettuata in accordo a questo standard contribuisce alle altre attività di risk management.

Lo standard introduce l'applicazione di una gamma di tecniche attraverso specifici riferimenti ad altri standard, i quali descrivono in dettaglio maggiore i relativi concetti e applicazioni.

Questo standard internazionale non fornisce criteri specifici per identificare il bisogno di analisi dei rischi, né specifica i metodi richiesti per particolari applicazioni.

Questo standard internazionale non tratta tutte le tecniche possibili e le tecniche non richiamate espressamente non vengono in alcun modo invalidate. Il fatto che una particolare metodologia sia applicabile a una determinata circostanza non postula che tale metodo debba obbligatoriamente essere applicato.

4.2 Cenni sugli strumenti del Risk Management

Il processo di Risk Management è affiancato da tecniche specifiche. La seguente tabella ne riporta le più conosciute.

	FTA	**FMEA/FMECA**	**HACCP**	**PHA/PRA**
Principio	Strumento deduttivo grafico e strutturato	Strumento induttivo strutturato. Può essere qualitativo e quantitativo	Previene i pericoli noti riducendone i rischi in specifici punti di controllo (CP)	Strumento induttivo qualitativo
Vantaggi	Diagramma visuale dei problem con simboli standard che illustrano il percorso dagli eventi base fino all'evento indesiderato	Universale e scalabile sia per valutazioni del rischio ad alto livello che di dettaglio	Processo completo di gestione del rischio. Specifico e flessibile focalizzato sulla prevenzione. Mantiene registrazione delle responsabilità sul prodotto e sulle questioni di compliance	Facilmente adattabile alla maggioranza delle situazioni
Limitazioni	Può diventare velocemente molto complesso in quanto analizza un problema alla volta.	Lo strumento non considera problemi di operatività o le performance degli operatori. Non mostra le interazioni tra i diversi eventi.	Richiede informazioni dettagliate sul prodotto e sul processo	Relativamente non strutturato perciò può tralasciare potenziali pericoli
Strumento	Grafici con simboli standard. Raccomandato con software dedicati	Tabelle	Diagrammi di processo dettagliati. Tabelle.	Disegni e tabelle
Principali applicazioni e utilizzi	Utilizzato per definire un particolare evento indesiderato e identificare le cause (evento base). Per potenziali problemi ad impatto elevato	Utilizzo universale (es. dispositivi medici, ospedali). Utilizzato per identificare potenziali e noti modi di guasto e l'impatto sui processi, infrastrutture ed equipaggiamenti. Si usa durante il progetto e le operazioni.	Industrie del cibo e chimiche. Adattato per l'industria farmaceutica dal WHO. Copre tutta la catena del prodotto.	Utilizzato nelle fasi iniziali dei nuovi prodotti e delle modifiche ai prodotti e processi (fase di progetto). Adatto per le industrie chimiche. Rappresenta il primo passo di una valutazione del rischio complessa.

4.3 Strumenti per la gestione del Security Risk

Piano generale di gestione del rischio (Risk Management Master Plan)

Una delle maggiori sfide nella gestione del rischio è quello di rendere oggettiva la valutazione, il che significa renderlo indipendente dalle opinioni soggettive dei soggetti coinvolti nella valutazione. La legislazione non dà alcuna soluzione a questo problema specifico e diverse metodologie nonché autori privati danno risposte differenti al problema.

Ad esempio, i numeri consigliati per la gamma delle probabilità o la gravità possono variare da 0 a 1 piuttosto che da 5 a 10. Alcuni metodi includono "rilevabilità" o "probabilità di scoperta" nella formula e vi è anche incoerenza nelle stesse formule utilizzate per il calcolo.

Tuttavia, mentre può essere molto difficile ottenere una condivisione comune a tutta l'industria del processo formale e dei criteri per valutare il rischio, all'interno di una determinata organizzazione le cose vanno diversamente.

I Master Plan, in generale, sono ottimi strumenti per ottenere la condivisione di argomenti specifici. Ad esempio, i piani generali di convalida sono ben accettati e frequentemente usati per garantire la coerenza e l'efficacia dei progetti di convalida.

Il Risk Management Master Plan fornisce una struttura per le pratiche di gestione del rischio di processi e attrezzature. Questa garantisce che la valutazione dei rischi e i controlli vengano effettuati in modo efficace e coerente in tutta l'organizzazione, così come la soddisfazione dei requisiti normativi, dei clienti, della qualità e del business.

Il piano dovrebbe garantire che le procedure di gestione del rischio della società abbiano basi scientifiche e che essi siano compresi e seguiti in tutta l'organizzazione.

In generale il Risk Management Master Plan descrive:

- La Politica di gestione del rischio della organizzazione.
- I legami tra gli obiettivi organizzativi della società e delle politiche e la politica di gestione del rischio.
- La relazione del piano di gestione del rischio con altri documenti, ad esempio, piani di validazione o manuale della qualità.

- L'approccio al processo di gestione del rischio della organizzazione.
- I membri del team di gestione del rischio (per funzione).
- Le responsabilità del capo progetto e membri del team.
- I prodotti e processi che dovrebbero essere coperti dalla gestione del rischio.
- Il contenuto dei singoli piano di Risk Management per progetto.
- La procedura dettagliata per la gestione del rischio.
- Come si definisce la probabilità.
- Come identificare i livelli di rischio.
- I fattori che contribuiscono ad alta e bassa gravità.
- La definizione e determinazione di RPN con esempi.
- I criteri ed esempi per le soglie di rischio accettabili.
- Come fare una valutazione del rischio di alto livello.
- La comunicazione di stato del progetto e l'esito dei processi di gestione del rischio.
- La frequenza e procedure per la revisione.

Il Master Plan di gestione del rischio dovrebbe essere sviluppato da un team interfunzionale al più alto livello possibile, per garantire la presenza del maggior numero di prospettive di analisi.

Procedure

Dovrebbero essere sviluppate procedure standard per avviare, attuare e aggiornare i singoli progetti di gestione del rischio per applicazioni specifiche. Esempi sono: valutazione dei fornitori basato sul rischio, validazione in base al rischio del sistema informatico o test basati sul rischio di materie prime per la produzione di farmaci. Sviluppo e utilizzo di tali procedure dovrebbero essere controllati dal quality assurance aziendale per garantire un uso coerente in tutta l'organizzazione.

Modelli e forme

Modelli e forme con esempi e diagrammi di flusso di processo sono strumenti semplici ma preziosi per migliorare la coerenza e l'efficienza per l'identificazione, valutazione e controllo dei rischi. Possono essere parte di SOP o del Master Plan di gestione del rischio o possono essere singoli documenti. Gli esempi sono particolarmente importanti per dare consigli su elementi di valutazione del rischio come la probabilità, individuabilità e la gravità.

Esempi e Casi

Mentre le organizzazioni acquisiscono esperienza con progetti di gestione del rischio e dopo che vari progetti sono stati eseguiti, dovrebbe essere sviluppata una libreria con esempi rappresentativi. Gli esempi aiutano manager e team di progetto per identificare, valutare e controllare i rischi. La biblioteca dovrebbe includere esempi buoni e non andati a buon fine. Ogni esempio dovrebbe includere raccomandazioni su come procedere con progetti simili.

Check list

Le check list sono elenchi di pericoli, eventuali danni e controlli che sono stati sviluppati per esperienza sia come risultato di progetti di valutazione precedenti o come risultato di fallimenti passati. Ad esempio, il desk IT può generare un elenco per vari sistemi informatici. Lo scopo delle check list è non dimenticare pericoli comuni importanti e le fasi di controllo.

Database del rischio

Un database aziendale con esempi di pericoli, di rischi e dei danni all'interno di una società contribuisce a facilitare la raccolta e la manutenzione dei dati di rischio. Aiuta anche ad armonizzare la valutazione all'interno di una società. Mentre inizialmente non ci possono essere molti dati, tale database fornirà maggior valore nel momento in cui potrà essere popolato con i dati dei progetti di gestione del rischio via via che vengono svolti.

Registro dei rischi di sicurezza (security)

Il Registro dei rischi di Security è il documento che in fase iniziale entra a far parte dei dati di input alla progettazione del sistema per la gestione della sicurezza.

Successivamente esso deve essere sottoposto a revisione durante gli incontri di Design Review (momenti del ciclo di vita progettuale dove si decide se quanto disegnato fino a quel momento soddisfa i requisiti e si può passare alle fasi successive del progetto) in modo da essere utilizzato come strumento per il controllo del livello di rischio del sistema fino alla sua implementazione.

Il Registro dei rischi di Security deve essere utilizzato anche come documento di input per le modifiche alla progettazione e va considerato in ogni intervento di change management.

4.4 Elementi per la riduzione dell'impatto di rischio residuo da coprire attraverso gli strumenti assicurativi

Attraverso un sondaggio interno su un campione significativo di associati ANIA conferma che il furto di medicinali presso le strutture ospedaliere è ritenuto dalle Compagnie un fenomeno di particolare attenzione. Infatti negli ultimi anni le stesse hanno subito dei sinistri molto importanti relativi a tale causale con notevoli esborsi.

La copertura dei rischi associati a questa fattispecie e la relativa onerosità del premio, risulta fortemente condizionata dalla presentazione – da parte dell'Azienda richiedente – di una informativa approfondita su alcuni aspetti:

- Sinistrosità pregressa;
- Misure di prevenzione/protezione dei rischi;
- Codici di comportamento interni alle strutture sanitarie.

Chiaramente informazioni positive e dettagliate consentono di elaborare offerte più vantaggiose in termini di tasso e soprattutto di massimali garantiti.

Si evidenzia inoltre che la garanzia generalmente viene concessa solo all'interno di una copertura più ampia incendio e furto (all risks).

Tale copertura si perfeziona tendenzialmente attraverso una specifica deroga per i farmaci, con l'introduzione di limiti d'indennizzo specifici rispetto alle condizioni standard contrattuali previste per il furto del "contenuto generico".

4.4.1 Garanzia furto farmaci: esempio di implementazione contrattuale

In questo paragrafo si riportano a titolo di esempio alcuni casi di clausole che descrivono i mezzi di protezione necessari affinché la garanzia assicurativa si possa intendere operante (fonte ANIA).

Esempio 1: condizione generale di copertura

> *"(…) limitatamente al* ***furto dei medicinali e/o farmaci****, l'assicurazione si intende operante a condizione che i locali contenenti le cose assicurate siano protetti, al momento del sinistro, dai seguenti mezzi di protezione.* ***Si conviene altresì che in assenza totale o parziale di anche uno solo dei mezzi di protezione di seguito descritti la presente garanzia non sarà in alcun modo operante****(…)".*

Successivamente a definizioni generali di applicabilità della copertura come quella evidenziata dall'esempio 1, spesso si vanno ad inserire clausole specifiche che entrano nel dominio della tecnica come quelle degli esempi seguenti.

Esempio 2: requisiti specifici di allarme e sensoristica

> *"(…) impianto di allarme volumetrico a doppia tecnologia collegato con ponte radio bidirezionale e/o in alternativa con sistema GSM (meglio il ponte radio bidirezionale) ad un Istituto di Vigilanza o a servizio equivalente a protezione dei locali destinati a deposito di farmaci e farmacia (è preferibile il collegamento anche con la guardiania interna). Per eventuali porzioni di locali, destinati alle funzioni di cui sopra, costruiti con materiali diversi dalla "muratura" e comunque limitatamente a piccole porzioni interne al complesso immobiliare dell'ospedale, si dovranno valutare soluzioni di protezione adeguate, con l'applicazione minima di sensori di vibrazione collegati all'impianto di allarme da applicare a predette pareti e relativi infissi (…)".*

Esempio 3: requisiti specifici strutturali

"(…) porte blindate a tutti gli accessi dei depositi ed alle farmacie, ben fissate nelle pareti in muratura (…)".

"(…) vetri stratificati di sicurezza alle finestrature quando non protette da inferriate. Tali protezioni sono indispensabili nelle aperture verso l'esterno dei locali contenti le cose assicurate, situate in linea verticale a meno di 4 m dal suolo o da superfici acquee, nonché da ripiani accessibili e praticabili per via ordinaria. Qualora, in taluni casi, si dovessero prendere in considerazioni inferiate, queste dovranno essere in ferro a piena sezione dello spessore minimo di 15 mm, ancorate nel muro, con luci, se rettangolari, aventi lati di misura rispettivamente non maggiori di 50 e 18 cm oppure, se non rettangolari, di forma inscrivibile nei predetti rettangoli o di superficie non maggiore di 400 cm^2 (…)".

Gli esempi illustrati fanno comprendere bene che gli oneri collegati al trasferimento di rischio residuo allo strumento assicurativo sono in correlazione inversa alla capacità dell'Azienda di dotarsi di strumenti integrati di gestione della sicurezza che possano essere in grado di rispondere alla visione assicurativa.

Le misure tecniche – incastonate in un coerente quadro progettuale – richiedono e integrano adeguati codici di comportamento interni alle strutture sanitarie e sistemi in grado di misurare gli accadimenti (sinistrosità pregressa) in logica di continuo intervento correttivo e preventivo sul disegno stesso del sistema di gestione per la sicurezza.

Questa logica – base dell'intero rationale di copertura con lo strumento assicurativo del rischio residuo – è la medesima utilizzata per guidare con il presente documento il disegno di sistemi di sicurezza adeguati.

4.5 Risk Assessment

La valutazione dei rischi (Risk Assessment) è definito dalla [ISO/IEG Guide 51: 1999, definition 3.12J] come "Processo complessivo che comprende l'analisi del rischio e la stima del rischio".

Per Analisi del Rischio (Risk Analysis) sempre la [ISO/IEG Guide 51: 1999, definition 3.10] dichiara "utilizzo sistematico delle informazioni di-

sponibili per identificare i pericoli e stimarne il rischio", a cui si affianca la nota della ISO 14971:2012 "L'analisi dei rischi include l'esame di differenti sequenze di eventi che possono produrre situazioni di pericolo e danni".

La Stima del rischio (Risk Evalutation) è secondo la [ISO 14971: 2012, definition 2.21] il "processo di comparazione tra il rischio stimato verso criteri di stima dati al fine di determinare l'accettabilità del rischio".

La valutazione dei rischi deve essere personalizzata in base a due argomenti generali:

- lo scenario criminale della zona;
- gli scenari di attacco a siti ospedalieri;
- la specifica situazione del sito in oggetto (infrastrutture, strumenti, personale ecc.).

Sulla base del Security risk master Plan deve essere redatta la prima release del Registro dei Rischi con i risultati della valutazione del rischio in situazione "as is" prima di ogni intervento progettuale per la sicurezza.

4.5.1 Valutazione preliminare dello stato di sicurezza della FO: il LMS

Quando si inizia ad approcciare per la prima volta il problema della sicurezza per il sito della FO invece di affrontare uno studio di risk assessment si è visto come possa essere molto più utile avvalersi dello strumento informatico messo a disposizione da SIFO con il progetto Padlock.

In questo caso si procede a registrare la Direzione sull'apposito sito del progetto Padlock e si affronta la serie di quesiti che vengono presentati dallo strumento.

È opportuno che – prima di iniziare a utilizzare lo strumento – si formi un gruppo di lavoro che annoveri almeno le seguenti competenze/conoscenze:

- gestione dei processi della FO;
- conoscenza degli attuali sistemi di sicurezza;
- conoscenza degli attuali impianti;
- conoscenza della pianta della FO e dell'ospedale (entrate/uscite, finestre, porte, consistenza delle pareti, locali adiacenti ecc.);
- conoscenza degli orari del personale ospedaliero, presidi PS ecc.

La compilazione dei dati richiesti dallo strumento di valutazione del LMS (Livello Minimo di Sicurezza) deve essere intesa come lavoro di gruppo. La diffusione del responso invece può essere a disposizione del solo Direttore della FO che deciderà in merito alla diffusione.

I risultati vengono presentati secondo l'indice Lockpill definito attraverso lo studio dedicato all'interno del progetto Padlock 2 e sono accompagnati da una coerente indicazione delle azioni generali che è opportuno intraprendere coerentemente con il valore Lockpill risultante dalla valutazione.

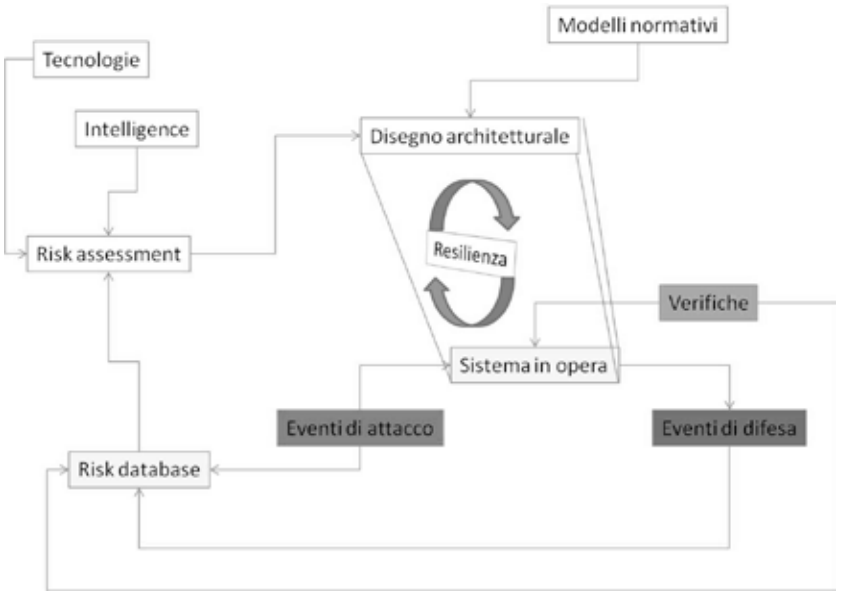
Il passaggio dello strumento informatico di valutazione consente di evitare approcci alla risoluzione del problema della sicurezza che non sarebbero percorribili in situazioni non sufficientemente mature.

Lo strumento pertanto suggerisce percorsi verso un LMS accettabile adatti a tutti i differenti scenari che si possono presentare nella FO italiana.

5. PROGETTAZIONE DEL SISTEMA PER LA GESTIONE DELLA SICUREZZA

Questo capitolo illustra i diversi momenti necessari per dimensionare correttamente un sistema di gestione per la sicurezza rispetto agli effettivi rischi per la garanzia di sicurezza in una determinata realtà operativa.

Lo schema seguente illustra il rationale alla base della progettazione di un sistema di gestione per la sicurezza che sia efficace e che possa offrire le necessarie caratteristiche di resilienza.



La resilienza si costruisce nella permanenza delle relazioni tra i diversi elementi del sistema. La continua attenzione a ciò che accade al sistema messo in opera e il monitoraggio ambientale dell'intelligence consentono di adeguare il disegno architetturale in logica preventiva – grazie all'adozione di modelli di risk management – al fine garantire la massima resilienza del sistema in presenza di eventi avversi.

5.1 Disegno architetturale del sistema

Uno degli output della prima fase di valutazione del rischio per la sicurezza è la messa in evidenza degli scenari di rischio e dei punti di debolezza.

Gli scenari di rischio così evidenziati vanno a definire il perimetro di intervento che diventa lo scopo del progetto del sistema di gestione per la sicurezza.

Gli scenari di rischio vanno ad interessare l'aggregazione di una serie di possibili eventi avversi così come si delineano in fase di analisi dei rischi.

Il singolo scenario di rischio si presenta quindi come una regola di correlazione tra una serie di eventi avversi o indesiderati.

Scopo della progettazione diventa il disegno di percorsi di risposta immediata all'accadimento degli specifici scenari di rischio e, allo stesso tempo, va a delineare comportamenti e procedure che intervengano in una logica architetturale di tipo preventivo.

L'intero sistema di gestione per la sicurezza deve essere disegnato specificatamente per il sito.

Non esistono due siti che condividano esattamente le stesse situazioni: differenze nell'organizzazione, ambiente di riferimento, personale sono tipiche così di fatto non esiste una soluzione buona per tutti.

La progettazione per la sicurezza segue un ciclo incrementale a partire dal Riesame degli scenari di rischio e della documentazione disponibile.

Tutta la documentazione raccolta, come le normative di settore o le guide specifiche dell'ente di appartenenza o del settore di appartenenza sulla sicurezza, sarà utilizzata come documentazione di riferimento per la progettazione. Per lo stesso motivo vanno opportunamente raccolti tutti i documenti relativi ad eventuali eventi avversi in ogni forma in cui si possano presentare.

Vanno raccolti tutti gli elementi documentali inerenti il sito – infrastrutture, mappe, impianti ecc. – e la documentazione inerente eventuali proprietà adiacenti e utilizzate ai fini dell'attività del sito stesso.

In questa fase si inizia la Redazione del master plan per la sicurezza. Tutta l'attività di raccolta dei dati di ingresso alla progettazione deve essere documentata.

