AiFOS
Associazione Italiana Formatori ed Operatori della Sicurezza sul Lavoro

A&T Ambiente Tecnologia Formazione

Convegno di studio e approfondimento

PRIVACY:
NUOVA FRONTIERA DELLA SICUREZZA
Il regolamento Ue 679/2016

Relatore: Dott. Francesco Naviglio

GARIGA DI PODENZANO (PC), 28 giugno 2017 - dalle ore 9.30 alle ore 13.00

CONFCOMMERCIO IMPRESE PER L'ITALIA

CIIP Consulta Interassociativa Italiana per la Prevenzione

ANMIL Onlus

Media Partner

PuntoSicuro

AMBIENTE&SICUREZZA

AiFOS

Un esperto quale l'RSPP oltre ad occuparsi di sicurezza (lato safety) deve essere un consulente olistico ossia essere in grado di analizzare e comprendere tutti quegli aspetti che stanno alla base della sicurezza dell'azienda e del lavoratore.

AiFOS

Quali sono gli aspetti fondamentali per l'integrazione del sistema privacy in azienda?

- Analisi del rischio
- Definizione delle procedure per ridurre i rischi
- Formazione degli addetti (tutti coloro che trattano i dati in azienda, a tutti i livelli)

AiFOS

Non esiste un modello valido per tutte le realtà aziendali.
Il processo di integrazione deve essere **personalizzato**, **progettato** e **contestualizzato** per ogni realtà lavorativa.

È necessario creare un modello integrato per la sicurezza dei dati

AiFOS

A quali rischi è esposta un'azienda?

I nostri sistemi sono vulnerabili?

oppure

Vi sono sufficienti protezioni ma l'errore umano è sempre in agguato?

La formazione interna

AiFOS

Occorre formare il personale dell'azienda affinché **sia preparato ad affrontare attacchi interni ed esterni**, oltre che ad agire in modo da ridurre il rischio d'attacco.
Ad esempio, conservare le password in luogo consono, non installare applicazioni di natura incerta, ecc.

L'azienda deve inoltre implementare i sistemi di protezione informatici (antivirus, firewall, ecc).

AiFOS

Con il termine **ATTACCO**, in ambito informatico, si intende qualsiasi agente *accidentale* o *intenzionale* finalizzato a sovvertire le misure di sicurezza di un sistema informatico.

Gli attacchi possono derivare da:

- **AGENTI NON UMANI**
- **AGENTI UMANI**

AiFOS

Agenti non umani

Quali ad esempio: interruzione della corrente elettrica, sbalzi di tensione, malfunzionamenti hardware, calamità naturali (fulmini, terremoto, incendio, alluvione…)

AiFOS

Agenti umani

Intenzionali quando vi è la volontà di realizzare un danneggiamento o una frode

Esempio:

- ***Hackeraggio:*** aggressione da parte di soggetti esterni intenzionati a compromettere la sicurezza del sistema informativo compromettendo o rendendo indisponibili informazioni
- ***Packet sniffing*****:** tecniche di monitoraggio del traffico di rete ed estrazione informazioni sensibili (password, coordinate bancarie, carte credito ecc)
- Infezioni da virus informatici o programmi dannosi

Non intenzionali se non vi è la volontà dell'atto, si tratta cioè di errori

- **Inadeguatezza** delle **politiche di sicurezza interne alla rete** (backup, visibilità ecc…)
- **Errata gestione** delle **password** e delle **politiche di accesso**
- **Sovrascrizione** involontaria di **dati**

AiFOS

Come garantire la sicurezza di un sistema informatico nelle specifiche realtà aziendali?

AiFOS

SICUREZZA DI UN SISTEMA INFORMATICO

La **sicurezza di un sistema informatico** coincide con l'insieme di tutti quegli accorgimenti organizzativi e tecnici che debbono essere adottati per ridurre al minimo tutti i possibili attacchi da parte di un qualsiasi agente (accidentale o intenzionale, umano o non umano).

AiFOS

La sicurezza del sistema informatico viene spesso indicata con l'acronimo **CIA** dalle iniziali di:

Confidentiality

mantenere la segretezza dei dati

Integrity

evitare che i dati vengano alterati

Availability

garantire che il sistema continuerà ad operare

AiFOS

Per ogni *asset* (insieme di dati, risorse umane e risorse tecnologiche per l'erogazione di un servizio IT) è indispensabile **eseguire**:

ANALISI (DEL RISCHIO):

- Individuare le situazioni di **vulnerabilità** e le possibili **minacce** contestualizzate alla realtà aziendale
  - **caratteristiche** delle **risorse interne**
  - **contesto territoriale** in cui l'azienda è inserita

GESTIONE (DELLA PROBLEMATICA):

