Roma – 19 marzo 2024

Paolo Guidelli

LA SALUTE E LA SICUREZZA: RISCHI ED AMBIENTI DI LAVORO

Innovazioni degli strumenti informatici: sicurezza informatica, archiviazione sicura

Agenda

Innovazione (in Inail)

Sicurezza e Prevenzione (guardando all’ICT)

Un po’ di pratica

Agenda

Innovazione (in Inail)

Sicurezza e Prevenzione (guardando all’ICT)

Un po’ di pratica

L'*Innovazione*

Innovazione: attività attraverso la quale vengono sviluppate nuove idee che possano essere fonte di nuovi prodotti, servizi o processi

Innovazione chiusa: processi verticali che si realizzano attraverso le tradizionali attività di R&D

Innovazione aperta: processi orizzontali caratterizzati da relazioni tra più soggetti i quali apportano e condividono conoscenze e competenze che possano creare più valore di quanto se ne creerebbe con un modello chiuso

Fonte: Open Innovation – Aspetti teorici ed evidenze empiriche – Gabriele Santoro

L'Innovazione aperta *in Inail*

Intercettare, valutare ed implementare soluzioni IT innovative è un requisito essenziale per favorire il percorso di evoluzione tecnologica di Inail

- ***Coinvolgere*** nel processo di innovazione competenze provenienti d***a diversi Uffici della Organizzazione*** nel rispetto delle competenze distintive di ciascuno

- ***Evitare le sovrapposizioni con altri processi aziendali*** incaricati di raccogliere ed analizzare le esigenze

- ***Mantenere*** la ***spinta innovativa*** all'interno dei ***binari strategici*** definiti dalla Organizzazione

Adozione incrementale dell'innovazione all'interno della strategia Inail

Piano 14 -16

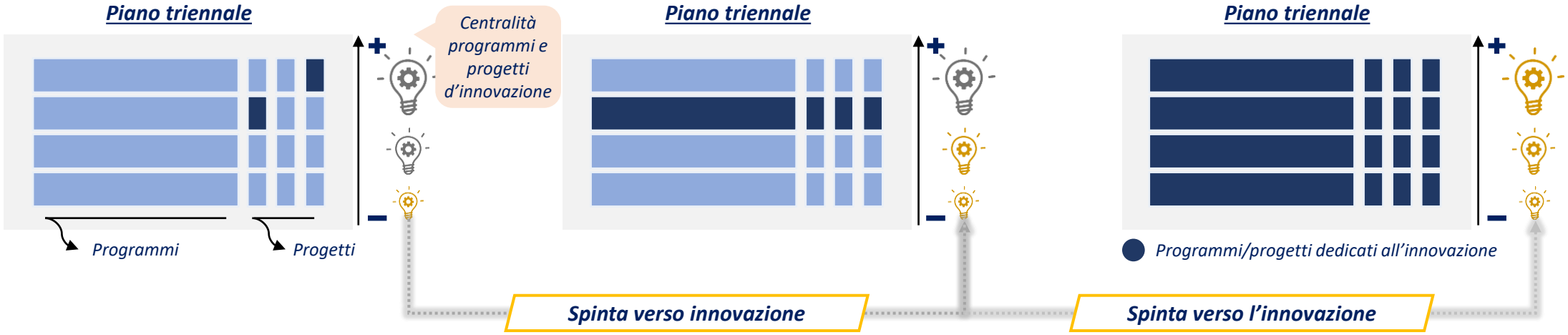
- **Disegno ed Implementazione di progetti** ad alto contenuto innovativo:
  - **SOE** (*Smart Orthopedic Equipment)*
  - **KHARE** (*Kinect Hololens Assisted Rehabilitation Experience)*

Piano 17 - 19

- **Introduzione programma** di **innovazione** *(sezione LP4: Promozione, diffusione e gestione delle soluzioni innovative sperimentate)*:
  - Gestione dinamica del portfolio dei progetti d'innovazione per favorire l'innesco delle iniziative

Piano 20 - 22

- L'**innovazione** non è più relegata ad **un'apposita sezione** ma è **diffusa** all'interno della pianificazione con un specifico programma (*P4: Tecnologie innovative*) dedicato alla strategia, in modo da fornire l'impulso a **sviluppare e rilasciare servizi digitali ad alto impatto**



Agenda

Innovazione (in Inail)

Sicurezza e Prevenzione (guardando all’ICT)

Un po’ di pratica

Dispositivi di proprietà del datore di lavoro o del lavoratore

Dispositivi aziendali

Politica organizzativa che prevede la fornitura dei dispositivi informatici da parte dall'azienda.

È importante che le aziende adottino un regolamento interno sull'uso degli strumenti informatici (siano essi hardware e/o software) utilizzati dai lavoratori e il cui scopo è quello di dettare le procedure per una corretta e adeguata gestione del patrimonio informativo aziendale.