L'attività di riesame dei risultati dell'analisi del rischio innesca in parallelo la pianificazione della progettazione del sistema di gestione per la sicurezza.

Partendo dalle conoscenze acquisite sul perimetro dei rischi e dall'obiettivo di costruire un sistema di gestione per la sicurezza adeguato, va sviluppato un piano del progetto che contenga le risposte ai seguenti quesiti: quali attività devono essere previste? Chi dovrà essere coinvolto nel progetto e per quanto tempo di svilupperà il progetto? Quali risorse serviranno?

Il piano di progetto può assumere diverse forme, da quelle più sofisticate a quelle più semplici a seconda della natura, della durata e della complessità delle attività di progettazione.

È perciò necessario allineare la complessità del piano del progetto alla natura del prodotto o del servizio da progettare. In alcuni casi – come la protezione di uno stanzino con i farmaci di reparto posto all'ultimo piano di una struttura ad accesso controllato – i piani di progetto possono essere dei semplici memo o un diagramma di flusso, mentre per situazioni più complesse un piano di progetto può includere diversi documenti come i diagrammi di Gantt, il percorso critico, la WBS, ecc.

Il piano di progetto dovrà, in ogni caso, gestire una serie di variabili, documentandole direttamente (autoportante) o richiedendo la predisposizione di documentazione specifica da rilasciare per garantire che tutte le decisioni progettuali siano tracciate e motivate:

- Durata del progetto – Quando inizia la progettazione? E quando è previsto che finisca? La durata stimata è in linea con la natura e la complessità del progetto?
- Attività della progettazione – Quali sono le attività che devono essere svolte per progettare e sviluppare i vostri prodotti e servizi? In quale sequenza devono essere svolte? In quali fasi andranno riesaminate per verificare che siano state svolte al meglio?
- Verifica e validazione – La verifica è l'attività di confronto tra gli input della progettazione e i suoi output (ad esempio la verifica che il sistema di telecamere funzioni, copra le aree desiderate e registri per il tempo predeterminato) mentre la validazione consiste nell'accertarsi che la progettazione possa dare i risultati attesi in certe condizioni di utilizzo del prodotto (ad esempio che il motion control faccia scattare l'allarme simulando un determinato scenario con soggetti reali). Entrambe queste attività devono essere pianificate.

- Responsabilità e autorità – Chi verrà coinvolto nelle attività di progettazione e sviluppo? Cosa dovrà fare ogni persona? Che autorità avrà ogni individuo? Le persone coinvolte comprendono e accettano le loro responsabilità?
- Risorse – Quali risorse interne ed esterne (soldi, spazi, macchinari, materiali, fornitori, ecc.) servono per completare il progetto? Sono state assicurate?
- Interfacce – Le persone che hanno la responsabilità delle attività di progettazione e sviluppo con chi si interfacceranno e interagiranno?
- Coinvolgimento degli utilizzatori interni ed esterni alla FO – è bene prevedere queste attività per capire come e se debbano essere modificati gli attuali comportamenti del personale che gravita attorno alle attività della FO.
- Requisiti della installazione – Bisogna pianificare come la progettazione influirà sulle altre parti dell'organizzazione. Ci sono requisiti relativi alla sicurezza da prevedere? Ci sono problematiche ambientali da tenere presenti? Ci sono implicazioni che riguardano l'imballaggio, l'immagazzinaggio e il trasporto? Ci sono implicazioni che riguardano l'installazione degli impianti e l'interfaccia degli stessi con gli impianti già residenti?
- Livello di controllo – I processi di progettazione e sviluppo devono essere sotto il pieno controllo dell'organizzazione ma ci sono certi aspetti della progettazione (partecipazione delle parti interessate – fornitori o appaltatori – alle riunioni di riesame, verifica e validazione della progettazione) che possono essere fuori dal controllo dell'azienda e che vanno ben definiti.
- Informazioni documentate – Durante la pianificazione della progettazione occorre definire quali documenti e registrazioni serviranno durante le attività di progettazione e sviluppo.

L'output dell'attività di progettazione è il documento di architettura del sistema che definisce le soluzioni che dovranno essere implementate come sottosistemi e le loro relazioni al fine di coprire la logica bidimensionale deterrenza/reazione del sistema garantendo il livello di risposta voluto.

5.1.1 Modellazione del sistema e scelta dei sottosistemi

Il modello generale del sistema prevede la definizione del migliore mix di elementi che possa soddisfare la copertura dei rischi rilevati dalla relativa analisi per il sito che si sta considerando.

Il modello generale del sistema si esemplifica in una mappatura di governance che illustra come i differenti elementi – i sotto-sistemi – dovranno dialogare tra di loro per garantire la migliore gestione delle strategie di rilievo delle minacce da una parte e di quelle di risposta dall'altra.

Parte della modellazione del sistema è la configurazione dei sotto-sistemi secondo una logica comune di interpretazione che vede ogni sistema come un insieme di mezzi, strumenti, persone, procedure.

Per ogni sotto-sistema viene definito uno scopo specifico che innesca un ciclo di attivazione dei componenti del sotto-sistema stesso di questo tipo:

- Rilievo della minaccia da parte di sensori a questo preposti;
- Gestione della comunicazione dei dati relativi alla minaccia con eventuali momenti di integrazione preliminare al fine di migliorarne il contenuto informativo;
- Interpretazione dei dati e delle informazioni e successiva decisione di innesco delle procedure di risposta;
- Esecuzione delle operazioni di risposta per innescare gli allarmi, comunicare la situazione agli organi preposti, richiedere interventi esterni.

Gli ultimi due elementi possono essere parte del singolo sotto-sistema in toto o possono essere dei sotto-sistemi generali di servizio che comunicano con il sotto- sistema originante.

5.1.2 Principi base dell'allarme

Nel disegno di un sistema di gestione per la sicurezza particolare importanza riveste il concetto di allarme.

La filosofia dell'allarme costituisce il razionale di base per il sottosistema di allarme. In fase di progettazione la filosofia dell'allarme dovrebbe risolvere i seguenti argomenti:

- Le funzioni principali dell'allarme: avviso e registrazione.
- Il ruolo dell'operatore, come questo debba cambiare in accordo allo stato operativo e quale supporto debba essere fornito all'operatore in ogni stato.
- Come il progetto debba tenere in considerazione le limitazioni umane.
- L'utilizzo delle priorità: lo scopo di usare le priorità, come queste sono definite nel sistema, e il rationale che supporta tale definizione
- L'innesco dell'allarme, descrivendone lo scopo e come l'operatore dovrebbe essere formato in merito.
- Gli Standard.
- I principi di generazione degli allarmi.
- I principi di strutturazione degli allarmi.
- I mezzi di presentazione (schermi, led, sirene ecc.).
- L'accesso controllato alla centralina di comando e gestione degli allarmi.

Fondamentali da includere nella filosofia sono i seguenti principi di base:

- Ogni allarme deve richiedere una risposta da parte dell'operatore.
- Deve essere definito e permesso un tempo adeguato affinché l'operatore possa rispondere.

5.1.3 Approccio a complessità modulare crescente

Non tutti i farmaci sono soggetti a furto, la fattispecie è limitata a determinate categorie – tendenzialmente farmaci ad alto costo/basso volume – e questo aspetto deve essere considerato quando si progetta la strategia di risposta agli scenari di attacco mappati in fase di risk assessment.

L'approccio architetturale dovrebbe prevedere – nel deployment dei sotto-sistemi nella peculiare orografia del sito – una disposizione modulare degli strumenti di deterrenza che incrementi in rapporto alla prossimità delle zone di stoccaggio dei farmaci a rischio maggiore di furto.

L'utilizzo di sotto-sistemi a tecnologia fumogena – che sono per natura associati a determinati costi di manutenzione e ripristino – può essere un utile elemento da piazzare come ultimo baluardo, così come l'utilizzo di gabbie di acciaio e porte blindate a protezione dei prodotti più sensibili.

5.1.4 Logiche di ridondanza

Un adeguato livello di sicurezza non può essere raggiunto attraverso sistemi monodimensionali.

Le strategie di risposta agli scenari di attacco deve prevedere diverse modalità sia dal punto di vista del rilievo dell'evento avverso che da quello della deterrenza verso il potenziale attacco.

Ad esempio è opportuno che le informazioni che attraversano un sotto-sistema di sensori di presenza sia separato dal flusso delle informazioni gestite da un sotto-sistema di sensori di contatto/vibrazione. Questo abbatte il rischio di inibizione del passaggio dell'informazione relativa all'attacco verso la centrale di allarme dovuto alla possibile disattivazione di un sotto-sistema.

La stessa cosa vale per le modalità di comunicazione della centrale di allarme con i destinatari dell'informazione che va prevista su differenti canali di telecomunicazione (linea telefonica fissa, linea mobile GSM, ponte radio).

5.1.5 Design Review

Per garantire la massima qualità del disegno del sistema di gestione per la sicurezza, vengono pianificate una serie di riunioni multidisciplinari tra le differenti competenza coinvolte nello sviluppo.

Questo tipo di incontri viene definito "design review" dalle maggiori normative e pratiche di progettazione e fondamentalmente sono definiti come di seguito.

Design Review: si tratta di incontri per la revisione dei risultati della progettazione condotti ad appropriate fasi dello sviluppo del sistema. Tali attività devono essere preventivamente pianificate, formalmente eseguite e documentate.

I design review richiedono la partecipazione dei rappresentanti di tutte le competenze coinvolte nelle fase specifiche del disegno di sistema sotto revisione assieme a tutti gli specialisti necessari. Il coordinamento delle attività dovrebbe essere assegnato a una persona che non abbia dirette responsabilità sul disegno specifico.

Il formalismo del meeting lo rende uno strumento atto ad assicurare che gli output della progettazione attesi nella fase specifica sotto esame rispondano agli input di progetto per quella stessa fase.

5.2 Disegno dei sottosistemi

Si tratta dell'attività di implementazione dei sottosistemi tecnici all'interno del quadro architetturale generale del sistema uscito dall'attività di disegno del sistema.

Il documento di architettura viene organizzato secondo le due dimensioni Dissuasione/Reazione e definisce la forma e le prestazioni del sistema che sarà necessario mettere in opera per garantire il livello di sicurezza desiderato nella particolare struttura.

I sotto-sistemi per la sicurezza possono essere prodotti tecnici o servizi specialistici, nel mix più opportuno definito in fase di disegno architetturale del sistema. La loro natura e le caratteristiche importanti ai fini della progettazione sono richiamati nel paragrafo dedicato di questa guida "Sistemi e servizi tecnici".

Per ogni sotto-sistema definito nel disegno architetturale sono definite le specifiche dei requisiti tecnici da sottoporre all'accettazione dei fornitori.

Sulla base di dette specifiche i fornitori dei sottosistemi provvedono all'esecuzione dei progetti tecnici elaborati sulla base delle norme tecniche applicabili e dichiarano le certificazioni e verifiche necessarie ai sensi di legge e le modalità tecniche di verifica dei requisiti architetturali che saranno eseguite e documentate in fase di validazione.

Per i sotto-sistemi forniti da più fornitori deve essere definito il fornitore – il prime contractor dove applicabile – responsabile per le verifiche di interfaccia e di integrazione delle varie componenti fino al sottosistema.

Viene infine svolta l'attività di raccolta e accettazione delle specifiche di dettaglio dei fornitori dei sotto- sistemi tecnici e vengono pianificate le verifiche prestazionali dei sotto-sistemi.

La verifica di completezza e pertinenza della documentazione di pianificazione per la costruzione e verifica dei sotto-sistemi viene formalizzata in un apposito incontro di Design Review.

5.2.1 Disegno del profilo di performance del sottosistema

Ci sono due dimensioni di sviluppo delle performance di sicurezza del sotto-sistema che diventano anche strumento di valutazione nel caso di auditing interni o esterni:

- il numero di elementi tecnici;
- il livello di performance degli elementi tecnici.

Queste due dimensioni di sviluppo danno luogo a un grafico, denominato "profilo di performance" caratteristico di ogni sotto-sistema. Il "profilo di performance" viene quindi sintetizzato dal "indice di security performance" del sottosistema che viene calcolato come media della somma pesata dei valori assegnati al livello di performance dei singoli elementi tecnici.

L'"indice di security performance" del sottosistema consentirà ai progettisti di valutare in modo sintetico la prestazione del sistema integrato finale come guida per l'ottenimento del livello di sicurezza voluto rispetto ai risultati dell'analisi dei rischi.

5.2.2 Disegno dell'indice di performance degli elementi tecnici

Per il calcolo del livello di performance del singolo elemento tecnico si utilizzano due criteri:

- Il "grado di integrazione" con gli altri elementi del sotto-sistema o del sistema complessivo (es. TVCC dedicato, integrato locale interno, integrato globale interno, integrato locale visibile da stazione di intervento esterna, integrato globale visibile da stazione di intervento esterna);
- Il "grado di performance" rispetto allo stato della tecnica in quel momento (es. TVCC – telecamera "fake", telecamera bassa risoluzione, telecamera alta risoluzione, telecamera con visione notturna, motion control, riconoscimento dei volti).

L'indice di performance del singolo elemento tecnico è un numero da 0 (non presente) a 5 (massimo livello della tecnica e dell'integrazione) calcolato come il prodotto dei valori assegnati alle due dimensioni rapportato a 5.

L'indice di performance consente di decidere il livello di complessità in senso costo/efficacia degli elementi tecnici che saranno implementati nel progetto del sistema.

5.2.3 Verifiche intermedie

Va prevista una fase di controlli pianificati della progettazione che verifichi il rispetto del flusso di progettazione, la pianificazione, i deliverables, le modifiche alla progettazione, il rispetto dei requisiti architetturali del sistema, il rispetto dei requisiti prestazionali dei singoli sotto-sistemi.

Con la Design Verification si valuta la conformità ai requisiti e la conferma che i risultati della progettazione sono coerenti ai requisiti di ingresso alla progettazione viene documentata in appositi rapporti. Si verifica che il prodotto sia stato "costruito correttamente", cioè si tratti effettivamente di quanto desiderato.

5.2.4 Desing Review di integrazione

Il fornitore – il prime contractor dove applicabile – responsabile per le verifiche di interfaccia e di integrazione delle varie componenti fino al sottosistema dovrà fornire il piano e le modalità tecniche di verifica e richiamare tutte le norme tecniche di riferimento e dichiarare le certificazioni che sarà necessario esibire ai sensi di legge per tutti i componenti del sottosistema.

La verifica di completezza e pertinenza della documentazione di pianificazione, costruzione e verifica dei sotto-sistemi viene formalizzata in un apposito incontro di Design Review.

Nello stesso incontro dovrà essere verificata l'efficacia dell'attività di "Design Transfer" con la quale si intende l'assicurazione che le specifiche architetturali siano recepite e correttamente tradotte in specifiche di prodotti in grado di rispondere ai requisiti voluti.

5.2.5 Performances del sistema di allarme

Devono obbligatoriamente essere definiti i requisiti del sistema di allarme.

I requisiti prestazionali sono importanti per assicurare che il sistema di allarme sia utile per gli operatori in tutte le situazioni operative pertinenti. Il monitoraggio delle prestazioni dovrebbe servire come input per il processo di miglioramento del sistema di allarme.

Deve essere impiantato un sistema di monitoraggio delle prestazioni che preveda strumenti e metodi per misurare i diversi indicatori di presta-

zioni del sistema di allarme. Il sistema di monitoraggio deve essere utilizzato per periodiche analisi delle prestazioni per identificare i problemi o le debolezze nel sistema di allarme, sia durante il funzionamento normale che in presenza di disturbi nel processo.

Queste informazioni dovrebbero essere utilizzate per il miglioramento continuo del sistema. Se è disponibile un simulatore del processo, il sistema di controllo deve essere usato in combinazione con il simulatore per la regolazione delle prestazioni del sistema di allarme per quanto riguarda i limiti di allarme, il filtraggio del segnale, soppressione di allarme, ecc, in una vasta gamma di condizioni di processo.

Le misure di performance includono:

- Tasso di allarmi in ingresso (con distribuzione di priorità);
- Numero di allarmi in lista principale (con distribuzione di priorità);
- Distribuzione di frequenza degli allarmi: per individuare eventuali "cattivi attori" che contribuiscono in modo significativo al carico complessivo di allarme (incrementando i rischi di sovraccarico delle informazioni);
- I tempi di risposta dell'operatore (tempo prima dell'accettazione): tempi di risposta troppo lunghi o troppo corti indicano che il sistema non viene utilizzato come previsto.

Tassi di allarme in condizioni operative stabili (valori medi):

- Più di 1 allarme ogni minuto: probabile che sia inaccettabile;
- Uno ogni due minuti: rischia di essere ingestibile;
- Uno ogni 5 minuti: inizia a essere gestibile;
- Meno di uno ogni 10 minuti: molto probabile che sia accettabile anche in strutture di risposta piccole.

Tassi di allarme durante le principali condizioni di disturbo (valori medi):

- Più di 10 allarmi al minuto: Decisamente eccessivo e molto probabilmente portano l'operatore ad abbandonare l'uso del sistema;
- 2-10 al minuto: difficile da affrontare;
- Meno di 1 al minuto: dovrebbe essere gestibile, ma può essere difficile se allarmi diversi richiedono una risposta complessa all'operatore.

Va verificato che la distribuzione di priorità degli allarmi che si verificano per un disturbo sia effettivamente utile al fine di concentrare l'attenzione sui pochi allarmi importanti in quel momento.

Altre azioni registrate dell'operatore potrebbero essere analizzate statisticamente alla ricerca di possibili falsi allarmi, identificando gli allarmi che vengono spesso accantonati o i limiti di allarme che vengono cambiati di sovente.

Gli avvisi vanno progettati in logica di escalation ed è molto importante il concetto di percezione:

- Percezione: La registrazione di input sensoriali. Affinché l'informazione di allarme possa essere facilmente percepita, è importante che sia ben visibile tra gli altri tipi di informazioni e sia facile interpretare gli elementi essenziali – cosa c'è di è sbagliato, dove si trova, quanto è grave.

5.2.6 Diversivi

L'impostazione degli allarmi deve essere progettata in modo che possa essere efficace anche in situazioni di diversivo come quelle rappresentate da un concomitante allarme anti incendio o sale di emergenza sovraccariche o anomali assembramenti di persone dovuti a orari di servizi limitrofi concomitanti (zone di ritiro farmaci territoriali, magazzino economale adiacente, ritiro merce per consegna ai reparti, ingresso ambulanze/pronto soccorso adiacente o limitrofo ecc.)

5.3 Validazione del sistema

Alla fine della progettazione, dopo l'implementazione del sistema completo nel sito vanno previste tutte le attività necessarie per verificare la rispondenza del sistema ai requisiti prestazionali, la capacità di risposta agli scenari di minaccia simulati, la preparazione del personale, la validazione delle attività di comunicazione, la presenza di tutti i piani di gestione e manutenzione.

Come condiviso dalle più diffuse normative internazionali si intende per Validazione:

- La Validazione segue la positiva verifica del sistema e viene svolta in condizioni operative predeterminate prima del rilascio del sistema stesso alla routine operativa. Il suo scopo è determinare – attraverso evidenze oggettive – che il sistema risulta conforme agli obiettivi per cui è stato pensato. Deve includere la verifica dei vari sotto- sistemi in scenari di stress operativo effettivi o simulati.

L'ampiezza della Validazione viene determinata in fase di risk assessment dove vengono evidenziati i rischi specifici associati alla particolare situazione contingente in cui andrà ad operare il sistema. Va inclusa la validazione del software – cioè la dimostrazione oggettiva che i sistemi di autorizzazione, di trasmissione, di generazione allarmi, di riconoscimento di scenari ecc. funzionino come previsto.

La Validazione conferma che tutti i sotto-sistemi e il sistema finale integrato siano sicuri (safe) ed efficaci, rispondano ai requisiti di garanzia della security garantendo che il "giusto sistema" sia messo in opera.

La validazione del sistema deve comprendere la validazione del software di gestione della centralina di allarme al fine di garantire la ripetibilità degli eventi nelle differenti casistiche di innesco e la verifica delle strategie di autorizzazione al trattamento dei dati stessi generati dal sistema.

5.4 Modifiche alla progettazione

Ogni modifica alla progettazione del sistema, dovuta a sopravvenuta obsolescenza o a incapacità di rispondere adeguatamente a nuovi scenari di rischio o all'emergere di nuovi scenari dalla connessione al lavoro dell'intelligence, deve seguire una procedura documentata.

Nella procedura va specificato come l'organizzazione intende operare per garantire che le modifiche al disegno del sistema siano documentate e validate o – dove appropriato – verificate nuovamente. Le modifiche devono essere anche riviste e approvate nuovamente prima della loro implementazione.