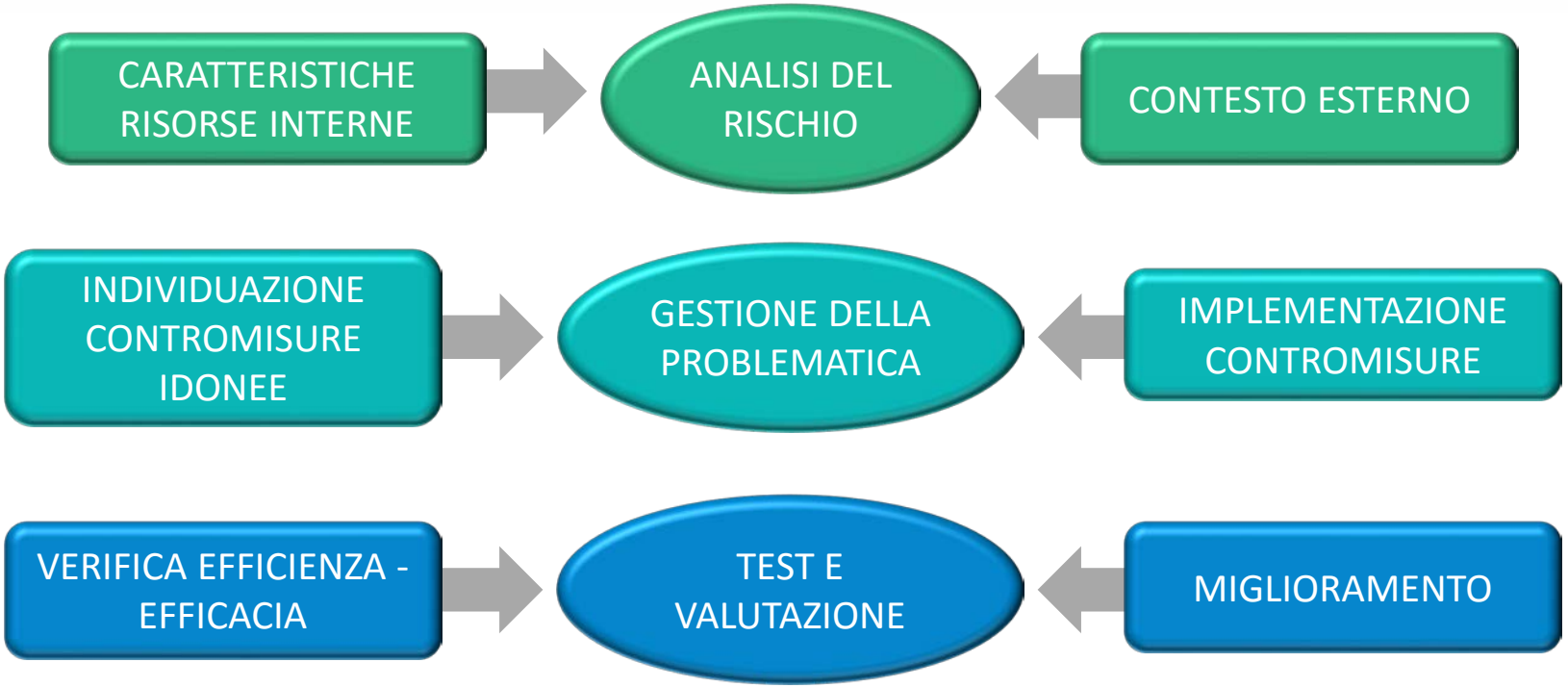
- **Individuare misure di prevenzione** idonee alle specifiche minacce rilevate
- **Implementare contromisure**

TEST E VALUTAZIONE (AUDIT):

- **Pianificare** il loro **controllo** al fine di verificarne l'efficacia e l'efficienza

Attacchi e contromisure

AiFOS



AiFOS

PRINCIPALI TECNICHE DI PREVENZIONE

Esistono tecniche di prevenzione volte a limitare la vulnerabilità dei sistemi che devono essere integrate necessariamente con la formazione e la sensibilizzazione delle risorse umane.

AiFOS

Contromisure Tecnologiche (attacchi esterni):

- **Uso della crittografia**: tecnica di codifica dei dati che li rende incomprensibili a persone non autorizzate agli accessi
- **Autenticazione degli utenti**: garantisce il riconoscimento in modo univoco dell'identità dell'interlocutore
- **Firewall**: dispositivo di sicurezza della rete volto a proteggerla dall'accesso di utenti non autorizzati

AiFOS

Contromisure di sensibilizzazione del personale (attacchi interni):

- **Fare formazione ed aggiornamento** a tutti i livelli
- **Definire regole** chiare e condivise
- **Responsabilizzare** gli utenti

AiFOS

Contromisure fisiche di un sistema informativo:

- Sicurezza dell'edificio e dei locali che ospita il sistema informativo, e i server di Backup che dovrebbero essere in zone geografiche sicure o a basso rischio
- Controlli di accesso delle persone all'edificio
- Sistemi di business continuity e di disaster recovery

La proposta AiFOS

AiFOS

1. Videoconferenza informativa
2. Corso DPO con la collaborazione di ente certificato
3. Corsi di aggiornamento RSPP, ASPP sulle novità del REGOLAMENTO UE 679/2016

Grazie per l'attenzione!

AiFOS
Associazione Italiana Formatori ed Operatori della Sicurezza sul Lavoro

A&T
Ambiente Tecnologia Formazione