BYOD (Bring Your Own Device)

È un'espressione usata per riferirsi alle politiche aziendali che permettono di portare i propri dispositivi personali nel posto di lavoro, e usarli per avere gli accessi privilegiati alle informazioni aziendali e alle loro applicazioni.

Impatti globali degli **attacchi informatici** sulle aziende e sui dipendenti

Nel teatro degli attacchi informatici alle aziende, l'attenzione tradizionalmente si concentra sull'interruzione dei servizi, sulla compromissione dei dati aziendali, dei clienti e dei brevetti.

Queste preoccupazioni, amplificate dagli attacchi ransomware (che minacciano la continuità operativa) e dalla data exfiltration (che espone dati sensibili) spesso oscurano un elemento essenziale: la **sicurezza** e la **privacy dei dipendenti**.

Mentre affrontiamo la protezione dei dati aziendali e la gestione della minaccia ransomware è imperativo riconoscere il ruolo spesso sottovalutato della tutela dei **dati personali** (dei lavoratori).

Un approccio olistico alla sicurezza aziendale deve integrare efficacemente la protezione dei dipendenti, garantendo un equilibrio che difenda sia la sicurezza aziendale che la **privacy dei lavoratori** in un contesto sempre più complesso e sfidante.

Sicurezza dei dispositivi e **consapevolezza del personale**

- Lavoratori "videoterminalisti" in smart working utilizzano dispositivi aziendali dotati di misure di sicurezza avanzate. Tuttavia, la pratica comune di combinare dati aziendali e personali in tali dispositivi aumenta il **rischio di esposizione**, specialmente quando i dipendenti non sono consapevoli di tale pratica.
- Promuovere una **consapevolezza** chiara tra i dipendenti e implementare politiche di sicurezza rigorose è fondamentale per garantire una **protezione** adeguata senza compromettere né la **sicurezza aziendale** né la **privacy dei lavoratori**.

Azioni chiave per la **sicurezza aziendale e dei lavoratori**

Sicurezza delle postazioni informatiche

Garantire la sicurezza della postazione informatica non solo per i **dati aziendali** ma anche per quelli **personali dei lavoratori**.

Raccolta e gestione responsabile dei dati

Garantire che vengano raccolti e gestiti solo i dati **strettamente necessari** per **evitare rischi** eccessivi di esposizione.

Formazione e sensibilizzazione

Fornire **formazione** e **sensibilizzazione** specifica sulla sicurezza delle informazioni personali dei dipendenti. Questa formazione dovrebbe andare oltre la semplice **consapevolezza** aziendale, concentrandosi anche sulla protezione dei **dati personali**.

Strumenti informatici accessibili e sicuri

Assicurare che gli strumenti informatici aziendali, come presenze/timesheet e intranet, rispettino i requisiti minimi di funzionalità, siano accessibili e semplici da utilizzare.

Protezione dell'immagine sociale dei dipendenti

Prevenire il rischio di esposizione sui social media in caso di eventi negativi legati all'azienda. In particolare, gestire attentamente la presenza sui social che prevedono il collegamento tra azienda e lavoratori, come LinkedIn e altri.

Agenda

Innovazione (in Inail)

Sicurezza e Prevenzione (guardando all’ICT)

Un po’ di pratica

Analisi dei rischi cyber nella gestione della sicurezza delle informazioni

I passi e le attività necessarie per raggiungere il traguardo possono così riassumersi:

- identificazione e classificazione degli asset informativi di valore;
- identificazione delle minacce cyber e vulnerabilità che potrebbero mettere a rischio tali asset;
- identificazione e valutazione delle contromisure di sicurezza a protezione di tali asset;
- analisi e **valutazione dei rischi**;
- definizione e attuazione di un piano di risposta ai rischi selezionati;
- monitoraggio e verifica del piano di risposta.

Valutazione del rischio

- Con il termine **valutazione del rischio** si fa riferimento alla determinazione quantitativa o qualitativa del rischio associato ad una situazione ben definita e ad una minaccia conosciuta (detta "pericolo").
- Una **valutazione quantitativa** del rischio richiede la determinazione di due componenti del rischio: la **gravità** (detta "magnitudo") di una **potenziale perdita** (o danno) e la **probabilità** che tale perdita si realizzi. Per "rischio accettabile" si intende un certo rischio che è identificato e tollerato generalmente perché i costi o le difficoltà per implementare una contromisura efficace risulterebbero eccessivi se confrontati con l'aspettativa della perdita.