Simulazioni periodiche dovrebbero essere tenute per stressare il sistema in diversi scenari di minaccia per capire eventuali carenze e agire di conseguenza, con le opportune modifiche alla progettazione, per evitare reazioni indesiderate o di scarsa efficacia.

5.5 Specifiche per i Security Services

Questo argomento viene sviluppato come capitolo a sè stante in quanto il servizio di security inteso come monitoraggio del sistema fino alla capacità di intervento armato prevede di condividere l'intero approccio alla sicurezza e le informazioni sensibili relative con il fornitore.

Pertanto se con tutti gli altri soggetti fornitori dei differenti servizi può essere applicato il mitigatore di rischio rappresentato dalla condivisione di informazioni parziali e attinenti alla sola area coperta direttamente e a semplici dati di segnalazione a livello di interfaccia con i soli sotto- sistemi direttamente in comunicazione con quello oggetto della specifica fornitura, per la "Security" vera e propria questo non è possibile.

È quindi necessario definire un processo documentato di selezione dei fornitori.

Il processo deve documentare i requisiti e le modalità per assicurare la capacità dei fornitori di fornire i servizi di security all'interno del sistema tecnico e procedurale come disegnato a livello progettuale, la sua coerente documentazione, la dimostrazione della conformità a tutti i requisiti prestazionali, normativi e legislativi previsti.

Il processo deve specificare almeno le regole per:

- Certificazioni specifiche del fornitore;
- Certificazioni specifiche del personale;
- Policy del personale;
- Training specifico;
- Turn over;
- Conoscenza di sistemi informatici;
- Protocolli di intervento;
- Protocolli di monitoraggio;
- Gestione della riservatezza delle informazioni e dei dati trattati.

5.6 Requisiti di gestione dei fornitori

La progettazione di dettaglio dei sottosistemi viene effettuata dai fornitori specializzati.

Per garantire che la qualità dei sottosistemi sia coerente con gli obiettivi di security dell'intero sistema è necessario che le specifiche funzionali, risultato del disegno dei sottosistemi, siano affiancate da un processo documentato di selezione dei fornitori.

Il processo deve documentare i requisiti e le modalità per assicurare la capacità dei fornitori di fornire i componenti del sottosistema, la sua coerente progettazione e documentazione, la dimostrazione della conformità dello stesso a tutti i requisiti prestazionali, normativi e legislativi previsti.

Il processo deve specificare le regole per:

- La ricerca e la valutazione dei fornitori;
- La definizione delle guide architetturali per innescare la progettazione di dettaglio dei sotto-sistemi;
- Il processo di gestione degli ordini;
- Le modalità di accettazione e controllo dei prodotti forniti;
- Il trattamento dei dati e delle informazioni scambiate.

5.6.1 Requisiti estesi

Comunicazione, valutazione, formazione, e miglioramento sono componenti chiave per estendere la sicurezza della catena logistica a partire dai fornitori.

A seconda dei casi va previsto il disegno appropriato di procedure per incoraggiare la negoziazione con partner / fornitori / appaltatori per valutare e migliorare, laddove necessario, la loro sicurezza nella catena logistica.

È opportuno prevedere accordi di sicurezza con i partner commerciali / fornitori / appaltatori dove includere richiesta scritta di elementi quali:

- Sigilli anti contraffazione a prova di manomissione o firme;
- Controlli orari;
- Mezzi di comunicazione concordati;
- La presa in considerazione di offrire incentivi ai partner / fornitori / appaltatori che assicurano una maggiore sicurezza attraverso il coordinamento e la cooperazione;

- La documentazione delle politiche di sicurezza della catena di fornitura reciproca;
- Il più ampio scambio di informazioni tra di loro: trading partner / fornitori / appaltatori;
- Istruzione, formazione e consapevolezza da parte dei partner commerciali su sicurezza della catena logistica.

5.7 Requisiti infrastrutturali generali

Per una impostazione generale degli aspetti di sicurezza a livello di edificio valgono le seguenti considerazioni di massima:

CCTV

Sebbene non sia raccomandabile come sotto-sistema indipendente (stand- alone system), l'aggiunta di sistemi di sicurezza video nel perimetro dell'edificio, può portare diversi benefici. Principalmente viene generato un effetto deterrente verso potenziali ladri che avrebbero una prima informazione di effettivi investimenti per la sicurezza in atto, inoltre l'effetto di salvaguardia si estenderebbe anche ad altri rischi (danni da vandalismo).

Dispositivi di bloccaggio e controllo delle chiavi

Finestre interne ed esterne, porte, portoni e recinti, devono essere fissati in modo sicuro con gli appropriati dispositivi di bloccaggio. I sistemi di controllo degli accessi sono ideali laddove sia necessario poter modificare i codici con facilità. Dove invece l'analisi dei rischi non ne postula l'effettiva necessità, semplici lucchetti di sicurezza e una buona procedura di controllo delle chiavi possono considerarsi sufficienti contro i furti, gli atti vandalici e gli accessi non autorizzati in genere.

Illuminazione

Un'adeguata illuminazione – sia interna che all'esterno della struttura – è un requisito chiave per la sicurezza. Tutti gli ingressi, le uscite, le zone di carico/scarico merce, le aree di stoccaggio, le linee di recinzione, e le aree di parcheggio dovrebbero essere ben illuminate.

Aree di parcheggio e punti di accesso

Le zone di spedizione dai parcheggi dello staff e dei visitatori devono essere separate per eliminare la possibilità di rapidi furti.

Visita delle strutture

Rappresentanti della Direzione al più alto livello possibile dovrebbero fare frequenti visite non programmate alle zone di magazzino per verificare i processi giornalieri. Questo tipo di attività è provato essere un efficace metodo di monitoraggio: imprevedibilità è il concetto chiave.

Accessi limitati

Si deve cercare di limitare gli accessi alle zone di magazzino attraverso un solo ingresso principale per tutti i membri dello staff, i visitatori e gli ospiti.

6. SOTTO-SISTEMI E SERVIZI TECNICI

Questo capitolo illustra i diversi sottosistemi e i servizi tecnici che alimentano la garanzia di sicurezza in un disegno architetturale bidimensionale (deterrenza/reazione).

Per ogni classe di sottosistemi o servizi sono evidenziati gli aspetti principali da considerare quando si affronta un intervento riguardante la messa in opera o l'implementazione di un sistema di sicurezza.

Questo capitolo vuole porre gli elementi minimi di riflessione per un team incaricato di valutare le necessità e gli impatti legati all'implementazione di tali sistemi e servizi tecnici nella propria particolare realtà.

Nella logica multidisciplinare della presente guida ogni sotto-sistema tecnico va visto nella sua complessità specifica con un approccio integrato agli elementi che lo compongono.

6.1 Misure fisiche

Le contromisure ai furti che si possono definire di tipo fisico comprendono le seguenti classi:

Protezione dei punti di ingresso

Porte standard, sia esterne o interne, possono essere facilmente forzate. Investire in porte in acciaio di sicurezza che forniscono ulteriori livelli di protezione con i vari sistemi di chiusura, a prova di urto e trapano.

Messa in sicurezza dei Punti di Consegna

I punti di consegna della merce e le finestre sono punti vulnerabili ai potenziali furti a causa della mancanza di sicurezza e dell'utilizzo di materiali poco robusti. Grate di sicurezza in acciaio costituiscono un ulteriore e versatile livello di protezione altamente raccomandato.

Messa in sicurezza delle scorte

Proteggere il magazzino all'interno è altrettanto importante. Le gabbie di sicurezza aumentano la protezione sia come custodie singole che co-

struite in moduli raccordati tra loro. Inoltre, le camere di sicurezza possono proteggere da furto e incendio e consentire misure aggiuntive come la ventilazione controllata.

6.1.1 Protezione del perimetro esterno

Il sotto-sistema del perimetro esterno è la prima linea di difesa. Un buon presidio dello stesso consente spesso di avere una forte azione di prevenzione degli eventi avversi in quanto può dare l'idea di quanto complesso, sofisticato e "voluto" sia il sistema di sicurezza.

La presenza di telecamere che coprono il perimetro, il presidio di guardiania degli ingressi, i sensori perimetrali di intrusione, la tipologia di cancelli, le recinzioni utilizzate sono gli elementi tecnici di questo sotto-sistema.

Costruzione del profilo di performance

Di seguito vengono forniti i criteri indicativi per valutare e pesare i diversi elementi tecnici del sotto-sistema di telesorveglianza.

- Il "grado di integrazione" con gli altri elementi del sotto-sistema o del sistema complessivo (es. TVCC dedicato, integrato locale interno, integrato globale interno, integrato locale visibile da stazione di intervento esterna, integrato globale visibile da stazione di intervento esterna);
- Il "grado di performance" rispetto allo stato della tecnica in quel momento (es. TVCC – telecamera "fake", telecamera bassa risoluzione, telecamera alta risoluzione, telecamera con visione notturna, motion control, riconoscimento dei volti).

Estratto della Check list di valutazione della dimensione (su scala Lockpill)

La valutazione secondo la scala Lockpill della dimensione base "sistemi video" è decomposta in diversi elementi di indagine. La seguente check list – estratta dal tool di valutazione della sicurezza della FO basato sulla scala Lockpill – ne illustra alcuni:

• È presente un sistema di video sorveglianza?	Si/No
• La video sorveglianza è attiva 24h?	Si/No
• È presente un sistema di registrazione dei filmati delle telecamere?	Si/No
• La durata di registrazione prima della sovrascrittura è di almeno 7 giorni?	Si/No
• Il sistema di registrazione è a nastro?	Si/No
• Il sistema di registrazione copre tutte le telecamere attive?	%
• Le telecamere esterne inquadrano tutti gli accessi principali alla FO?	%
• Le telecamere esterne inquadrano tutte le pareti con finestre della FO?	%
• I filmati sono visionati in tempo reale?	Si/No
• Le telecamere sono dotate di sistemi di rilievo del movimento?	Si/No
• Le telecamere esterne sono dotate di illuminatori a infrarossi per la visione notturna?	Si/No

Esempi tecnici:

Dal punto di vista della tecnologia bisogna tenere conto dello stato dell'arte al momento della valutazione fissandolo come fondo scala e giudicando quanto rilevato come relativo in termini di assegnazione del punteggio.

In questo momento un prodotto professionale di punta – a cui assegnare il massimo punteggio in fase di valutazione – potrebbe essere quello riportato in Allegato 2: Specifiche telecamera professionale top level, mentre il valore minimo più prossimo allo 0 (assenza di telecamere) potrebbe essere assegnato a un prodotto come quello descritto di seguito:

Contenitore metallico (alluminio anodizzato) che riproduce l'aspetto di una vera telecamera CCTV/IP Aspetto professionale, riproduce fedelmente una telecamera Supporto metallico a parete snodabile e regolabile Dotata di LED lampeggiante per simulare la piena operatività.

6.1.2 Perimetro interno

Il sotto-sistema del perimetro interno è la prima linea di difesa laddove non esistono barriere di recinto. Un buon presidio della stessa consente spesso di avere una forte azione di prevenzione degli eventi avversi in quanto può dare l'idea di quanto complesso, sofisticato e "voluto" sia il sistema di sicurezza.

La presenza visibile di telecamere che coprono gli ingressi e i punti finestrati del perimetro, il presidio di guardiania degli ingressi, la tipologia di cancelli, le protezioni delle finestre, la sensoristica anti-intrusione sono gli elementi tecnici di questo sotto- sistema.

Costruzione del profilo di performance

Di seguito viene fornito un esempio per determinare i criteri indicativi per valutare e pesare i diversi elementi tecnici centrato sulla protezione delle finestre:

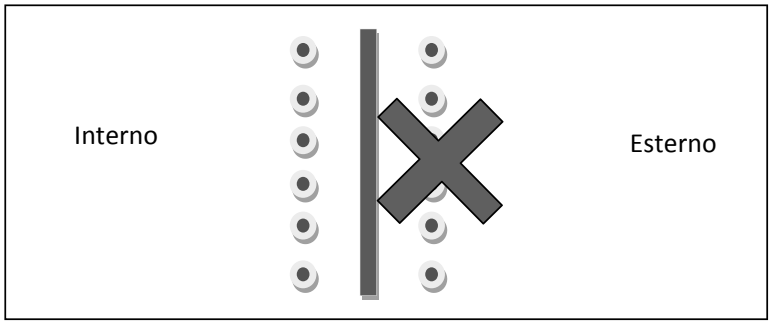
- Il "grado di integrazione" con gli altri elementi del sotto-sistema o del sistema complessivo (es. grate esterne non allarmate, grate interne non allarmate, grate interne allarmate, grate esterne allarmate, grate esterne allarmate localmente, grate esterne allarmate collegate alla centralina generale di allarme);
- Il "grado di performance" rispetto allo stato della tecnica in quel momento (es. grata esterna avvitata, grata esterna murata, grata esterna murata in acciaio anti taglio, grata esterna murata in acciaio anti-taglio con sensore di vibrazione, grata esterna murata in acciaio anti-taglio con sensore di vibrazione e di apertura).

Le grate di protezione hanno cinque fattori di valutazione:

- Tipo di materiale;
- Spessore delle sbarre;
- Sistema di fissaggio;
- Posizionamento rispetto alla finestra;
- Connessione al sistema di allarme.

Un prodotto che potrebbe essere considerato il riferimento per l'assegnazione del massimo punteggio avrebbe le seguenti caratteristiche:

- Classe 6 di sicurezza (dato da materiale usato, spessore delle sbarre e sistema di fissaggio);
- Posizionamento all'interno della finestra;
- Collegamento al sistema di allarme attraverso sensore sismico.



Esempio di posizionamento corretto della grata antintrusione

Nota:

I test antintrusione vengono eseguiti sulla base delle norme Uni En 1628, 1629 e 1630, e servono a determinare la resistenza al carico statico, dinamico e manuale.

Le prove evidenziano le carenze progettuali, anche nei particolari che possono inficiare la sicurezza di tutta la struttura, come il diametro delle viti o le saldature imperfette. E simulano l'attacco di un malintenzionato, secondo particolari strategie e con un preciso set di strumenti da scasso a disposizione». Attrezzature e tempo di effrazione definiscono il livello di resistenza.

In breve, la classe 1 (livello più basso) è efficace contro chi utilizza solo la forza fisica per aprire la porta. La classe 2 è invece in grado di resistere a tentativi di scasso con attrezzi semplici (cacciavite, tenaglie, ecc.). Per la classe 3, il test prevede anche l'uso di un piede di porco e simili. Mentre la classe 4 è adatta a respingere uno scassinatore esperto, che può servirsi anche di seghe, accette, scalpelli e trapani portatili a batteria. Si aggiungono poi attrezzi elettrici più sofisticati come le seghe a sciabola (classe 5) e ad alta potenza (classe 6). In base alla classe, sono richiesti tempi netti massimi di attacco da 3 a 20 minuti, mentre i tempi totali – che includono l'osservazione, la preparazione degli attrezzi, il cambio punte – vanno da 15 a 50 minuti.

6.1.3 Rilievo di presenza

Il sotto-sistema di rilievo di presenza è pensato come seconda linea di difesa laddove i sotto-sistemi di deterrenza periferica si siano rivelati non sufficienti a fermare l'azione criminosa. Qui l'azione non è più volta alla deterrenza ma è già parte della dimensione di reazione del sistema di sicurezza.

Sono componenti tipici del sotto-sistema i sensori volumetrici, i sensori di pressione, i sensori acustici, le gabbie di sicurezza, le porte interne di sicurezza, le stanze di sicurezza.

Questa componentistica è accomunata dal fatto che la sua azione si applica quando i malintenzionati si trovano già all'interno della struttura del sito.

Costruzione del profilo di performance

Di seguito viene fornito un esempio per determinare i criteri indicativi per valutare e pesare i diversi elementi tecnici centrato sui sensori volumetrici:

- Il "grado di integrazione" con gli altri elementi del sotto-sistema o del sistema complessivo (es. sensori in posizione casuale e non completa, sensori in posizione di copertura completa delle zone a rischio, sensori collegati ad allarme locale, sensori collegati ad allarme generale, sensori collegati ad allarme generale con visibilità della loro mappa e rilievo immediato dello specifico sensore in allarme);

- Il "grado di performance" rispetto allo stato della tecnica in quel momento (es. sensore singola tecnologia, sensore doppia tecnologia, sensore doppia tecnologia non oscurabile, sensore tripla tecnologia, sensore tripla tecnologia non oscurabile).

In questo momento un prodotto professionale di punta – a cui assegnare il massimo punteggio in fase di valutazione – potrebbe essere quello riportato in Allegato 3: Specifiche sensore volumetrico professionale top level, mentre il valore minimo più prossimo allo 0 (assenza di sensori) potrebbe essere assegnato a un prodotto come quello descritto di seguito:

Sensore infrarosso passivo con chiusura ad incastro senza l'utilizzo di viti.

- Portata 15 m. Lente volumetrica di 100°;
- Piroelettrico doppio elemento;
- Filtro disturbi elettromagnetici;
- Tamper antiapertura e protezione anti strisciamento.

6.1.4 Nebbiogeni

In generale, sia il gas irritante che i nebbiogeni (il principio in fondo è lo stesso) sono dei validi complementi ad un sistema antintrusione. Si tratta di sistemi attivi che agiscono come effettivi anti-furto.

Se l'intrusione è rapida, infatti, e il malvivente pensa di avere comunque abbastanza tempo per arraffare qualcosa, l'uso di un deterrente tipo nebbiogeno o gas irritante costituisce un ottimo aiuto ad evitare che il danno vada oltre lo scasso.

La normativa europea, EN 50131 – 8, regola e determina le modalità installative e le caratteristiche obbligatorie dei sistemi nebbiogeni, il D.L. n° 103 del 12 Maggio 2011, pubblicato su G.U. n° 157 dell'8 Luglio 2011, in attuazione dell'art. 3, comma 32, della Legge n° 94/2009 con-

sente l'utilizzo dei gas irritanti basati sulla OC = Oleoresin Capsicum (con una concentrazione pari al 10%).

All'estero sono gli enti assicurativi e le organizzazioni omologhe del CEI ad imporre l'utilizzo del nebbiogeno, non solo esplicitando come e dove impiegarlo, ma anche richiedendo che i prodotti siano certificati secondo la norma europea EN50131-8.

Costruzione del profilo di performance

Di seguito vengono forniti i criteri indicativi per valutare e pesare i diversi elementi tecnici di un sotto-sistema nebbiogeno:

- Il "grado di integrazione" con gli altri elementi del sotto-sistema o del sistema complessivo (es. impianto dedicato al solo locale farmaci, impianto dislocato su uno o più percorsi di aggressione critici, integrazione con allarme locale, integrazione con allarme globale, integrazione con sistemi cloud di visione remota);
- Il "grado di performance" rispetto allo stato della tecnica in quel momento (es. copertura fino al 10% della zona critica, copertura fino al 30% della zona critica, copertura fino al 50% della zona critica, copertura fino al 70% della zona critica, copertura fino al 100% della zona critica).

6.2 Sistema di controllo degli accessi

Il sotto-sistema degli strumenti di gestione del controllo degli accessi ha lo scopo di regolare chi può accedere in un determinato ambiente.

Il termine Controllo Accessi infatti va a definire una architettura sia fisica che elettronica che possa impedire l'ingresso di persone, mezzi o cose all'interno di aree protette se non autorizzate. Nel contempo deve garantire comunque l'accesso a coloro i quali siano regolarmente autorizzati.

I principali strumenti di controllo degli accessi sono le chiusure con chiave, le chiusure elettroniche e le chiusure con sistemi di riconoscimento biometrico (impronte digitali, scansione retinica, riconoscimento facciale) attraverso cui il sistema esegue l'identificazione dei soggetti e delle loro credenziali (tra cui password, numeri di identificazione personale (PIN), scansioni biometriche, e tasti fisici o elettronici).

Il controllo di accesso è fondamentale per identificare la persona che fa un lavoro specifico, autenticarne le credenziali di accesso dando poi a quella persona solamente la possibilità di accedere al locale o allo strumento di cui necessita inibendo il resto. Va da sé che a livello progettuale questo aspetto non possa essere disgiunto dalla profonda conoscenza delle procedure operative aziendali che vanno a definire i compiti delle persone e quindi la necessità delle stesse di accedere a determinati locali. Deve essere sempre presente la necessità di un compromesso tra le esigenze di sicurezza e la velocità di passaggio e autenticazione dei soggetti nelle varie aree onde evitare rischi di bypass del sistema.

I controlli degli accessi possono essere installati a differenti livelli e in diversi luoghi del sito come uffici, ripostigli, magazzino ma anche mense, ristoranti e altre aree pubbliche del sito per fornire livelli supplementare di protezione.

