In quest'ultima lezione parleremo di **Risk Management** (Gestione del Rischio) in ambito di sicurezza che fa parte di un concetto più grande quale il GRC - Governance RiskManagament & Compliance.

Tutto ciò ha portato oggi le aziende ad investire in ambito di cybersicurezza.

L' **ISO 27001** è lo standard e la certificazione per la gestione della sicurezza delle informazioni.

N.B. OWASP é orientata alle Web Application (ed é pubblico);
ISO 27001 é orientata alle organizzazioni (ed é a pagamento).

probabilità — interamente o parzialmente

Rischio Informatico: possibile verificarsi di eventi rilevanti nel perimetro ICT che possono avere un impatto negativo su una organizzazione.

es: economico

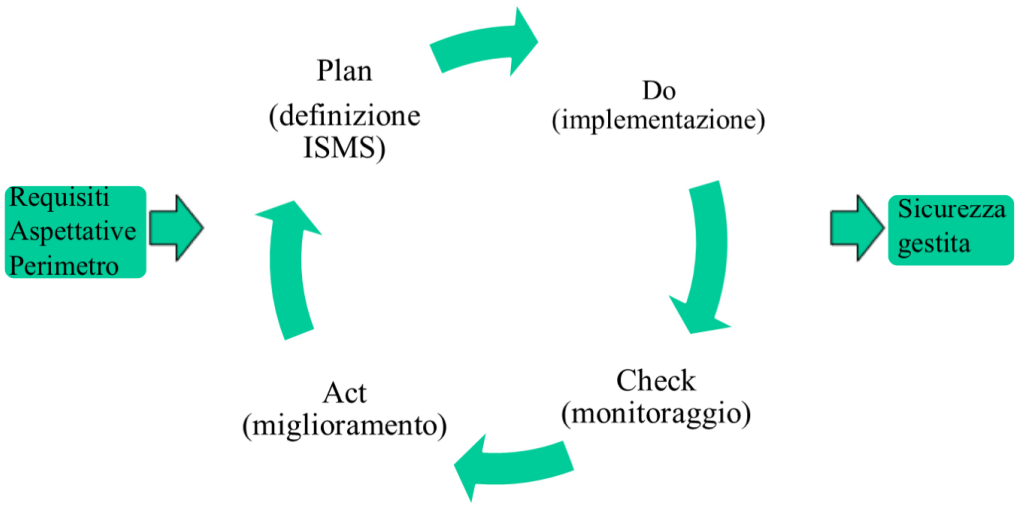
Da qui possiamo determinare la
Gravità del Rischio = Probabilità (Evento) * Peso (Impatto)

Il perimetro ICT, nel caso di organizzazioni molto grandi, generalmente si riferisce solo a specifiche parti (e non all'intera organizzazione troppo vasta). Può essere delineato indicando ad esempio un insieme di indirizzi IP oppure una lista di applicazioni.

Entrando più nello specifico, ISO 27001 é un insieme di normative (aggiornate di anno in anno) che prevede il rilascio di una certificazione da parte di un ente accreditato. Esempio (in Italia): Accredia
Perché lo fanno? É uno stimolo a fare le cose in modo corretto e ha una valenza a livello internazionale.

Tale ISO (così come altre) si basa sul concetto di "***sistema di gestione***" che esce da una "visione binaria" del mondo (sicuro/insicuro) e viene chiamato **ISMS -** *Information Security Management System* che va ad integrarsi con i processi aziendale.

Un Sistema di Gestione è un sistema che mi permette di implementare delle misure di sicurezza (in gergo detti *controlli*).



Questo ISMS viene continuamente migliorato attraverso un modello PDCA - *Plan Do Check Act*

In questo ambito parleremo di:

- **Asset:** qualunque bene o entità che può avere un valore per l'organizzazione
- **Sicurezza delle Informazioni:** confidenzialità ed integrità.
- **Controlli:** mezzi per gestire e limitare il rischio
- **Minacce (threats):** eventi possibili con un impatto

Ogni fase di *Plan Do Check Act* ha delle sottofasi.

Il Plan (Pianificazione) è diviso in 6 sotto-fasi:

1. Definire il perimetro
    a. Perimetro fisico, Anagrafica degli asset, Risorse tecnologiche …
2. Scrivere una politica dell'ISMS
    a. Principi Strategici Generali, Obblighi contrattuali e vincoli …
3. Analizzare e valutare il rischio
    a. Asset, minacce, impatti, contromisure…
4. Trattare (Pianificare) il rischio
    a. Implementare difese, Accettare alcuni rischi, Trasferire i rischi a terzi …
5. Ottenere approvazione ed autorizzazione
    a. Accettazione del rischio residuo, Implementazione dei controlli …
6. Redigere lo "Statement of Applicability"
    a. Documento dettagliato sull'applicazione dei controlli di sicurezza e la loro pertinenza rispetto a uno standard o una norma specifica

Il Do (Implementazione) è diviso in 5 sotto-fasi:

1. Realizzare i controlli selezionati
2. Misurare l'efficienza dei controlli realizzati
3. Attuare un piano di formazione
4. Gestire l'operatività dei controlli e la loro manutenzione

Il Check (Monitoraggio) è diviso in 3 sotto-fasi:

1. Monitoraggio per rilevare problemi
    a. Rilevare errori, incidenti di sicurezza …
2. Riesame proattivo
3. Riesame della valutazione dei rischi residui

L'ACT (Miglioramento) è diviso in 3 sotto-fasi:

1. Identificare miglioramenti
2. Attuare miglioramenti
3. Verifica dei miglioramenti