RISCHIO= Impatto x Probabilità

IMPATTO	IMPROBABILE	SCARSAMENTE PROBABILE	PROBABILE	FREQUENTE	MOLTO FREQUENTE
MOLTO ALTO	5	10	15	20	25
ALTO	4	8	12	16	20
SIGNIFICATIVO	3	6	9	12	15
TRASCURABILE	2	4	6	8	10
NESSUN EFFETTO	1	2	3	4	5

PROBABILITÀ

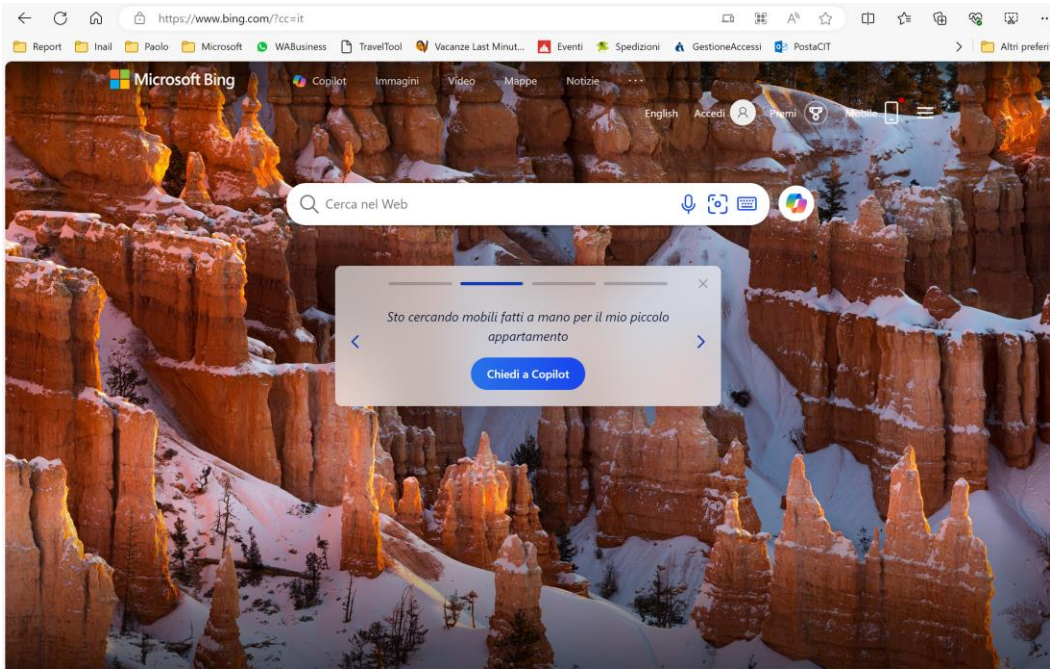
Criptazione dispositivi di memorizzazione

- BitLocker (Microsoft)
  - Selezionare il pulsante Start
  - Selezionare Impostazioni
  - Aggiornamento e sicurezza
  - Crittografia dispositivo

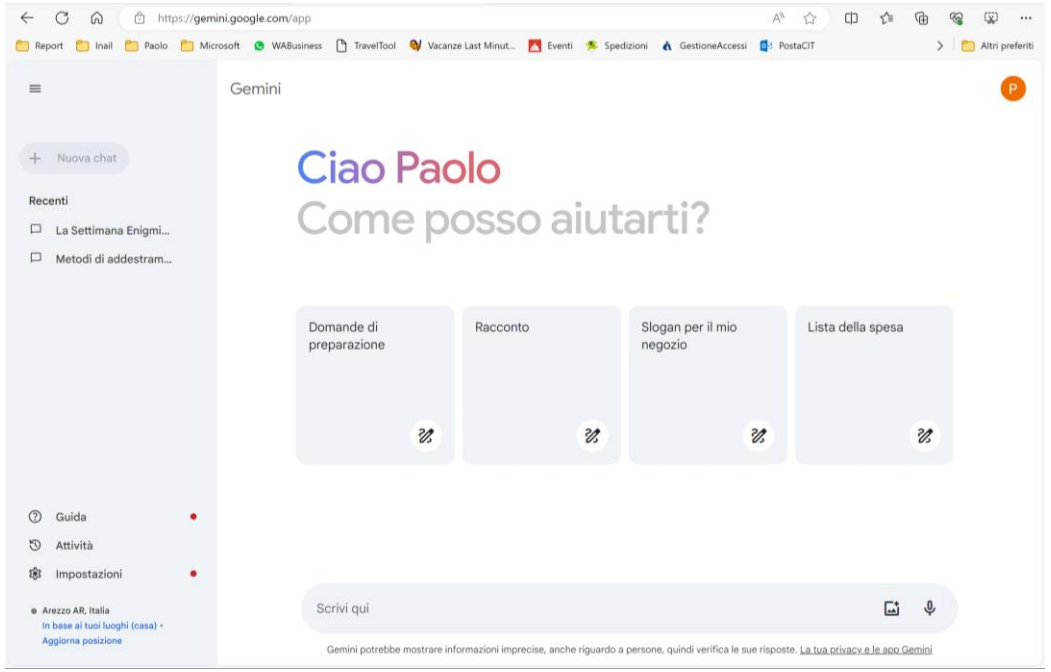
- FireVault (Apple)
  - Nel Finder sul Mac aprire una finestra
  - Tenendo premuto il tasto Ctrl fare click sull’elemento che si desidera codificare
  - Scegliere la voce cripta [nome dell’elemento] dal menu di scelta rapida

Intelligenza artificiale generativa

Bing - Copilot



Google - Gemini



Grazie per l’attenzione