Costruzione del profilo di performance

Di seguito vengono forniti i criteri indicativi per valutare e pesare i diversi elementi tecnici centrato sulle serrature:

- Il "grado di integrazione" con gli altri elementi del sotto-sistema o del sistema complessivo (es. serrature elettroniche locali, serrature elettroniche diffuse, serrature elettroniche locali con registrazione log off-line, serrature elettroniche diffuse con registrazione log off-line, serrature elettroniche con attivazione diretta dell'allarme on-line);
- Il "grado di performance" rispetto allo stato della tecnica in quel momento (es. porta di sicurezza con serratura molto basica, serrature del tipo calettato blocco catenaccio, serratura a cifrario che consente l'accesso solo se si conosce il codice per aprire la porta. Token elettronici in genere consistono di un badge che può essere sia strisciato per l'accesso, o possono invece contenere un tag di identificazione a radiofrequenza (RFID) che contiene le informazioni per identificare l'individuo che necessita di accedere ai locali. Infine serrature a comando biometrico attivate da sensori di impronte, lettori di retina o telecamere a riconoscimento facciale).

Il livello minimo è rappresentato dalla chiave unica duplicata senza una lista di persone autorizzate a detenerne la copia, il massimo livello po-

trebbe essere rappresentato da lettori biometrici come quelli evidenziati in Allegato 4: Specifiche sistema di controllo accessi a lettura della retina professionale top level.

6.2.1 Serrature elettroniche

L'utilizzo di serrature elettroniche consente di disporre dei log di accesso della chiave elettronica. Questo permette agli addetti al monitoraggio e controllo di accedere ai percorsi dei singoli e all'identificazione immediata di chi era in un determinato luogo in un determinato momento (sono tracciabili dati tipo: nome, azienda, numero di telefono, tempo all'interno, e il tempo all'esterno). La stessa cosa può essere fatta con gli ospiti esterni e i dati possono completare quanto registrato da un eventuale sistema di video sorveglianza.

Per la messa in opera di un sotto-sistema di controllo degli accessi si utilizzano principalmente tre modelli:

- Controllo di accesso discrezionale o DAC: Il proprietario di un particolare o una risorsa è il principale responsabile della concessione ad altri utenti di tale accesso.
- Controllo di accesso obbligatorio MAC: Questo sistema non consente ai proprietari di avere il privilegio di decidere a chi sarà consentito l'accesso. Tutti gli utenti e le risorse sono classificati e assegnatari di una etichetta di sicurezza che garantisce loro i relativi diritti di accesso. Queste etichette di sicurezza determinano la politica di sicurezza e consente al soggetto di accedere all'oggetto previsto senza ulteriori azioni da parte sua.
- Tecnologia di controllo degli accessi basato sul ruolo o RBAC: Questa è la tecnologia più utilizzata nel mondo delle imprese. In questo modello, l'accesso concesso a una risorsa è strettamente basata sul ruolo che il soggetto detiene nell'organizzazione. La maggior parte delle persone sono assegnatarie di un certo numero di privilegi in accordo con i loro ruoli.

6.2.2 Sistemi biometrici

I sistemi di controllo degli accessi basati sulla biometria vengono attivati attraverso strumenti tecnici che consentono analisi di impronta digitale, geometria della mano, configurazione del viso, caratteristiche dell'iride o della voce.

Questo consente di riconoscere e identificare una persona attraverso una particolare caratteristica fisica, biologica o comportamentale. Tale caratteristica, confrontata con i dati immagazzinati all'interno del sistema che costituisce il lettore biometrico, permette il riconoscimento e, quindi, l'autorizzazione per quella data persona, all'accesso ad aree riservate o a informazioni memorizzate su particolari strumentazioni, siano essi computer o altro.

Quando si decide di utilizzare questo particolare sotto-sistema tecnico all'interno del progetto, deve essere messo in evidenza come il prodotto che verrà poi installato in fase di messa in opera del sistema sia stato sviluppato per essere utilizzato esclusivamente in ambito lavorativo e non rappresenti una violazione alla privacy. Per questo deve essere specificato che il sotto-sistema tecnico sia realizzato in modo da attenersi strettamente alle direttive del Garante della Privacy e allo Statuto dei Lavoratori venga previsto che le informazioni riportate siano utilizzate solo ed esclusivamente per l'ambito lavorativo. Più in particolare, il database che elabora i dati per il riconoscimento e quindi autorizza l'accesso non deve essere nominativo, ma permettere solo il rilievo di corrispondenza tra l'elemento biologico analizzato e la presenza di tale dato all'interno del database delle persone autorizzate all'accesso. Il sotto-sistema tecnico deve essere stato progettato per assicurare che nessun dato o immagine personale venga riportato all'interno del database, garantendo così di non violare la privacy di quanti fanno uso dei sistemi biometrici di accesso.

Al momento, grazie al consolidarsi della tecnologia, la biometria ha raggiunto un alto livello di efficienza mettendo in evidenza i seguenti vantaggi principali per il suo utilizzo diffuso a livello di garanzia della sicurezza:

- I tratti biometrici (di qualsiasi tipo) non posso essere dimenticati o persi;
- I tratti biometrici non possono essere rubati;
- I tratti biometrici non possono essere passati ad altri individui.

Solo a riconoscimento avvenuto i dispositivi di accesso collegati (tornelli, porte di accesso, portoni, serrature elettroniche ecc.) si aprono altrimenti rimangono bloccati impedendo l'ingresso.

Fondamentalmente si passa da utilizzare ai fini del controllo di accesso qualcosa che CONTRADDISTINGUE l'utente (dati biometrici) invece di qualcosa che l'utente POSSIEDE (chiave, badge) o che CONOSCE (password). Nel secondo e terzo caso infatti non si riconosce l'utente stesso ma lo strumento utilizzato che diventa oggetto di furto diretto o indiretto (pishing).

Naturalmente al momento dell'installazione di questo strumento ogni dipendente deve sottoporsi ad uno scanner relativo al tipo di riconoscimento che si è scelto di utilizzare, digitalizzando e archiviando così i suoi dati. Da quesl momento il sistema potrà riconoscere quella determinata persona.

Le principali tecnologie biometriche oggi diffuse sul mercato sono:

- Impronta digitale;
- Geometria della mano;
- Lettura iride o retina;
- Geometria del volto.

La soluzione ad oggi più diffusa è il riconoscimento attraverso le impronte digitali. Per evitare che un dipendente rimanga bloccato a causa di ferite, fasciature o gessi solitamente si digitalizzano almeno due dita. è inoltre possibile digitalizzare un terzo dito da tenere come allarme in caso di minaccia. In questo ultimo caso un messaggio di allerta viene così inviato ai preposti in modo che possano intervenire rapidamente.

La geometria della mano si basa sul riconoscimento di elementi come la grandezza della mano, la lunghezza delle dita, le curvature specifiche.

Si considerano poche caratteristiche ma si tratta di uno strumento piuttosto preciso.

Il riconoscimento attraverso l'iride o la retina funziona tramite una fotocamera che scansiona l'occhio attraverso un fascio di luce a raggi infrarossi. I macchinari di ultima generazione sono in grado di scansionare anche gli occhi con lenti a contatto o con occhiali. Sono inoltre in grado di capire la differenza tra un occhio vivo e uno morto.

La geometria del volto riconosce parametri come i lati della bocca, gli zigomi, il profilo degli occhi, la posizione del naso.

Al momento gli algoritmi di riconoscimento facciale presentano problematiche relative alle condizioni di luminosità ambientale, alla posa del soggetto (orientamento della testa), alle espressioni facciali, alle occlusioni (o auto occlusioni – make up) e all'età. Per questo motivo si stanno mettendo a punto nuovi sistemi in tecnologia 3D e altri che riescano prendere in considerazione anche i flussi sanguigni interni.

6.3 Sistemi intelligenti

Con "sistemi intelligenti" si intendono tutte quelle nuove applicazioni software che utilizzano le telecamere come sensore complesso non solo come terminali per informare i decisori e registrare gli avvenimenti, ma come agenti attivi del sistema di garanzia per la sicurezza.

Il sotto-sistema intelligente più basico è il riconoscimento di movimento. In questo caso il software rileva il movimento nella zona coperta dalla telecamera e – oltre alle immagini – manda una segnalazione di preallarme alla sorveglianza e/o a una eventuale serie di soggetti preposti a ricevere detta segnalazione per ulteriori decisioni.

Il sotto-sistema di riconoscimento facciale si integra a livelli differenti infatti può essere un valido sostituto di un sistema di controllo degli accessi specialmente in zone poco presidiate dal personale. Se il sistema di telecamere copre correttamente tutta la zona a rischio col modello "a inseguimento" (cioè quando si esce dalla zona coperta da una telecamera il soggetto sotto controllo entra nella zona coperta dalla telecamera successiva senza soluzione di continuità) è possibile attuare opportune tattiche di intercetto da parte della sorveglianza.

Il sotto-sistema di riconoscimento delle situazioni – apparso recentemente come applicazione di tecniche machine-learning – lavora integrando diverse reti di sensori per rilevare e – auto apprendendo nel tempo – anticipare gli eventi criminali.

Costruzione del profilo di performance

Di seguito vengono forniti i criteri indicativi per valutare e pesare i diversi elementi tecnici centrato sul rilievo di movimento:

- Il "grado di integrazione" con gli altri elementi del sotto-sistema o del sistema complessivo (es. applicato alle telecamere degli ingressi visibile solo dal personale interno, applicato a tutte le telecamere visibile solo dal personale interno, applicato alle telecamere degli ingressi visibile da stazione di intervento esterna, applicato a tutte le telecamere visibile da stazione di intervento esterna);
- Il "grado di performance" rispetto allo stato della tecnica in quel momento (es. telecamera bassa risoluzione, telecamera alta risoluzione, telecamera con visione notturna, linea di trasmissione a bassa velocità, linea di trasmissione ad alta velocità).

6.4 Controllo delle consegne

Il controllo dei percorsi di consegna è un sotto-sistema procedurale che ha lo scopo di ridurre la variabilità degli scenari di attacco.

Il disegno procedurale degli assetti di sicurezza nel trasporto fornisce una protezione contro l'introduzione non autorizzata di personale e materiale nella catena di fornitura, coprendo le aree di discontinuità della catena di fornitura.

A seconda dei casi il sotto-sistema procedurale di controllo comprenderà uno o più dei seguenti aspetti:

- La definizione di routine di controllo periodico di tutte le aree di parcheggio, di stoccaggio, di carico e di transito facilmente accessibili;
- Il controllo del fissaggio di scomparti interni / esterni e pannelli;
- La regolazione degli interventi per i casi di segnalazione in cui vengano scoperti personale non autorizzato, materiale non previsto o non conforme, o segni di manomissione di un mezzo di trasporto;
- L'utilizzo di veicoli che possano essere bloccati o comunque assicurati quando merci ad alto valore o ad alto rischio devono essere trasportati a una distanza notevole dal punto di scarico;
- L'utilizzo di blocchi a prova di manomissione, sigilli non contraffabili o sigilli elettronici sui mezzi di trasporto;
- Se rispetta i criteri interni di costo-efficacia, l'utilizzo di transponder per facilitare un continuo monitoraggio dei mezzi di trasporto.

6.5 Sistema di allarme

Il sotto-sistema dell'allarme è uno strumento di supporto all'operatore per la gestione di situazioni anomale ed ha principalmente le seguenti due funzioni:

La funzione primaria è avvisare l'operatore di una situazione che non è normale

Il sistema dovrebbe informare l'operatore sulle condizioni anomale del sito che richiedono una valutazione tempestiva – eventualmente seguita da opportune azioni correttive, – al fine di mantenere gli obiettivi del sito in termini di sicurezza, produttività, ambiente ed efficienza.

Ogni allarme deve avvisare, informare e guidare l'operatore. L'allarme dovrebbe:

- Essere rilevante per il ruolo dell'operatore al momento;
- Indicare quale azione è richiesta;
- Presentarsi con una frequenza che l'operatore sia in grado di affrontare;
- Essere facilmente e immediatamente comprensibile.

La funzione secondaria del sistema di allarme è l'evento di registro

La funzione di registro (log) supporta la necessità dell'operatore di analizzare gli eventi che hanno portato alle condizioni di processo attuali o precedenti.

Il registro di allarme deve essere utilizzato per:

- Analisi di incidenti;
- Ottimizzazione del funzionamento dell'impianto.

Il registro di allarme dovrebbe essere flessibile e contenere anche eventi, allarmi soppressi e altri pezzi di informazione non presentati nella lista di allarme principale, ma che potrebbero essere utili per ulteriori indagini sugli incidenti.

Le informazioni del registro di allarme dovrebbero essere utilizzate anche per il monitoraggio e il miglioramento delle prestazioni del sistema di allarme.

Il sistema di allarme deve fornire informazioni e funzionalità utili per supportare le attività dell'operatore.

Le informazioni devono essere presentate e gestite in modo che siano compatibili con le limitazioni e capacità umane, così che il sistema sia utilizzabile per l'operatore in tutte le situazioni.

In aggiunta al sistema di allarme, diverse altre fonti di informazione possono essere importanti nella gestione di situazioni anomale, come le tendenze, la video sorveglianza, i quadri di visualizzazione panoramica per la valutazione rapida della situazione, le simulazioni di processo e i sistemi di supporto avanzati agli operatori per il monitoraggio delle condizioni, la diagnosi, o le procedure informatizzate.

6.5.1 Allarme silenzioso

Allarme che non emette alcun segnale acustico (tutto rimane silenzioso, sia all'interno che all'esterno). La centrale di emergenza viene informata con discrezione, quando l'obiettivo è cogliere i malviventi in flagranza di reato (cioè evitare che il ladro fugga, che l'aggressore sia provocato, ecc.).

6.5.2 Allarme acustico

In generale è buona norma installare almeno una sirena all'esterno. Serve sia come prodotto deterrente per informare l'eventuale malintenzionato che il sito è protetto da un sistema di allarme, sia nel caso scatti l'allarme per attirare l'attenzione di reparti vicini e passanti e quindi mettere in fuga il ladro.

All'interno dei locali del sito invece si può aggiungere una sirena per l'interno.

La sirena all'interno ha sempre lo stesso scopo, ossia di mettere in fuga il ladro ed allertare i reparti vicini.

Le sirene disponibili sono sia di tipo wireless (senza fili) che cablate (via filo) e la maggior parte di esse resiste agli agenti atmosferici.

Possono essere anti-manomissione (anti-schiuma) ed essere dotate di batterie tampone per funzionare anche con l'interruzione dell'alimentazione.

6.5.3 Allarme luminoso

I dispositivi luminosi di allarme trovano collocamento in impianti d'allarme dove è richiesta grande visibilità.

Buone dimensioni del segnalatore e l'impiego di lampade allo xeno con elevato rendimento ottico, garantiscono un'ottima segnalazione.

I diversi colori della calotta (rosso – giallo – arancio – verde – blu – bianco) permettono di soddisfare le varie esigenze di progettazione dell'impianto.

I segnalatori per lampade stroboscopiche sono forniti con un circuito elettronico basato su microprocessore che fornisce la cadenza di lampeggio e su un condensatore che pilota la lampada.

Gli allarmi luminosi sono molto utili sia come immediato deterrente all'azione criminosa – specie nelle ore notturne – che nel presidio di zone non immediatamente visibili e non presidiate continuamente da servizi di sorveglianza tipo ronde ecc.

6.5.4 Centralina

Il componente primario dell'impianto antifurto è la centralina d'allarme, attraverso cui si attiva, disattiva e si gestisce l'intero sistema. La centrale, nel momento in cui scatta l'allarme, determina quali azioni intraprendere, gli attuatori da attivare e la loro durata.

Esistono svariate tipologie di centrali, che si differenziano tra loro per il numero di zone gestibili, ma anche per le funzionalità possedute, come ad esempio l'interfaccia wireless o il combinatore GSM integrato. All'interno la centralina spesso ha installato anche il combinatore telefonico GSM integrato con l'apposito alloggio della scheda SIM per inviare messaggi di allarme ai numeri pre-selezionati dall'utente. In alcuni modelli il combinatore o commutatore può essere collegato in seguito.

Per comunicare con i vari componenti, le migliori centraline wireless utilizzano una doppia frequenza di trasmissione su due bande radio: la 434 e la 868 MHz. Nel caso una delle due frequenze venga sabotata o intercettata l'altra frequenza garantirebbe comunque la comunicazione.

Comandi della centralina

Sulla centralina generalmente si trova la tastiera stessa, tramite la quale è possibile interagire per attivare e disattivare le varie funzioni, inserendo una password personale per attivare o disattivare l'allarme; stessa funzione tramite chiavi elettroniche e telecomando.

Diversi modelli di centraline di ultima generazione possiedono anche il controllo biometrico tramite impronte digitali o carta RFID.

La suddivisione in zone

Ogni centrale di allarme permette solitamente di impostare e configurare diverse "zone", ovvero di suddividere il sistema in diverse aree con possibilità di gestirle in modo indipendente l'una dall'altra. A ciascuna zona possono essere associati uno o più sensori, a seconda di come viene configurato l'impianto. Questa suddivisione è molto importante per due principali motivi:

- La possibilità di attivare l'impianto di allarme solo in determinate aree del sito, escludendone altre. Ad esempio può essere utile, attivare il sistema di allarme in modo completo (esterno e interno) durante le ore notturne, mentre durante l'orario di lavoro del sito ha più senso attivare l'impianto antifurto solamente per le zone perimetrali (esterno o porte e finestre).
- La possibilità di rilevare con precisione eventuali intrusioni distinguendole dai falsi allarmi, se la centralina rileva un allarme in una zona esterna potrebbe anche trattarsi di un errore, ma se l'allarme viene rilevato anche all'interno del sito l'intrusione potrebbe essere certa.

Anche la scelta delle zone risulta quindi estremamente importante, deve essere infatti effettuata non solamente in base alla struttura dell'abitazione, ma anche in base al traffico delle persone che vi lavorano, i visitatori, i pazienti.

Controllo a distanza della centrale antifurto

La tecnologia in materia di sicurezza ha fatto enormi passi avanti negli ultimi anni, con le più moderne centrali di allarme è infatti possibile ve-

rificare e gestire l'impianto antifurto anche in remoto, da un computer collegato ad internet o direttamente tramite il cellulare, con le dovute precauzioni.

Alcune centrali infatti sono corredate da specifici software, sviluppati direttamente dal produttore, per il controllo remoto delle stesse mediante gli smartphone di ultima generazione (iPhone, Android, ecc.).

Sono considerati praticamente degli standard i normali collegamenti LAN, WiFi, combinatore telefonico, ponte radio.

Protezione della centralina

La centralina dovrebbe essere posta in un locale ad accesso controllato o almeno nei locali più interni della Farmacia Ospedaliera dove l'accesso sia limitato al minor numero di persone possibile.

La centralina dovrebbe essere posta in posizione protetta da urti accidentali e sotto gruppo di continuità – meglio se dedicato. Laddove l'accesso controllato non potesse essere garantito, va previsto un armadio di sicurezza o almeno una gabbia di sicurezza entrambi dotati di adeguate serrature.

Costruzione del profilo di performance

Di seguito vengono forniti i criteri indicativi per valutare e pesare l'impatto della scelta del tipo di centralina sull'intero sistema.

- Il "grado di integrazione" con gli altri elementi del sotto-sistema o del sistema complessivo (es. integrazione dei sotto-sistemi con interfaccia dedicata, integrazione dei sotto-sistemi plug&play, integrazione parziale con i sistemi di comunicazione, integrazione totale con i sistemi di comunicazione);
- Il "grado di performance" rispetto allo stato della tecnica in quel momento (es. livello di protezione del sistema di accesso ai comandi, numero di zone, numero di sistemi collegabili, tecnologie di collegamento disponibili, grado di interfacciabilità con sistemi di analisi e controllo dei dati di allarme).

6.5.5 Documentazione del sistema di allarme

Il sistema di allarme deve essere adeguatamente documentato, e devono essere stabiliti chiari ruoli e responsabilità per il mantenimento e il miglioramento del sistema nel tempo.

La documentazione dovrebbe assicurare che siano stabilite buone prassi e che queste siano sostenute in tutte le modifiche del sistema, che i progettisti e gli utenti del sistema abbiano una comprensione comune delle funzionalità del sistema. Si deve anche assicurare che ogni allarme definito nel sistema venga documentato con una descrizione dello scopo dell'allarme e una valutazione di criticità. La definizione di ruoli e responsabilità chiare dovrebbe assicurare che siano stabilite responsabilità per tutti i problemi e compiti relativi al sistema di allarme durante la sua vita operativa.

Oltre alla filosofia di allarme descritta sopra, dovrebbe essere documentato anche:

- La strategia di progettazione allarme: sulla base della filosofia di allarme, questa dovrebbe essere una metodologia strutturata per lo sviluppo del sistema di allarme che assicuri che ogni allarme è giustificato, correttamente progettato e documentato. Le questioni importanti sono: coinvolgimento dell'utente, individuazione delle esigenze degli utenti, obiettivi di performance, una guida per subappaltatori sulla progettazione degli allarmi, dizionario dei termini e delle abbreviazioni da utilizzare nei messaggi di allarme.

- La strategia di gestione degli allarmi del sito: descrive l'assegnazione di ruoli e responsabilità per il mantenimento e la gestione del sistema di allarme, nonché le procedure per la revisione, la manutenzione, il monitoraggio delle prestazioni del sistema, le prove, la modifica e la documentazione.

- Gli allarmi individuali: il sistema deve essere auto-documentante e fornire informazioni dettagliate su ogni allarme (lo scopo dell'allarme, così come le informazioni di configurazione sui criteri di soppressione, ecc.).

6.6 Gestione del personale

Il sotto-sistema procedurale di gestione del personale mira a garantire la piena consapevolezza dello stesso in materia di sicurezza. Questa logica va estesa anche al personale esternalizzato come vedremo in seguito nei paragrafi dedicati.

Devono essere messe in opera procedure che coprano i seguenti aspetti:

- Gestione delle assunzioni: avere regole per cercare di assumere le persone giuste. Assicurarsi di prendere rigorose misure di valutazione del personale durante il processo di reclutamento e controllare accuratamente le referenze, il background di esperienza, la presenza di precedenti penali.
- Formazione sulla sicurezza: assistere i dipendenti con le pratiche per mantenere l'integrità della merce in carico, addestrare le persone a riconoscere la potenziale minaccia e come agire di conseguenza, formarle sulle regole di protezione per il controllo degli accessi.
- Controlli di sicurezza e del background: definire le regole per controllare i nuovi dipendenti e periodicamente tutti gli altri. Definire le modalità per assicurare che i dipendenti siano presenti nelle aree protette solo se sono necessari per lo svolgimento delle loro funzioni.
- Visitatori: devono essere regolati i processi per la registrazione e il rilascio di account per tutti i dipendenti di società in appalto. Va considerata la richiesta di identità con foto a scopo di documentazione.
- Confidenzialità: vanno messe in atto regole precise – meglio se parte dei contratti di assunzione e di appalto – per evitare la fuga di informazioni sensibili sulla sicurezza attraverso il canale dei social media.

6.6.1 Training e consapevolezza della sicurezza

L'istruzione, formazione e sensibilizzazione del personale per quanto riguarda le politiche di sicurezza, è volta a favorire il diffondersi di una cultura della vigilanza per le deviazioni da quelle politiche e sapendo le azioni da intraprendere in risposta a carenze nella sicurezza.

A seconda dei casi è utile procedere con le seguenti azioni:

- Comunicare le politiche di sicurezza e gli standard per i dipendenti, tra cui conseguenze inadempienza.
- Richiedere la partecipazione di tutto il personale in programmi di sensibilizzazione e di formazione di sicurezza.
- Promuovere il riconoscimento per la partecipazione dei dipendenti attivi in controlli di sicurezza.
- Promuovere una politica di incentivazione per gli individui o dipendenti che segnalano attività sospette.
- Utilizzare i comunicati stampa, le liste di distribuzione e-mail e bacheche per diffondere la cultura della sicurezza a tutti i livelli

6.6.2 Formazione sull'allarme

Gli operatori devono ricevere istruzioni e formazione sistematica in merito a tutte le condizioni operative realistiche di utilizzo del sistema di allarme.

L'obiettivo di tale formazione è quello di garantire che l'utilizzo e la funzionalità del sistema di allarme siano familiari e ben comprese dagli operatori.

La formazione di base sul sistema di allarme dovrebbe comprendere:

- Le regole di prioritizzazione;
- I meccanismi di soppressione;
- L'interfaccia utente del sistema di allarme;
- Le procedure di accettazione dell'allarme.

Utilizzare il sistema di allarme in condizioni limite di processo sarà tipicamente molto diverso da utilizzarlo durante il normale funzionamento delle operazioni. Deve quindi essere fornita una formazione periodica e realistica, come la simulazione della gestione di tutti i tipi di disturbi per garantire che gli operatori saranno in grado di utilizzare il sistema di allarme nelle situazioni critiche, quando di fatto è maggiormente necessario.

Affinché l'eliminazione dell'allarme sia efficace, gli operatori devono poter acquisire esperienza pratica e sviluppare fiducia nelle strategie di eliminazione in uso nel sistema.

6.6.3 La minaccia dei Social media

I social media sono piattaforme eccezionali per tenersi in contatto con amici e parenti in tutto il mondo. Le statistiche Portal rilevano che ne 2016 c'erano 2,13 miliardi di utenti di social network in tutto il mondo, e nel 2012 erano 1,4 miliardi.

La condivisione di aspetti quotidiani della vita su siti come Facebook, Twitter e Instagram è diventato un evento troppo frequente. Che si tratti di check-in su Facebook, eventi su Twitter, o scatti della famiglia e amici su Instagram sembra come se la popolazione non possa resistere dal mettere in mostra le loro vite. Tuttavia, questo comportamento sta diventando un problema enorme perché gli individui non riescono ancora a comprendere i rischi connessi con la libera condivisione di queste informazioni.

Esempi dalla cronaca ci parlano di effrazioni in un'abitazione della città "X" dopo un tweet dove il proprietario "condivideva" la notizia che avrebbe trascorso la sua giornata nella città "Y" a qualche ora di aereo di distanza. Questo a conferma della tesi che vede i social media come uno strumento di intelligence per i criminali.

Il problema della condivisione di informazioni di fatto sensibili presenta due dimensioni:

- Le persone non percepiscono la facilità di utilizzo di queste informazioni.
- Non sono comprese le opzioni di sicurezza disponibili.

Una rapida ricerca e i ladri possono accedere a informazioni sensibili condivise con leggerezza. Informazioni sugli allarmi, sulle presenze, sulle turnazioni, sulla presenza o meno di prodotti, su prodotti in arrivo, su scioperi sia del personale interno che esterno, sulla organizzazione, foto dei locali, foto del sito che possano far capire eventuali scoperture di sicurezza come interruzioni dei recinti, non presenza di telecamere o finestrature non protette ecc. sono dati intercettabili dai criminali che possono emergere da normali colloqui on line tra persone che operano nella Farmacia Ospedaliera e familiari, amici, colleghi ecc.

Condivisione di fotografie

Ogni foto che si carica on-line è piena di informazioni preziose tipo: quando e dove è stata scattata, che tipo di macchina fotografica o smart-

phone è stato utilizzato ecc. I meta-dati contenuti in file di immagini possono rivelare molto. Per esempio molti telefoni cellulari con fotocamera come iPhone includono automaticamente i dati delle immagini posizione GPS. Purtroppo, questa informazione può essere facilmente utilizzata per monitorare la posizione specifica di un utente.

Vanno sensibilizzate le persone affinché si avvalgano della possibilità – data dagli stessi strumenti social – di rimuovere queste informazioni dalle immagini.

Si deve evitare di rivelare informazioni come i nomi delle strade, informazioni personali, e punti di riferimento che possono essere ripresi all'interno delle foto.

Uno scenario tipico potrebbe essere l'esempio in cui venisse postata una foto della vacanza su Twitter, e poi si distribuisse – attraverso la condivisione tipica dei social – su altre piattaforme, come un blog, Pinterest e Instagram.

In questo caso criminali esperti potrebbero scaricare la foto ed eseguire una ricerca di immagini inversa che li condurrebbe a tutte le conversazioni/condivisioni su queste piattaforme multiple dalle quali potrebbero essere estratte informazioni dannose per la sicurezza (esempio: sapere che diverse persone sono in ferie potrebbe far ipotizzare ai criminali scenari favorevoli al furto dati da una probabile minore sorveglianza).

I Social Media aumentano la vulnerabilità

I modi in cui si usano i social media possono incrementare gli scenari di vulnerabilità.

Le seguenti pratiche tecniche e comportamentali devono essere messe in atto per ridurre al minimo l'impatto dei social:

- Gestione Impostazioni – Questo è il punto principale di difesa. Mantenere le informazioni trattate sugli strumenti social visualizzabili al minimo in modo che nessuno al di fuori del vostro gruppo di fiducia di amici e familiari possano usufruire dei suoi dati.

- Gestione Foto – Le fotografie potrebbero confermare il fatto che la persona non è in ufficio (vacanza o missione di audit presso un fornitore o un'altra sede) in ufficio. Ci si deve assicurare di migliorare le impostazioni di sicurezza, compresa la disabilitazione del location

tracking e considerare la modifica delle abitudini di utilizzo dello strumento social sia in casa che in ufficio.

- Indirizzo – Evitare di visualizzare l'indirizzo dei vari ingressi al sito ovunque sui social media: è una delle informazioni più sensibili per i criminali.

6.7 Sicurezza della documentazione

Il sistema di controllo della sicurezza della documentazione, sia elettronica e manuale, è il sotto-sistema procedurale con il compito di assicurare che l'informazione sia leggibile e che il sistema di sicurezza venga protetto contro la perdita di dati o l'introduzione di informazioni errate.

A seconda dei casi deve essere valutata l'opportunità di mettere in opera le seguenti procedure:

- Salvaguardia dell'accesso del computer e informazioni.
- Controllo dell'accesso ai sistemi informativi, sia per livello di responsabilità che di ruolo, e del livello di sensibilità informazioni.
- Garanzia di sicurezza fisica nelle zone del computer.
- Monitoraggio dell'utilizzo da parte dei dipendenti dei sistemi di dati.
- Gestione dei processi di backup dei dati.
- Registrazione della quantità di unità, le condizioni di imballaggio, il sigillo di sicurezza.
- Richiesta di firma per tutti i punti di controllo di processo (ad esempio, preparazione di documenti, apposizione sigilli, ispezione del vettore, controllo della merce entrante, controllo dei documenti di ricezione).
- Procedure di controllo speciali per preparare le spedizioni di emergenza / dell'ultimo minuto e, se necessario, informare le autorità per quanto riguarda tali spedizioni.
- Registrazione del tempo di ingresso e di uscita delle persone che ricevono e consegnano le merci.
- Documentazione dei ritardi significativi di processo.

7. GESTIONE DELLE ATTIVITÀ ESTERNALIZZATE (OUTSOURCED ACTIVITIES)

Cosa è l'outsourcing?

Nell'accezione più semplice, l'outsourcing (o esternalizzazione) è la delega di una funzione aziendale a un fornitore esterno. Questa operazione postula il trasferimento di persone, processi e risorse. L'esternalizzazione può essere condotta sia applicandola a processi che rimangono interni al sito che a trasferimenti all'esterno del sito; può essere affidata a un solo partner (single-sourced) o a più partner o più partner (multi-sourced).

L'esternalizzazione è un processo maturo nel settore dell'Information Technology (ICT Outsourcing) ma si sta sviluppando a includere una vasta gamma di processi di business (Business Process Outsourcing), quali risorse umane, Finanza, Acquisti, Customer Service, e la più ampia funzione di back office.

Il fattore chiave per l'attività di outsourcing è la riduzione dei costi. Tuttavia, ci sono altri driver che è importante considerare:

- Velocità di sviluppo: nel caso di una nuova entità di business – interna o esterna – essere in grado di utilizzare l'outsourcing per mettere in atto le funzioni chiave è molto più rapido ed economico che sviluppare delle capacità in-house da zero.
- Flessibilità: con l'outsourcing è possibile fornire la flessibilità necessaria per fare fronte a una rapida crescita – o un calo – della domanda di un certo servizio o prodotto
- Competenze specialistiche: in aree specialistiche quali IT, attrarre, sviluppare e trattenere personale qualificato può essere una vera sfida (i fornitori di outsourcing possono offrire l'accesso a queste competenze tendenzialmente scarse quando serve).

Ridurre i rischi per la sicurezza legati all'outsourcing

Con la prospettiva di gestire la sicurezza anche in caso di processi esternalizzati si deve ragionare su due principali direttrici di intervento: a livello preventivo si segue la logica dei pre- assessment e si attuano opportune dinamiche di costruzione contrattuale; a livello del monitoraggio e della correzione si agisce con gli strumenti dell'auditing periodico e attuando politiche di condivisione dei dati dei flussi di azione correttiva e preventiva.

Il processo di esternalizzazione non porterà i vantaggi desiderati se non si adotta un approccio strutturato. Tendenzialmente qualunque metodo sia seguito, si dovrebbero attraversare le seguenti fasi:

- Definire un piano adeguato per gestire e conservare il giusto livello di controllo / direzione nel rapporto di outsourcing.
- Stabilire e gestire un processo di governance efficace.
- Gestire efficacemente i rischi commerciali, legali e finanziari di outsourcing.
- Gestire efficacemente eventuali fasi di transizione e trasformazione (che rappresentano il rischio maggiore di fallimento dell'operazione).

Va stabilito un piano per la sicurezza assieme all'appaltatore che evidenzi i mezzi, gli strumenti, le persone, il training, le informazioni, le responsabilità da mettere in atto e riprendere nel contratto tra le parti.

Il processo di gestione della sicurezza all'interno di un'operazione di esternalizzazione si divide sostanzialmente nei seguenti momenti principali:

- Attività preliminari o pre-contrattuali;
- Valutazione dei rischi per la sicurezza;
- Specificazione dei requisiti di sicurezza;
- Valutazione delle competenze in materia di sicurezza dell'appaltatore;
- Esecuzione del contratto di esternalizzazione;
- Stabilire le obbligazioni tra le parti;
- Valutare continuamente la performance dell'appaltatore;
- Attività post-contrattuali;
- Requisiti per la sicurezza da attuare in fase post-contrattuale.

7.1 Azioni pre-contrattuali

Prima di procedere con il contratto vero e proprio va prevista un'azione incisiva sulla valutazione dei rischi connessi alla specifica attività da esternalizzare. Questa valutazione è parte delle attività del progetto complessivo per la sicurezza laddove l'esternalizzazione sia già definita. È un processo a sé stante laddove il progetto complessivo per la sicurezza sia attivo da tempo e pertanto deve armonizzarsi allo stesso in modo da evitare duplicazioni e inefficienze.

La prima azione riguarda la valutazione dei rischi. Il committente dovrebbe salvaguardarsi in termini di rischi sicurezza come:

- Accessi non autorizzati alle proprie strutture;
- Accessi non autorizzati alle strutture informatiche e alle informazioni sensibili nel caso di servizi che richiedano la connessione ai propri sistemi;
- Introduzione di software dannoso (virus, worm, trojan, trapdoors);
- Furti di identità;
- Attacchi informatici dai sistemi del service provider;
- Processi o procedure operative inadeguate.

Per la valutazione del rischio vanno presi in considerazione fattori come: lo scopo dell'esternalizzazione, tipologie e livelli di accesso necessari all'appaltatore, durata, forza della protezione offerta dai controlli residenti e l'impatto potenziale sull'organizzazione del committente.

I risultati derivanti dalla valutazione dei rischi aiuteranno il committente per:

- Determinare il livello di rischio e decidere se sia accettabile per l'organizzazione.
- Accertare l'adeguatezza e l'efficacia della sicurezza e i controlli procedurali e decidere se siano necessari controlli aggiuntivi.

Quando i rischi per la sicurezza sono alti, la decisione aziendale di esternalizzare dovrebbe essere riconsiderata. L'outsourcing non deve avvenire quando i rischi per la sicurezza individuati non possono essere efficacemente ridotti o quando i controlli di sicurezza necessari non sono adeguati. Quando possibile, controlli tecnici o procedurali supplementari dovrebbero essere messi in atto per ridurre i rischi per la sicurezza individuati portandoli a un livello accettabile.

Specificare i requisiti per la sicurezza

Quando la decisione di esternalizzare è presa, il committente deve procedere a elencare tutti i requisiti per la sicurezza del servizio. Questi vanno commisurati ai bisogni di confidenzialità, integrità e disponibilità del servizio.

Le aree di rischio da considerare nell'elenco sono:

- Requisiti di sicurezza correlati al livello di servizio;
- Requisiti per il personale;
- Ruoli e responsabilità per la sicurezza;
- Trattamento e accesso alle informazioni;
- Requisiti di training e consapevolezza;
- Requisiti di controllo degli accessi;
- Requisiti e gestione delle responsabilità;
- Requisiti di sicurezza della rete;
- Requisiti di sicurezza delle operazioni;
- Requisiti di auditing e monitoraggio;
- Requisiti di gestione degli incidenti;
- Requisiti di gestione della continuità operativa.

Il committente deve inoltre procedere alla valutazione delle competenze dell'appaltatore per la sicurezza nelle seguenti aree:

- Requisiti di training e consapevolezza;
- Esperienza e competenze tecniche;
- Efficacia delle misure per la sicurezza;
- Compliance alla policy, agli standard e alle procedure del committente per la sicurezza;
- Policy, agli standard e procedure dell'appaltatore per la sicurezza.

7.2 Esecuzione del contratto

Secondo quanto esposto dalle normative europee di riferimento per il farmaco (EudraLex The Rules Governing Medicinal Products in the European Union – Volume 4 – EU Guidelines for Good Manufacturing Practice for Medicinal Products for Human and Veterinary Use – Chapter 7 Outsourced Activities), va scritto un capitolo dedicato – nel contratto – riguardante gli aspetti di security richiesti dal committente, le modalità di attuazione e i mezzi in carico all'appaltatore e le modalità di controllo e le frequenze di auditing del committente.

Citando la supply chain infatti, la normativa di fatto incorpora la security come elemento da regolare all'interno del contratto di outsourcing nei

termini e con le responsabilità previste in logica più generale di gestione della qualità.

Nel contratto devono essere stabilite le obbligazioni nelle seguenti aree:

- Obbligazioni contrattuali;
- Responsabilità;
- Diritto di auditing del committente;
- Obbligazioni nella gestione post-contrattuale.

Il committente deve mettere in atto l'organizzazione necessaria per verificare continuamente per tutta la durata del servizio esternalizzato quanto definito nel contratto.

Di seguito si riporta come, nel caso di processi in outsourcing, la legislazione europea di attuazione delle GMP (Good manufacturing Practices) regoli la fattispecie:

> *"Any activity covered by the GMP Guide that is outsourced should be appropriately defined, agreed and controlled in order to avoid misunderstandings which could result in a product or operation of unsatisfactory quality. There must be a written Contract between the Contract Giver and the Contract Acceptor which clearly establishes the duties of each party".*

E continua più profondamente definendo gli obblighi delle parti e gli elementi base dei contratti:

• Committente

> *"The pharmaceutical quality system of the Contract Giver should include the control and review of any outsourced activities. The Contract Giver is ultimately responsible to ensure processes are in place to assure the control of outsourced activities".*

• Appaltatore

> *"The Contract Acceptor must be able to carry out satisfactorily the work ordered by the Contract Giver such as having adequate premises, equipment, knowledge, experience, and competent personnel. The Contract Acceptor should not subcontract to a third party any of the work entrusted to him under the Contract without the Contract Giver's prior evaluation and approval of the arrangements".*

• Contratto

"The Contract should describe clearly who undertakes each step of the outsourced activity, e.g. knowledge management, technology transfer, supply chain, subcontracting, quality and purchasing of materials, testing and releasing materials, undertaking production and quality controls (including in- process controls, sampling and analysis)".

7.3 Auditing

Deve essere previsto un piano di audit dei processi/servizi esternalizzati al fine di garantire che siano attuate tutte le misure per la sicurezza definite a livello di contratto.

Apposite check list di controllo devono essere sviluppate per garantire che vengano coperti tutti i punti necessari.

Gli audit vanno pianificati e la loro esecuzione programmata con l'appaltatore in modo da avere tutto il personale necessario disponibile sul luogo in quel momento. L'audit deve essere visto in logica di collaborazione e buona fede tra le parti come strumento per far funzionare le cose e cercare di capire se ci sono malinterpretazioni che possano – nella prosecuzione delle attività – creare problemi o interruzioni della security a tutti i livelli.

Di seguito si riporta come, nel caso di processi in outsourcing, la legislazione europea di attuazione delle GMP (Good manufacturing Practices) regoli la fattispecie:

• Committente

"The Contract Giver should monitor and review the performance of the Contract Acceptor and the identification and implementation of any needed improvement. The Contract Giver should be responsible for reviewing and assessing the records and the results related to the outsourced activities".

• Appaltatore

"The Contract Acceptor should understand that outsourced activities, including contract analysis, may be subject to inspection by the competent authorities".

• Contratto

"The Contract should permit the Contract Giver to audit outsourced activities, performed by the Contract Acceptor or his mutually agreed subcontractors".

7.4 Azioni post-contrattuali

Alla chiusura del contratto il committente dovrebbe assicurarsi di coprire le seguenti aree per garantirsi da problemi di "sicurezza residua":

- Revoca di eventuali account utente e diritti di accesso.
- Documentazione (tutta la documentazione, le informazioni, gli strumenti e gli asset del servizio esternalizzato dovrebbero essere distrutti o resi alla fine del servizio).
- Ritorno delle risorse IT e dei dati (laddove siano prestate risorse IT come il software, attrezzature e dati del committente queste devono essere restituiti. Se è previsto contrattualmente la distruzione di dati da parte dell'appaltatore, questi deve fornire adeguati rapporti o registri che consentano il controllo dell'avvenuta attività).
- Obbligazioni contrattuali (ci fosse la necessità da parte dell'appaltatore di seguire dei requisiti contrattuali dopo la fine del servizio, questo deve essere preventivamente notificato – ad esempio la confidenzialità di dati e informazioni).

7.5 Outsourcing: Elementi generali per la riduzione dei rischi per la sicurezza

Esempi di elementi da considerare per la riduzione dei rischi in un processo di esternalizzazione.

- Continuità del personale
  Spesso le competenze necessarie per la gestione del contratto possono essere diverse da quelle di chi ha condotto la negoziazione. Tipicamen-

te le imprese si organizzano con team il cui compito è quello di vincere il contratto, che viene poi sostituito da un team operativo una volta che il contratto ha inizio. E a volte la squadra delle operazioni non riesce a credere a quello che il team di offerta ha promesso!

- Interfaccia con l'appaltatore
  Valutare il giusto mix di strutture formali ed informali. Utilizzate in modo appropriato, si risolvono rapidamente i problemi rinforzando il rapporto. Considerare l'istituzione di un comitato di partenariato in modo che i dirigenti possono dare l'esempio e prendere decisioni collettivamente.

- Co-localizzazione
  Lavorare nello stesso luogo consente di stabilire buoni rapporti personali. Questo supporta una migliore comunicazione e consente scambi informali di messaggi e dati. Viene favorita la discussione faccia a faccia per risolvere i problemi insieme.

- Registrare gli obiettivi quando sono raggiunti
  Gestire gli obiettivi consente di comunicare i vantaggi ottenuti con il progetto a tutte le parti interessate. Va predisposto un piano degli obiettivi che mostri come e quando saranno raggiunti. Vanno poi monitorati e regolarmente comunicati agli stakeholder. È fondamentale che le parti interessate non dimentichino il motivo della scelta di ricorrere all'outsourcing.

- Controllare tutte le modifiche al contratto
  Ogni contratto ha bisogno di un processo di controllo delle modifiche chiaro e condiviso. È necessario capire il costo di ogni cambiamento su tutto il ciclo di vita del contratto. Tutte le modifiche devono essere registrate integralmente e concordate. Anche se tentati, evitare sempre di fare affidamento solo sulla fiducia.

- Mettere le persone giuste a gestire il contratto
  Un'adeguata gestione del contratto e delle relazioni richiede risorse qualificate. I contratti devono essere gestiti da persone dedicate. Le funzioni necessarie possono essere di natura finanziaria, tecnica, valu-

tazione del rischio, controllo delle prestazioni e gestione delle relazioni. La gestione di servizi critici non è sicuramente un'attività minore; se deve essere assegnata al chi gestiva il servizio in-house, questi deve essere opportunamente addestrato nella nuova situazione.

- Incentivare il contraente
  Vanno stabiliti chiari standard di prestazione. Meglio collegare i pagamenti alle prestazioni. Se fatto, va gestito correttamente: decidere se applicare le penali automaticamente o a discrezione; tenere sempre ben presente che la priorità è assicurarsi un buon servizio, non raccogliere risarcimenti o multe.

- Creare l'ambiente per una buona comunicazione
  Questo è spesso il principale fattore di buon funzionamento del rapporto. Permette di risolvere velocemente i problemi. Sostiene un clima di fiducia reciproca. Andrebbero fatti incontri regolari, e di persona. Va deciso chi comunica con chi e vanno programmate revisioni regolari per tutta la durata del contratto.

- Cultura, atteggiamento e comportamenti
  Ci sono sempre alcune tensioni tra le diverse prospettive del cliente e dell'appaltatore. Il primo è lì per mantenere bassi i costi. Il secondo è lì per fare soldi. Ma le imprese non possono far crescere il business senza clienti felici. Va cercato un terreno comune su costruire la reciproca soddisfazione. È fondamentale l'esperienza di lavorare insieme sulla soluzione dei problemi per costruire la fiducia, l'ingrediente essenziale per il successo a lungo termine.

- Gestire il rapporto, non solo gli aspetti formali del contratto
  Un contratto ben elaborato offre una 'rete di sicurezza' legale, ma si tratta dell'ultima spiaggia che alla fine porta costi a tutte le parti. La vera chiave è nella relazione che si è riusciti a costruire e il primo obiettivo dei professionisti coinvolti deve essere la gestione efficace delle relazioni quando l'eccellenza del servizio e il rapporto qualità-prezzo devono essere assicurati alle nostre istituzioni.

8. INTELLIGENCE

L'Intelligence deve essere considerata un processo integrato nel sistema di gestione per la sicurezza.

Gli scenari di minaccia devono essere considerati come input al processo di progettazione e deve essere messo in opera un processo per aggiornare l'organizzazione sull'evoluzione degli stessi.

Continui contatti con gli Enti competenti e monitoraggio attivo degli eventi interni e delle notizie dell'ambiente di riferimento dovrebbero essere parti integranti di detto processo.

Ci sono tre diverse dinamiche per la definizione degli scenari di minaccia:

- La prima è il rilievo generale degli accadimenti sul territorio da parte delle Autorità competenti (Carabinieri NAS) che individua tutte le modalità criminali che interessano la fattispecie in esame – furto di materiale alto valore/basso volume – e può informare sulla tipologia criminale statisticamente significativa nel determinato territorio
- La seconda è la segnalazione da parte degli enti sanitari, degli eventi di attacco subiti sia riusciti che tentati. Questo – in una logica di rete nazionale delle Farmacie Ospedaliere del SSN – fornisce informazioni sugli specifici scenari di attacco statisticamente attuati a livello nazionale.
- La terza è la proiezione ipotetica di scenari di minaccia riferiti alla specifica realtà operativa di una determinata Farmacia Ospedaliera durante la progettazione del sistema di gestione per la sicurezza nelle analisi della situazione specifica degli elementi caratterizzanti la stessa.

9. MIGLIORAMENTO

Lo scopo del sistema di gestione per la sicurezza della Farmacia Ospedaliera è dissuadere i criminali dal perpetrare l'illecito e, nel caso ciò dovesse comunque avvenire, garantire un pronto intervento coerente.

Il sistema però non può essere considerato statico e immutabile in quanto gli viene richiesto di rispondere a stimoli provenienti dall'ambiente esterno (realtà criminale) che è in continuo mutamento. Nuove tecnologie, nuovi strumenti, nuovi sistemi, diverse strategie di attacco si profilano ininterrottamente per cambiare i futuri scenari di minaccia.

Per questo motivo è di fondamentale importanza porre particolare attenzione al concetto di miglioramento del sistema – di cui si è già accennato nei concetti generali sul ciclo di Deming.

Quando si parla di miglioramento bisogna tenere presente due aspetti dello stesso che vanno a delineare differenti strategie di intervento e diverse complessità di attuazione:

- il miglioramento incrementale;
- la re-ingegnerizzazione del processo.

Il primo aspetto vede il monitoraggio dei processi come elemento fondamentale per l'innesco e prevede interventi continui da parte di tutto il personale per trovare soluzioni più efficienti per incrementare le prestazioni dei processi nei quali sono coinvolti.

Il limite di questa soluzione è rappresentato dal concetto di "capacità naturale del processo" cioè il limite prestazionale implicito – connaturato a ogni processo – che non è superabile senza uscire dalle logiche strategiche e progettuali con cui il determinato processo è stato concepito.

Il secondo aspetto – che nella letteratura specialistica anglosassone è definito come "dramatical improvement" – inizia quando si prende atto che il processo attuale non è più "capace" di ottenere i risultati attesi – e la soluzione diventa la sua cosiddetta re-ingegnerizzazione.

La sopravvenuta non capacità del processo può essere dovuta sia al raggiungimento del limite naturale dello stesso, sia alla sopravvenuta esigenza di far fronte a scenari totalmente differenti da quelli ipotizzati ed evidenti nella situazione presente.

La re-ingegnerizzazione del processo prevede di ripartire da zero su un "foglio di carta bianco" ripensando il processo a partire dalle nuove esigenze ridefinendo le strategie e operando scelte progettuali nuove.

Dal punto di vista operativo la differenza tra i due approcci risiede nella complessità degli interventi necessari. Nel caso del miglioramento continuo o continuativo si parte da una forte conoscenza del processo attuale e dei suoi obiettivi condivisa e trasferita a tutto il personale coinvolto dove ognuno possa vedere opportunità di miglioramento negli aspetti di sua stretta competenza.

Nel caso della re-ingegnerizzazione invece si richiede un approccio strutturato di tipo progettuale assimilabile al lavoro svolto in fase iniziale di disegno del sistema di gestione per la sicurezza, dedicato al processo in esame. Un approccio di questo tipo è aperto al punto non solo di mettere in discussione il processo attuale, ma anche di rivedere tutti gli aspetti connessi del sistema volti a garantire la prestazione voluta. Il risultato è spesso una modificazione del sistema fino alle radici dello stesso.

Il concetto di miglioramento si fonde con le dinamiche di gestione delle modifiche al sistema e va loro connesso proceduralmente al fine di definire lo standard interno che renda l'azione operativa il più veloce ed efficace possibile.

10. GESTIONE DELLE MODIFICHE AL SISTEMA

Con Change Management si intende un approccio strutturato a cambiamenti significativi delle situazioni in essere.

Il ricorso al processo di Change Management può avvenire in risposta ad un problema, per eventi esterni (ad es. per cambiamenti legislativi), proattivo per il raggiungimento di nuovi livelli di efficienza ed efficacia, da programmi per il miglioramento dei servizi.

Obiettivo del Change Management è assicurare che metodi e procedure standard vengano utilizzati per una efficiente e pronta gestione di tutti i cambiamenti operativi e infrastrutturali, al fine di minimizzare l'impatto e gli incidenti in capo ai servizi erogati.

Al processo di Change Management deve essere data una buona visibilità e all'interno dell'ente vanno aperti tutti i canali di comunicazione necessari, che possano favorire una transizione fluida alla nuova situazione.

Il processo di Change Management deve essere documentato e tendenzialmente deve coprire i seguenti aspetti:

- Valutazione preliminare dell'attitudine al cambiamento dell'organizzazione (per impostare le migliori strategie di comunicazione e anticipare gli ostacoli il più possibile);
- Pianificazione della comunicazione (ad esempio le comunicazioni iniziali sono in genere progettate per creare consapevolezza intorno alle ragioni per il cambiamento e i rischi associati al non cambiare. Successivamente, ad ogni passo del processo, le comunicazioni devono essere disegnate per condividere i messaggi giusti al momento giusto);
- Sponsorship (chi è in carica per il progetto di Change Management deve sviluppare un piano per le attività dello sponsor di spinta del progetto);
- Training dei responsabili (il supporto dei manager e supervisori è fondamentale in quanto sono questi ad avere la reale influenza sulla motivazione a cambiare dei dipendenti);
- Sviluppo ed erogazione del training (la formazione delle persone sui nuovi aspetti tecnici e organizzativi deve avvenire solo dopo che

le stesse siano pienamente consapevoli della effettiva necessità di cambiare);

- Gestione delle resistenze (sponsor, manager e responsabili del cambiamento devono collaborare per vincere le normali resistenze dei dipendenti coinvolti);
- Coinvolgimento del personale (il processo deve essere a due vie e coinvolgere il personale per attuare le migliori soluzioni fa del cambiamento un'opera condivisa e non subita incrementando le possibilità di successo);
- Riconoscere il successo (comunicare l'ottenimento degli obiettivi rinforza la consapevolezza sull'opportunità effettiva del cambiamento);
- Revisione post-implementazione (si rivede tutto il programma, valutando successi e fallimenti, e identificando i cambiamenti di processo per il prossimo progetto. Questo rientra nel processo generale del miglioramento continuo della gestione).

11. MANUTENZIONE

La manutenzione è intesa come necessaria sia all'interno dei contratti di esternalizzazione, sia come elemento a sé stante laddove i componenti del sistema siano acquistati a scaffale ed entrino a far parte dei cespiti aziendali.

La scelta di avere le competenze di manutenzione internamente o esternamente alla struttura fanno parte dei piani di sviluppo strategico dell'Azienda e vanno prese come vincoli in ingresso alla progettazione del sistema quando si vanno a considerare i rischi nelle fasi iniziali di valutazione.

Lo scopo della manutenzione è la riduzione dei rischi di interruzione della copertura del sistema a causa di guasti e malfunzionamenti tecnici. Sia all'interno dei contratti di esternalizzazione che in un rapporto diretto, devono essere definiti precisi requisiti di disponibilità del servizio primario attraverso la definizione di opportuni SLA (Service Level Agreement) dove possano essere precisati indici e obiettivi numerici che possano essere misurati e monitorati nel tempo.

I rischi connessi alle attività legate alla manutenzione sono principalmente legati alle autorizzazioni necessarie al personale della manutenzione, che lasciano ampio margine di intervento sul sistema e vasta conoscenza della dislocazione dei sensori e delle strategie di difesa messe in atto in termini di sicurezza. Fughe di informazioni e sabotaggi tecnici possono essere alla base del successo delle azioni criminose.

Il personale tecnico della manutenzione deve essere preparato e addestrato in merito ai sistemi tecnici utilizzati dall'Azienda in modo da poter intervenire prontamente sia a livello preventivo che correttivo su qualsiasi delle parti.

Quando si affronta l'analisi dei rischi connessi alla manutenzione bisogna tenere presente che il rischio può essere definito come una funzione delle variabili "vulnerabilità" e "minaccia" (intesa come probabilità di guadagno – *funzione a sua volta delle variabili "motivazione", "opportunità" e "capacità" rispetto allo scenario di attacco*).

Qualsiasi intervento di manutenzione deve essere comunicato e approvato da una figura Responsabile opportunamente definita. Una procedura scritta di gestione delle autorizzazioni e la registrazione informatica o manuale di tutte le operazioni va prevista come parte del sistema di sicurezza.

12. BIBLIOGRAFIA E RIFERIMENTI SITOGRAFICI

1. Abus security tech germany - glossario sulla sicurezza. https://www.abus.com/it/Consigli- utili/Glossario-sulla- sicurezza/Impianti-di-allarme.
2. Adger N., Brooks N., Bentham G., Agnew M. & Eriksen S. 2004. New Indicators of Vulnerability and Adaptive Capacity, Tyndall Centre for Climate Change Research, Technical Report 7.
3. AEMI 2013, Organizational Resilience. Professional Development Program. AEMI, Mt Macedon.
4. Alberts C. and Dorofee A. "Managing Information Security Risks: The OCTAVE (SM) Approach", July 2002, Addison Wesley Professional.
5. Alexander D.E. 2013. Resilience and disaster risk reduction: an etymological journey, Natural Hazards and Earth Systems Sciences vol. 13, pp. 2707-16.
6. Alhazmi O., Malaiya Y. & Ray I. (2005). "Security Vulnerabilities in Software Systems: A Quantitative Perspective". Lecture Notes in Computer Science, Volume 3654/2005. (2005) Publisher: Springer-Verlag GmbH.
7. Altmann R. 2000. Understanding Organizational Climate: Start Minimizing Your Workforce Problems, Water Engineering & Management, vol. 147, no. 6, pp. 31-32.
8. *APEC Private Sector Supply Chain Security Guidelines.*
9. Arabaci I.B. 2010. Academic and Administration Personnel's Perceptions of Organizational Climate, Procedia – Social and Behavioral Sciences, vol. 2, pp. 4445-50.
10. Avizienis A., Laprie J.C., Randell B. and Landwehr C. (2004). "Basic Concepts and Taxonomy of Dependable and Secure Computing". IEEE Tr. On Dependable and Secure Computing, Jan–March 2004 (Vol 1, no. 1), pp 11–33.
11. BCI Continuity and Resilience (CORE) ISO 22301 presentation.
12. BertinoE. , BruschiD. , FranzoniS. , Nai Fovino I. and Valtolina S. "Threat modelling for SQL Servers". Eighth IFIP TC-6 TC-11 Conference on Communications and Multimedia Security (CMS 2004), September 2004, UK, pp. 189-201.

13. Bishop M. (2004). "Computer Security Art and Science" (November 2004) AddisonWesley.
14. Building resilient organisations – aligning individual and organisational 'bounce' – The Congruence framework.
15. Choudhury G. 2011. The Dynamics of Organization Climate: An Exploration, Management Insight, vol. 7, no. 2, pp. 111-16.
16. Ciampa M. (2009). *Security+ Guide to Network Security Fundamentals* Third Edition. Boston, MA.
17. CIPD (2011). "Developing Resilience: An evidence-based guide for practitioners", London, CIPD.
18. *CoBIT Audit Guidelines*, CoBIT IT Steering Committee and IT Governance InstituteTM, CoBIT 3rd Edition, Delivery and Support 2.0, July 2000, pg 130.
19. Code of Practice for Information Security Management. International Standard (ISO/IEC) 17799:2000.
20. Cole E. & Buckle P. 2004. Developing community resilience as a foundation for effective disaster recovery, Australian Journal of Emergency Management, vol. 19, no. 4, pp. 6-16.
21. Colwill C. & Gray A. (2006). Creating an Effective Security Risk Model for Outsourcing Decisions, BT Technology Journal 25(1).
22. Country Fire Authority 2013, CFA Strategy 2013-18: Towards Resilience, CFA, Melbourne.
23. Coutu D. L. (2002). "How resilience works". Harvard business review, 80 (5), pp. 46.
24. Coutu D.L. 2002. How Resilience Works, Harvard Business Review, vol. 80, no. 5, pp. 46-55.
25. Critical Infrastructure Protection, Challenges and Efforts to Secure Control Systems. United States Government Accountability Office, 2004. GAO-04- 628T.
26. CSARN Conference Building organizational resilience.
27. den Braber F., Dimitrakos T., Axel Gran B., Stølen K., Øyvind Aagedal J., "The CORAS methodology: Model-based risk management using UML and UP", in UML and the Unified Process. IRM Press, 2003.
28. Dondossola G., Szanto J., Masera M. and Nai Fovino I. "Evaluation of the effects of intentional threats to power substation control systems". International Journal of Critical Infrastructure, 2007.

29. DTI (2005). Technology Partnership Initiative News Issue 47, 10/05.
30. Dulaimi M.F., Nepal M.P. & Park M. 2005. A Hierarchical Structural Model of Assessing Innovation and Project Performance, Construction Management and Economics, vol. 23, no. 6, pp. 565-77.
31. EMV 2015, Victorian Emergency Strategic Action Plan 2015-18. Government of Victoria, Melbourne.
32. Enterprise Resilience – BS 65000 – Charley Newnham – BCI Forum June 2015.
33. Essential elements and domains of Organizational Resilience – BSI.
34. EudraLex, The Rules Governing Medicinal Products in the European Union - Volume 4 EU Guidelines for Good Manufacturing Practice for Medicinal Products for Human and Veterinary Use - Chapter 7: Outsourced Activities.
35. Everly G.S., Strouse D.A. & Everly G.S. 2010. The Secrets of Resilient Leadership: When Failure is Not an Option. Six Essential Skills for Leading through Adversity, DiaMedica, New York.
36. Fairbrother P., Mees B., Tyler M., Phillips R., Akama Y., Chaplin S., Toh K. & Cooper V. 2014. Effective Communication – Communities and Bushfire. Bushfire CRC, Melbourne.
37. GCHQ/CESG (ND) UK Government's Infosec Standard no. 1: Residual Risk Assessment Method (IS1).
38. Glaser B. G. & Strauss A. L. (1967). The discovery of grounded theory: strategies for qualitative research. New Brunswick: Aldine de Gruyter.
39. Gormley D.K. & Kennerly S. 2009. Influence of Work Role and Perceptions of Climate on Faculty Organizational Commitment, Journal of Professional Nursing, vol. 26, no. 2, pp. 108-15.
40. Guidance on organizational resilience - BSI Standards Publications.
41. *Guidance on the security and management of NHS assets* - May 2012.
42. Hamel G. & Valikangas L. 2003. The Quest for Resilience, Harvard Business Review, vol. 81, no. 9, pp. 52-63.
43. Holling C.S. 1973. Resilience and stability of ecological systems, Annual Review of Ecological Systems vol. 4, pp. 1-23.
44. IEEE Std 610.12-1990, IEEE Standard Glossary of Software Engineering Terminology.

45. Improving organisational resilience – The EPC approach.
46. *Information security management, Part 1: Code of practice (BS7799- 1:1999)*, sections 4.3.1 Security requirements in outsourcing contracts, British Standards Institute, 1999.
47. Information security management, Part 2: Specification for information security management systems (BS7799-2:1999), sections 4.2.2 – 4.2.3, British Standards Institute, 1999.
48. Isaken SG & Lauer KJ 2002, The Climate for Creativity and Change in Teams, Creativity and Innovation, vol. 11, no. 1, pp. 74-86.
49. [ISO 14971: 2012].
50. [ISO/IEG Guide 51: 1999].
51. Jones, A., Ashenden, D.(2005). "Risk Management for Computer Security : Protecting Your Network & Information Assets". Elsevier (March 2005).
52. Keeney M., Kowalski E., Cappelli D., Moore A. Shimeall T., Rogers S. . "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors". CMU, May 2005.
53. Knights M. (2006). Computer Weekly: "A More Sophisticated Approach", 11/7/06.
54. Kobayashi Hillary M. (2006). Computing: " Offshoring is Changing the focus of IT", 5/6/06.
55. Leigh J. (2004). Security News: "Managing outsourcing security risks", 18/11/04.
56. Lengnick-Hall C.A., Beck T.E. & Lengnick-Hall M.L. 2010. Developing a Capacity for Organizational Resilience through Strategic Human Resource Management, Human Resource Management Review, vol. 21, no. 3, pp. 243-55.
57. Management of Outsourced Activities and Purchased Materials: Addressing the Interfaces - Mary Oates, PhD Vice President, Global Quality Operations Pfizer.
58. Masera M. (2006). "Interdependencies and Security Assessment: a Dependability view". In proceeding of the IEEE Conference on Systems, Man and Cybernetics, October 8- 11 2006, Taipei.
59. Masera M. & Nai Fovino I. "Models for security assessment and management". In proceeding of the International Workshop on Complex Network and Infrastructure Protection, 2006.
60. Masera M. & Nai Fovino I. (2005). "A framework for the security

assessment of remote control applications of critical infrastructures", ESREDA 2005.
61. Masera M. & Nai Fovino I. (2006). "Modelling Information Assets for Security Risk Assessment in Industrial settings". 15th EICAR Annual Conference.
62. McDermott J. (2000). "Attack Net Penetration Testing". In The 2000 New Security Paradigms Workshop (Ballycotton, County Cork, Ireland, Sept. 2000), ACM SIGSAC, ACM Press, pp. 15-22.
63. McMurray A.J. 2003. The Relationship between Organizational Climate and Organizational Culture, Journal of the American Academy of Business, vol. 3, no. 1, pp. 1-8.
64. Mohyeldin A & Suliman T 2001, Are We Ready to Innovate? Work Climate-readiness to Innovate Relationship: The Case of Jordan, Creativity and Innovation Management, vol. 10, no. 1, pp. 49-59.
65. Morgan R. & Bravard J. L. (2006) Computer Weekly: "How globalisation alters your world", 8/8/06.
66. Nai Fovino I. (Global Cyber Security Center) - *Security Assessment of Critical Infrastructures, Definitions Methodology*.
67. Nai Fovino I. & Masera M. (2006). "Emergent Disservices in Interdependent Systems and System-ofSystems". In proceeding of the IEEE Conference on Systems, Man and Cybernetics, October 8-11 2006, Taipei.
68. Nai Fovino I. & Masera M. (2006). "Through the Description of Attacks: a multidimensional View". In proceeding of the 25th International Conference on Computer Safety, Reliability and Security 26-29 September 2006 Gdansk, Poland.
69. Nai Fovino I., Masera M. "InSAW-Industrial Security Assessment Workbench". In proceeding of the International Conference on Infrastructure Systems, Rotterdam, November 10-12, 2008.
70. Nai Fovino I., Masera M., Guidi L., Stefanini A. "Cyber Security Assessment of a Power Plant". International Journal of Electric Power System Research, Elsevier, 81 (2), pp. 518-526.
71. NISCC (2006). Good Practice Guide. Outsourcing: Security Governance Framework for IT Managed service Provision, 8/06.
72. Norman S., Luthans B. & Luthans K. 2005. The Proposed Contagion Effect of Hopeful Leaders on the Resilience of Employees and

Organizations, Journal of Leadership and Organizations Studies, vol. 12 no. 2, pp. 55-65.
73. Organisational resilience – Australian leadership survey – TLC.
74. Organisational resilience and emergency management – Bernard Mees, Adela McMurray, Prem Chhetri – Peer-reviewed Article.
75. Organisational Resilience: Concepts, Integration, and Practice – Ran Bhamra.
76. Outlaw.com (2006). The Register: "Outsourced data must be protected, says privacy chief", 12/7/06.
77. Pelling M., High C., Dearing J. & Smith D. 2008. Shadow Spaces for Social Learning: A Relational Understanding of Adaptive Capacity to Climate Change within Organizations, Environment and Planning, vol. 40, pp. 867-884.
78. Preserving order amid change and change amid order – organizational resilience risk advisory.
79. Ritter L., Barrett J. and Wilson R. 2006. *Securing Global Transportation Networks.* New York: McGraw-Hill.
80. Rolf J. E. & Glantz M. D. (1999). 'An Interview with Norman Garmezy'. Resilience and development: Positive life adaptations, pp. 5.
81. Schneider B., Ehrhart M.G. & Macey W.H. 2013. Organizational Climate and Culture, Annual Review of Psychology, vol. 64, pp. 361-88.
82. SES 2013, Building Community Resilience. Victoria State Emergency Service Annual Report 2012-13, Government of Victoria, Melbourne.
83. Sheffi Y. 2006. The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage, MIT Press, Cambridge, Mass.
84. Steffan J., Schumacher M. "Collaborative attack modeling". In proceeding of the Symposium on Applied Computing, Madrid, Spain (2002) pp. 253-259.
85. StoneburnerG. , GoguenA. , FeringaA. . "Risk Management Guide for Information Technology Systems". Special publication 800-3, National institute of Standards and Technology.
86. Sweet K. M. 2006. *Transportation and Cargo Security: Threats and Solutions.* Upper Saddle River, N.J.: Pearson/Prentice Hall.
87. Swiderski F. and Snyder W. "Threat Modeling", Microsoft Press 2004.

88. The value proposition for organizational resilience – Corporate cyber security summit – Ernst&Young – 13 novembre 2013.
89. Thibodeau P. (2005). Computerworld: "Firms in India seek better backgroundcheck system", 18/4/05.
90. Thomas D. (2004). Computing: Security must be key part to outsourcing, 18/11/04.
91. Todd et al (2006). Security Risk Management in the BTHP Alliance, BT Technology Journal 24(4).
92. Underwood G. (2006). Computer Weekly: "How the four Ps pay off", 28/2/06.
93. United Nations 2012, Resilient People, Resilient Planet: A Future Worth Choosing, Final Report of the United Nations Secretary-General's High-level Panel on Global Sustainability, UN, New York.
94. Vogus T.J. & Sutcliffe K.M. 2007. Organizational resilience: Towards a theory and research agenda. IEEE International Conference on Systems, Man and Cybernetics, 2007, New York, IEEE, pp. 3418-22.
95. Whitman Z.R., Kachali H., Roger D., Vargo J. & Seville E. 2013. Short-form Version of the Benchmark Resilience Tool (BRT-53), Measuring Business Excellence, vol. 17, no. 3, pp. 3-14.
96. http://www.change-management-consultant.com/deming-cycle.html.
97. http://www.whatissixsigma.net/pdca- cycle/.
98. http://www.fda.gov/Drugs/DrugSafety/DrugIntegrityandSupplyChainSecurity/DrugSupplyChainSecurityAct/ucm424963.htm.
99. http://www.who.int/3by5/en/storage_pocketguide.pdf - John Snow, Inc./DELIVER in collaboration with the World Health Organization. 2003. *Guidelines for the Storage of Essential Medicines and Other Health Commodities*. Arlington, Va.: John Snow, Inc./ DELIVER, for the U.S. Agency for International Development.
100. http://apps.who.int/medicinedocs/documents/s16755e/s16755e.pdf - Seiter, A. 2005. Pharmaceuticals: Counterfeits, Substandard Drugs and Drug Diversion. HNP brief #2. Washington, D.C.: World Bank.
101. http://www.who.int/hiv/amds/step_by_step_procure_subs_treat.pdf - United Nations Office on Drugs and Crime (UNODC)

Regional Centre for East Asia and the Pacific. 2007. *A 'Step-by-Step' Algorithm for the Procurement of Controlled Substances for Drug Substitution Treatment*. Internal document no. 3/2007. Thailand: UNODC.
102. http://www.who.int/mediacentre/factsheets/fs275/en - WHO (World Health Organization). 2010. "Medicines: Spurious/Falsely-Labelled/ Falsified/Counterfeit (SFFC) Medicines" Fact sheet no. 275. Geneva: WHO.
103. http://whqlibdoc.who.int/hq/1999/WHO_EDM _QSM_99.1.pdf - 1999. *Guidelines for the Development of Measures to Combat Counterfeit Drugs*. Geneva: WHO.
104. http://www.who.int/impact/FinalBrochureWHA2008a.pdf - WHO/IMPACT (World Health Organization/International Medical Products Anti- Counterfeiting Taskforce). 2008. *Counterfeit Drugs Kill!* Geneva: WHO/IMPACT.
105. http://www.rocketwatcher.com/blog/2013/08/speed-up-b2b-sales- process.html.
106. https://totalproductmarketing.com/digital- changed-b2b-buyers-journey/.
107. https://it.pinterest.com/obanajun/buying- process/.
108. http://marketinginteractions.typepad.com/marketing_interactions/2012/10/the- role- of- content-in- the-b2b-it-buying-process.html.
109. http://www.ducatiperformanceparts.net/photographyzym/buyer- decision- process.
110. http://securityfocus.com - Bugtraq vulnerability database.
111. https://www.schneier.com/paper-attacktrees-ddj-ft.html - Schneier, B.: Modeling Security Threats, Dr. Dobb's Journal. (2001).
112. https://www.securityguidance.com/"Citicus ONE". http://www.citicus.com - "Microsoft Security Assessment Tool" .
113. Stuxnet dossier: http://www.symantec.com/connect/blogs/w32 stuxnet-dossier.
114. http://www.lazer.ie/blog/3-types-of-access- control-systems.
115. http://searchsecurity.techtarget.com/definition/access-control.
116. http://www.secsolution.com/articolo.asp?id=305.
117. http://www.secsolution.com/tecnologia.asp?id=3704.
118. http://www.secsolution.com/tecnologia.asp?id=5002.

119. http://www.teknofog.com/it/.
120. http://www.protectglobal.it/nebbiogeno-azienda-negozio-ufficio/business- video/.
121. http://www.naebula.it/language/it/sistemi_nebbiogeni.php.
122. http://www.arturodicorinto.it/tecnologia/lettore-biometrico-per-il-controllo-degli-accessi/ - Lettore Biometrico Per Il Controllo Degli Accessi: Normativa, Uso E Modelli Tecnologia by pg .
123. http://www.axitea.it/offerta/servizi/progettazione-e-realizzazione-di-sistemi-di-controllo-accessi-e-controllo-biometrico/ - Progettazione e realizzazione di sistemi di controllo accessi e controllo biometrico – Axitea URL.
124. http://www.rilevatoripresenze.com/controllo-accessi-biometrico/6.htm - Controllo degli Accessi Biometrico - i sistemi di controllo degli accessi biometrici.
125. http://www.aes-antideflagranti.it/index.php/it/produzione/segnalatori- luminosi/serie-evaflash-200.html.
126. http://www.directindustry.it/cat/sicurezza-delle-macchine-dei-locali/allarmi-visivi-indicatori-luminosi-colonne-luminose-K-637.html.
127. http://www.efficiencyexchange.ac.uk/5496/ten-tips-for-managing-outsourced-contracts/ - Ten tips for managing outsourced contracts By Andy Davies - 22 October 2014.
128. https://www.deloitte.co.uk/makeconnections/assets/pdf/the-outsourcing- handbook-a-guide-to-outsourcing.pdf.
129. https://www.fedpartnership.gov/bank-life-cycle/start-a-bank/outsourcing- and- vendor-management.
130. http://www.firmbuilder.com/articles/5/27/518/ - Corbett, Michael F., & Association, *Best Practices for Deciding What Should be Outsourced*, Firmbuilder.com.
131. Harreld, Heather, *Outsourcing opens security risks*, Federal Computer Week, 5 Jan 1998, http://www.fcw.com/fcw/articles/1998/fcw-risks-1-5- 1998.asp.
132. http://csrc.nist.gov/publications/nistpubs/800-30/sp800- 30.pdf - *Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology (NIST), Special Publication 800-30, Jan 2002.
133. http://www.coltexpress.com/files/WhyOutsource1_AskBefore.

pdf - Manring, Audrey Y., *Ask Before You Outsource: Ten Critical Questions to Put to Potential Service* Providers, (i)Structure Inc., 2001.
134. http://www.cert.org/security-improvement/modules/m03.html - Security *for Information Technology Service Contracts*, Cert Coordination Center, Security Improvement Module, CMU/SEI-SIM- 003, Jan 1998, pg 2.
135. http://users.bestweb.net/~bgeiger/art_paper/pr_csitable.htm - *CSI Roundtable on Outsourcing: managing related security* risks, Computer Security Institute.
136. https://www.prosci.com/change-management/thought-leadership-library/change-management-process - Change Management process.
137. https://www.tutorialspoint.com/management_concepts/change_management_process.htm - Kotter eight steps Change Management process.
138. http://www.itil.co.uk/refresh.htm - ITIL Refresh Statement, Office of Government Commerce.
139. https://www.google.it/search?q=organisational + resilience+images&rlz =1C2GGGE_ itIT397& biw =1366&bih =700&source= lnms&tbm=isch&sa=X&ved= 0ahUKEwiL6Z6rkb XSAhXjQZoKHWCTAOAQ_AUIBigB#imgrc=XWNFbSSBhhK7nM: - Bulding organizational resilience.
140. http://figaro.ae.katowice.pl/~pank/secout2.htm. - Pankowska, M., *Outsourcing Impact on Security Issues*, University of Ecomomics, Information Systems Department, Katowice Poland.
141. http://www.secure20.com/pdfs/InherentSecurityRisksin Outsourcing.pdf - Harris, Michael, *Inherent Security Risks in Outsourcing and Vendor/Partner connections – What the CIO Should Know*, Computer Security Journal, spring 1998.
142. *Crafting a Better Outsourcing Contract*, White Paper, Everest Group, Inc., 1999, http://nersp.nerdc.ufl.edu/~dicke/ism/everest.pdf.
143. http://news.bbc.co.uk/1/hi/business/4094894.stm - Ahmed, Z. (2006) Outsourcing exposes firms to fraud.
144. http://news.bbc.co.uk/1/hi/business/5122886.stm - BBC (2006a) Man held in HSBC India scam probe.

145. http://news.bbc.co.uk/1/hi/uk/4122772.stm - BBC (2006b) Are overseas call centres a fraud risk?
146. http://news.bbc.co.uk/1/hi/uk/4121934.stm - BBC (2006c) India call centre 'fraud' probe.
147. http://news.bbc.co.uk/1/hi/business/3593885.stm - BBC (2006d) Fear over India call centre fraud.
148. http://news.bbc.co.uk/1/hi/business/3569743.stm - BBC (2006e) Credit card chaos in India.
149. http://news.bbc.co.uk/1/hi/world/south_asia/4619859.stm - Biswas, S. (2006) How secure are India's call centres?.
150. http://www.opengroup.org/projects/jericho/uploads/40/6809/vision_wp.pdf - Bleech, N. (2005) What is Jericho Forum?.
151. http://www.nasscom.in/Default.aspx? - NASSCOM (2006). NASSCOM.
152. www.organisationalresilience.gov.au/resources/Pages/default.aspx#_pub. - Australian Government 2011, Organisational Resilience Position Paper. Australian Government.
153. Attorney-General's Department 2010, Insider Threat to Business. Attorney-General's Department. URL: www.organisationalresilience.gov.au/resources/Documents/the-insider-threat-to-business.pdf.
154. www.ag.gov.au/EmergencyManagement/Documents/NationalStrategyforDisasterResilience.PDF. - COAG 2011, National Strategy for Disaster Resilience, Commonwealth of Australia, Canberra.

13. APPENDICE.
RESILIENZA ORGANIZZATIVA: CONCETTI E MODELLI

Il panorama mondiale della ricerca normativa sul tema della Resilienza Organizzativa propone diverse definizioni del termine, tra cui le seguenti sono tra quelle maggiormente accreditate:

- *The ability of an organization to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation by preventing, avoiding and resisting damage and recovery quickly* (BCI conference speaker 2013).
- *The capacity of an organization to plan for and adapt to change or disruption, through anticipation, protection, responsive capacity and recoverability* (BCI working group paper, 2012).
- *The capability of an organization to anticipate, and respond and adapt to, incremental change and sudden disruption in order to survive and prosper* (BS65000).
- *The capacity of an organization to react to change to survive and evolve* (PwC).
- *The maintenance of positive adjustment under challenging conditions such that the organization emerges from those conditions strengthened and more resourceful* (Vogus and Sutcliffe, 2007).

Dal punto di vista di un sistema (organizzazione) che ha lo scopo di garantire la sicurezza, le definizioni generali portano a evincere la resilienza come la capacità di garantire la sicurezza nel tempo (obiettivo dichiarato del sistema) a fronte sia di cambiamenti continui (skill e numerosità del personale, tecnologie, lavori di manutenzione, organizzazione ospedaliera ecc), sia in presenza di casi imprevisti (lavori di riparazione o costruzione straordinari, flussi imprevisti di personale esterno, eventi criminosi).

Nel tempo sono stati sviluppati diversi modelli per affrontare l'argomento della resilienza organizzativa e sono accomunati da questi tre punti chiave:

1. La resilienza organizzativa è la capacità di mantenere livelli sostenibili di sopravvivenza e successo
2. La resilienza è generata o diminuita da fattori come CHI è, COSA fa e COME lo fa riferito alla determinata organizzazione
3. La resilienza – una volta compresa e recepita in tutti i suoi aspetti – può essere alterata, manipolata e moltiplicata al fine di sostenere la permanenza e il successo dell'organizzazione.

Resiliente a che cosa?

Ogni organizzazione ha la propria 'tempesta perfetta' – una combinazione di eventi o circostanze che ha il potenziale per metterla in ginocchio. Per un sistema finanziario, il peggior incubo potrebbe essere l'improvvisa perdita di fiducia dei clienti con l'effetto valanga di 'corsa alla banca'. Per le altre organizzazioni può essere il fallimento di un fornitore chiave, una contaminazione sulla linea di produzione, un caos scatenato da un dipendente scontento, etc.

La resilienza è una capacità strategica

Non si tratta solo di attraversare le crisi; un'organizzazione veramente resiliente ha altri due importanti funzionalità: la previsione e la sensibilizzazione sulla situazione per prevenire possibili crisi, nonché la capacità di trasformare le crisi in una fonte di opportunità strategica.

Le organizzazioni sono inserite in un sistema più grande

Mentre i modelli della ricerca si concentrano fondamentalmente sulla resilienza delle organizzazioni (aziende, agenzie governative, istituzioni, ecc), ogni organizzazione si trova all'interno di un ecosistema e la resilienza è una proprietà di tutti i livelli di questo sistema.

Nessuna organizzazione è un'isola

La resilienza di un'organizzazione è direttamente correlata alla capacità di recupero delle altre organizzazioni da cui dipende (clienti, fornitori, autorità di regolamentazione, e anche concorrenti). Un'organizzazione dipende e contribuisce anche alla resilienza individuale del suo personale e la resilienza delle comunità in cui opera. Allo stesso modo, la resilienza di un'organizzazione è direttamente correlata alla capacità di recupero del suo settore, e la capacità di ripresa del settore si intreccia con la resilienza della Nazione.

13.1 Resilienza Organizzativa: alcuni modelli

Una prospettiva australiana: resilienza ed emergenza

Il concetto di resilienza o la capacità di assorbire gli urti (intesi come avversità) è diventato il tema favorito nell'ambito della gestione dell'emergenza negli ultimi anni, favorito anche da iniziative degli enti governativi.

Raggiungere la resilienza organizzativa, tuttavia, è un processo complesso che coinvolge la gestione delle risorse fisiche e umane, il contesto, la strategia e la valutazione del rischio.

Diversi quadri di teoria organizzativa stabiliscono la varietà di modi nei quali la resilienza può essere migliorata in organizzazioni di servizi di emergenza. L'attenzione si concentra sul concetto di clima organizzativo come prospettiva fondamentale, ma spesso trascurata, da cui partire per capire la resilienza nelle organizzazioni di gestione delle emergenze.

Sotto l'influenza della ricerca sul clima organizzativo, sono emerse quattro dimensioni chiave di analisi:

- Capacità e competenza;
- Vulnerabilità;
- Adattabilità;
- Cultura organizzativa e clima;

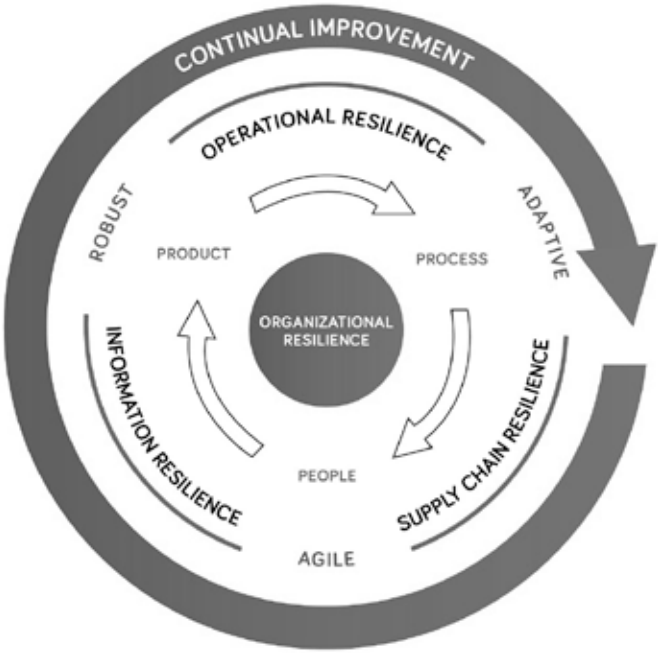
che si sono dimostrate in forte relazione secondo lo schema della figura seguente che mostra le interrelazioni e le interdipendenze tra queste dimensioni.

Come esempio dal modello, l'adattabilità può essere vista come la possibilità di modificare il comportamento per fronteggiare l'evento di stress (Adger et al. 2004) previsto o attuale. L'adattabilità dell'organizzazione è legata alle istituzioni e reti che interfaccia per imparare, acquisire conoscenza ed esperienza, e quindi effettuare le regolazioni in modo da rispondere coerentemente alle perturbazioni di sistema (Pelling et al. 2008).

Similmente, il clima e la cultura organizzativa influiscono sulla capacità dell'organizzazione di far fronte a eventi inattesi e influenzano anche le dimensioni collegate che è stato rilevato essere dipendenti dalla leadership organizzativa.

Il modello del BSI

Il modello BSI divide I requisiti della Resilienza Organizzativa in tre elementi essenziali: eccellenza del prodotto, affidabilità dei processi e comportamenti del personale.



- *Eccellenza del prodotto*: In questo contesto 'prodotto' si riferisce a qualsiasi prodotto, servizio o soluzione un'organizzazione porti al mercato per generare entrate. Il punto di partenza è chiedere quali mercati (bisogni) serve l'organizzazione. Le sue capacità e prodotti corrispondono alle esigenze del mercato – e sono conformi ai requisiti normativi – e se non è così, come si adattano?

- *Affidabilità dei processi*: Incorporare abitudini all'eccellenza nello sviluppo di prodotti e servizi e portarli al mercato, è una componente chiave del successo. Le organizzazioni hanno bisogno di un approccio sistematico alla qualità nel senso più ampio del termine. Queste devono garantire che 'fanno bene le cose' *costantemente* attraverso la forza e l'affidabilità dei loro processi, pur lasciando spazio per l'innovazione e la creatività.

- *Comportamenti del personale*: le persone, la cultura di un'organizzazione e i loro valori determinano il successo aziendale. 'La gente fa affari con persone' può essere un cliché, ma rimane vero che spesso giudichiamo un organizzazione attraverso l'esperienza personale che abbiamo con la stessa. Questo include il modo in cui i suoi dipendenti ci servono, come osserviamo l'azienda interagire con l'ambiente, la società civile e i suoi partner della supply chain su questioni di responsabilità etiche e sociali. Se la nostra esperienza è positiva noi, e molti altri come noi, contribuiremo attivamente a rafforzare cumulativamente la reputazione del marchio.

Il modello del ThinkGRC Business Resiliency Index Survey Tool

Il modello ThinkGRC evidenzia l'emergenza dal lavoro di ricerca sull'argomento della resilienza organizzativa in tre categorie generali:

- Leadership e cultura;
- Preparazione al cambiamento;
- Reti.

Queste a loro volta sono esplose in 13 indicatori che vengono utilizzati per valutare la resilienza di un'organizzazione:

- *Leadership*: una forte leadership capace di fornire una buona gestione e decisioni rapide in tempi di crisi, così come la valutazione continua delle strategie e dei programmi di lavoro verso gli obiettivi organizzativi.

- *Impegno del personale*: L'impegno e il coinvolgimento del personale che capisca il legame tra il proprio lavoro, la resilienza dell'organizzazione, e il suo successo a lungo termine. Al personale va assegnato il potere necessario a utilizzare le proprie competenze per risolvere i problemi.

- *Consapevolezza della Situazione*: Il personale è incoraggiato ad essere vigile verso l'organizzazione, le sue prestazioni e potenziali problemi. Il personale è ricompensato per la condivisione di buone e cattive notizie sulla organizzazione compresi i segnali di allarme precoce e questi vanno rapidamente riportati ai leader dell'organizzazione.

- *Processo decisionale*: il personale ha l'autorità appropriata per prendere decisioni relative al proprio lavoro e l'autorità è chiaramente delega-

ta per consentire una risposta adeguata alle crisi. Personale altamente qualificato è coinvolto, o è in grado di prendere decisioni, laddove la conoscenza specifica aggiunge un valore significativo, o dove il coinvolgimento sarà di aiuto per l'attuazione delle soluzioni.

- *Innovazione e creatività*: Il personale è incoraggiato e premiato per utilizzare le proprie conoscenze in modi nuovi per risolvere problemi nuovi ed esistenti, e per utilizzare approcci innovativi e creativi a soluzioni in via di sviluppo.

- *Collaborazioni efficaci*: La comprensione dei rapporti e delle risorse che l'organizzazione potrebbe necessitare da altre organizzazioni nel corso di una crisi, e la pianificazione e gestione per garantirne l'accesso.

- *Accesso alla Conoscenza*: le informazioni critiche sono memorizzate in un certo numero di formati e posizioni e il personale ha accesso alle opinioni degli esperti in caso di necessità. I ruoli sono condivisi e il personale viene addestrato in modo che qualcuno sarà sempre in grado di ricoprire i ruoli chiave.

- *Rottura dei Silos*: Minimizzazione delle barriere sociali, culturali e comportamentali di divisione, che spesso si manifestano come barriere di comunicazione che creano vie disconnesse, impervie e dannose per il lavoro.

- *Risorse interne*: la gestione e la mobilitazione delle risorse dell'organizzazione al fine di garantire la sua capacità di operare nel business standard, oltre ad essere in grado di fornire capacità supplementari necessarie durante una crisi

- *Unità di intenti*: vasta diffusione delle priorità a seguito di una crisi, chiaramente definite a livello di organizzazione, così come la comprensione delle esigenze minime di funzionamento dell'organizzazione.

- *Attitudine proattiva*: prontezza strategica e comportamentale di rispondere ai segnali premonitori di cambiamento dell'ambiente interno ed esterno dell'organizzazione, prima che si aggravino in crisi.

- *Pianificazione delle strategie*: Lo sviluppo e la valutazione di piani e strategie per gestire le vulnerabilità in relazione al contesto economico e le parti interessate.

- *Pianificazione di stress test*: La partecipazione di personale nelle simulazioni o scenari progettati per esercitare le modalità di risposta e validare piani.

BS65000 standard model

La normative BS 65000 propone invece un modello circolare che mira a costruire la resilienza organizzativa attraverso la governance di una serie di processi per preparare l'organizzazione a rispondere e adattarsi al cambiamento sia continuo che inatteso sopravvivendo e prosperando nel mercato.

Developing Resilience

14. Allegato 1: Questionario base per lo strumento di calcolo del LMS

La base di dati per la valutazione dello stato di sicurezza del sito della FO secondo la scala Lockpill, viene costruito a partire da un questionario basato sulle cinque dimensioni base della Linea Guida del progetto Padlock 1 edita come Quaderno del Sole24ore.

La seguente tabella riporta i quesiti definiti all'interno del progetto Padlock 2 suddivisi secondo la dimensione di valutazione della sicurezza di appartenenza:

N° Criterio	Denominazione Criterio	Quesito
1	**Controllo degli accessi**	Esiste un sistema di controllo degli accessi alla FO?
		Il sistema di controllo degli accessi è centralizzato per tutto l'ospedale? (se NO segnare la percentuale di accessi collegati al sistema)
		Le chiavi elettroniche sono personalizzate?
		Esiste una lista delle persone autorizzate con chiave?
		La lista delle persone autorizzate ad avere la chiave è mantenuta in luogo accessibile solo al Responsabile delle autorizzazioni?
		Il personale autorizzato ha un codice unico?
		Il codice assegnato alle singole persone viene modificato periodicamente?
		La modifica del codice assegnato viene notificata al Responsabile?
		I codici sono noti al personale preposto alla gestione della sicurezza attiva? (sorveglianza)

		Il sistema di controllo della FO è parte del sistema di controllo generale dell'Ospedale?
		Il codice assegnato alle persone per accedere ai Reparti dell'Ospedale è diverso da quello per accedere ai locali della FO? (se SI, compilare coerentemente la % di applicabilità – solo per alcuni 10%, per tutti 100%)
		Le chiavi fisiche dei locali della FO sono assegnate a una lista di persone specifiche?
		Le copie delle chiavi dei locali della FO sono assegnate anche agli addetti all'anti incendio?
		La sorveglianza è l'unica a disporre di copia delle chiavi dei locali della FO?
		Quando la FO è aperta le chiavi sono conservate in luogo non accessibile alle persone non autorizzate?
		Le chiavi, negli orari di apertura della FO, sono mantenute in zona non accessibile in armadietto con chiusura di sicurezza?
		Il sistema di controllo dell'ingresso non viene mai by-passato forzando la porta in posizione aperta in determinati orari?
		Il personale autorizzato provvede a far registrare tutto il personale di ditte fornitrici, rappresentanti farmaceutici ecc. prima di farli accedere ai locali della FO?
		Esiste un sistema di registrazione dell'ingresso di personale esterno alla FO?
		Il registro del personale esterno viene controllato dal Responsabile o da suo incaricato periodicamente?
2	**Sistemi di protezione volumetrica interna**	LA FO dispone di sistemi di rilevazione volumetrica?
		I sensori volumetrici sono a tecnologia non oscurabile? (se SI specificare in quale %)
		I sensori volumetrici sono almeno a doppia tecnologia? (se SI specificare in quale %)

		Ci sono sensori a tripla tecnologia anti mascheramento, anti accecamento e anti strisciamento? (se SI specificare in quale %)
		I sensori coprono le zone di ingresso alla farmacia? (se SI specificare in quale %)
		I sensori coprono le stanze della FO che hanno un collegamento con l'esterno (porta, finestra)? (se SI specificare in quale %)
		I sensori coprono l'area delle stanze in cui sono inseriti? (se SI specificare in quale %)
		Ci sono ostacoli al raggio di rilevamento dei sensori? (se SI specificare in quale %)
		Le scaffalature e i materiali vengono posizionati in modo da non costituire ostacolo alla visione dei sensori? (se SI specificare in quale %)
		Se momentaneamente i volumi di merce da conservare in FO sono tali da dover necessariamente oscurare il raggio di rilievo dei sensori, dove questo accade viene segnalato e vengono prese decisioni in merito?
		In caso di inevitabile oscuramento del sensore è prevista la messa in opera di una modalità di controllo alternativo?
		Si è evitato di avere aree completamente sprovviste di protezione volumetrica in corrispondenza di finestre prive di grate e/o sensori anti intrusione? (se SI specificare in quale %)
		La capacità di copertura delle aree da parte dei sensori è verificata periodicamente?
		Vengono registrate le verifiche periodiche di copertura dei sensori?
		Vengono eseguite prove periodiche di funzionamento dei sensori anche in rapporto alla capacità di innesco del sistema di allarme? (blocco porte, sirene ecc)
		L'installazione dei sensori è fatta – o coordinata se da appaltatore esterno – dal personale autorizzato dell'ospedale?

		In caso di prova periodica dei sensori da parte di personale esterno, è stato definito un incaricato interno per la supervisione delle attività?
		In caso di guasto di un sensore, è prevista una procedura per la sostituzione urgente dello stesso anche con acquisto per via straordinaria?
		Viene verificato periodicamente che le zone di installazione dei sensori non siano soggette a episodi di infiltrazione di umidità, muffe e altri elementi ambientali non tipici che possano minare la funzionalità del sensore?
		I sensori dispongono di batteria di back up in caso di taglio dell'alimentazione di rete?
		Viene verificato periodicamente lo stato di carica o viene periodicamente sostituita la batteria di back up dei sensori?
3	**Protezione perimetrale (passiva e attiva)**	Gli ingressi ai locali della FO sono protetti da porte blindate?
		Le porte di ingresso ai locali della FO che non sono blindate sono provviste di grate di protezione?
		Le finestre dei locali della FO sono provviste di grate di protezione?
		Le grate di protezione sono poste all'interno del serramento?
		Il sistema di fissaggio delle grate di protezione è permanente (perni cementati nel muro)?
		Le grate di protezione sono in acciaio ad alta resistenza al taglio? (almeno classe 4 – resistenza al taglio 10min – o classe 5 – resistenza al taglio 15min)?
		Le grate di protezione delle porte sono dotate di snodi autobloccanti?
		Le grate di protezione delle porte hanno almeno tre punti di chiusura?
		Le grate di protezione sono allarmate con sensori di vibrazione (inerziali o sismici)?

		Le finestre sono allarmate con sensori di contatto o magnetici per il rilievo di apertura infisso?
		Le finestre sono allarmate con sensori di vibrazione (inerziali o sismici)?
		Le grate di protezione sono fissate con viti?
		Le porte di ingresso alla FO sono allarmate con sensori di contatto o magnetici per il rilievo di apertura infisso?
		Le porte di ingresso alla FO sono allarmate con sensori di vibrazione (inerziali o sismici)?
		La funzionalità dei sensori viene verificata periodicamente?
		Lo stato di conservazione delle grate viene verificato periodicamente?
4	**Allarmi/procedure di intervento**	La centralina dell'allarme è posta in locale ad accesso controllato?
5	**Sistemi video**	È presente un sistema di video sorveglianza?
		La video sorveglianza è attiva 24h?
		È presente un sistema di registrazione dei filmati delle telecamere?
		La durata di registrazione prima della sovrascrittura è di almeno 7 giorni?
		Il sistema di registrazione è a nastro?
		Il sistema di registrazione copre tutte le telecamere attive?
		Le telecamere esterne inquadrano tutti gli accessi principali alla FO?
		Le telecamere esterne inquadrano tutte le pareti con finestre della FO?
		I filmati sono visionati in tempo reale?
		La visione dei filmati in tempo reale è presso il servizio di portineria interno dell'ospedale?
		La visione dei filmati in tempo reale è presso il servizio di guardiania interno dell'ospedale?

		La visione dei filmati in tempo reale è gestito da appaltatore esterno che visualizza la situazione da remoto?
		Sono presenti telecamere all'interno dei locali della FO?
		Le telecamere interne sono accese sempre nelle ore di chiusura della FO?
		Le telecamere interne inquadrano almeno gli ingressi principali alla FO?
		Le telecamere sono dotate di sistemi di rilievo del movimento?
		Le telecamere esterne sono dotate di illuminatori a infrarossi per la visione notturna?
		La centralina di allarme per movimento rilevato da telecamere integra anche i sensori anti intrusione?
		Le telecamere sono in posizioni elevate protette da facili manomissioni?
		Ci sono telecamere "fake" deterrenti?
		Il sistema di telecamere della FO è integrato con quello dell'Ospedale?
		Le telecamere con sensore di movimento sono parte della sensoristica collegata con il sistema di allarme della FO?

15. Allegato 2: Esempio specifiche telecamera professionale top level

Tipo	IP
Posizionamento supportato	Outdoor
Controllo PTZ (Pan/Tilt/Zoom)	
Modalità giorno/notte	
Ingresso/uscita allarme	
Fattore di forma	box
Colore del prodotto	White
Tipo di montaggio	Wall
Codice IP (Marchio Internazionale Protezione)	IP66
Risoluzione massima	1920 x 1080
Formati video supportati	H.264,M-JPEG,MPEG4
Risoluzioni grafiche supportate	176 x 144,1920 x 1080 (HD 1080)
Modalità video supportate	1080p
Frame rate	30
Megapixel	2
Angolo di visualizzazione (orizzontale)	73.5
Angolo di visualizzazione (verticale)	42.5
Tipo sensore	CMOS
Dimensioni sensore ottico	1/2.7
Zoom digitale	10
Filtraggio per indirizzo IP	
Algoritmi di sicurezza supportati	HTTPS
Crittografia HTTPS	
Tipi schede di memoria	SD,SDHC

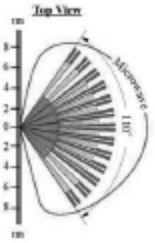
Visione notturna	
Distanza di visione notturna	30
Tipo LED	IR
Lunghezza d'onda a infrarossi	4.3
Collegamento ethernet LAN	
Tecnologia di cablaggio	10/100Base-T(X)
Protocolli di rete supportati	IPv4, ARP, TCP/IP, RTSP, RTP, RTCP, HTTP, SMTP, FTP, NTP, DNS, DHCP, UPnP, DDNS, PPPoE, Samba Client, 3GPP
Tecnologia di connessione	Wired
Microfono incorporato	
Larghezza	97.5
Profondità	316.5
Altezza	249.1
Peso	1920
Tensione di ingresso AC	100-240
Frequenza di ingresso AC	50/60
Consumi	11.2
Jack DC-I	
Ampère CC in uscita	25
Volt CC in uscita	+12V
Certificazione	CE, CE LVD
Intervallo temperatura di funzionamento	-40 - 50
Intervallo di temperatura	-20 - 70
Range di umidità di funzionamento	20 - 80
Umidità	5 - 95
Sistema operativo Windows supportato	
Cavi inclusi	AC
Manuale dell'utente	
Sistema operativo compatibile	MicrosoftWindows 7/Vista/XP
Numero F (apertura relativa)	2

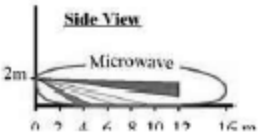
16. Allegato 3: Esempio specifiche sensore volumetrico professionale top level

RIVELATORE TRIPLA TECNOLOGIA
2PIR+MW ESTERNO/INTERNO 12M

CARATTERISTICHE TECNICHE

ALIMENTAZIONE	12Vcc
ASSORBIMENTO	40mA max
PORTATA CONT. ALLARME	250mA a 50Vcc max
PORTATA CONT. ANTIM.	100mA a 24Vcc max
PORTATA CONT. TAMPER	100mA a 24Vcc max
TEMPO DI AUTOVERIFICA	2 minuti
DURATA ALLARME	2 secondi
RISPOSTA AL MASCHERAM.	2 minuti max
VELOCITA' RILEVABILE	da 0,1 a 5 m/sec
COPERTURA	12 metri a 110°
TEMP. DI FUNZIONAMENTO	-37° +70°C
IMMUNITA' RFI	20V/mt. Dc a 1 GHz
UMIDITA'	95%
FREQ. MICROONDA	10,525 GHz - 2,4 GHz
DIMENSIONE	160x95x59
PESO	130g





17. Allegato 4: Esempio specifiche sistema di controllo accessi a lettura della retina professionale top level

IRI-06	
Descrizione	Il più elevato sistema di riconoscimento disponibile oggi sul mercato
	Precisione e velocità per ogni esigenza di sicurezza
Applicazioni	Controllo Accessi di massima sicurezza
	Video Sorveglianza (telecamera CCVE a colori integrata)
Dimensioni / Peso	212 x 216 x 55 mm / 2,4 kg
Comunicazione	TCP/IP
Specifiche	Non invasivo: il contatto con il sensore non è necessario
	FAR e FRR praticamente nulli
	Design di qualità
	Sistema formato da 2 telecamere che rilevano entrambi gli occhi
	Voce guida sintetizzata in italiano per il corretto posizionamento
	Insensibile a normali occhiali (anche da sole) e lenti a contatto

finito di stampare nel mese di giugno 2018
dalle Edizioni Il Campano

con il contributo non condizionato di

SIFO
Via Carlo Farini, 81 - 20159 MILANO
Tel. 02 6071934 - Fax 02 69002476
www.sifoweb.it - segreteria@sifoweb.it