I sistemi di gestione integrati aziendali: sinergie evoluzioni, opportunità

Secondo la nuova norma ISO/IEC 27001

Prepared by Adriano Russo

Membro Comitato AIAS C.2.1 Sistemi di Gestione

5 novembre 2021

ing.adrianorusso@gmail.com

EPC EDITORE

aias dal 1975 networkaias

PREMESSA

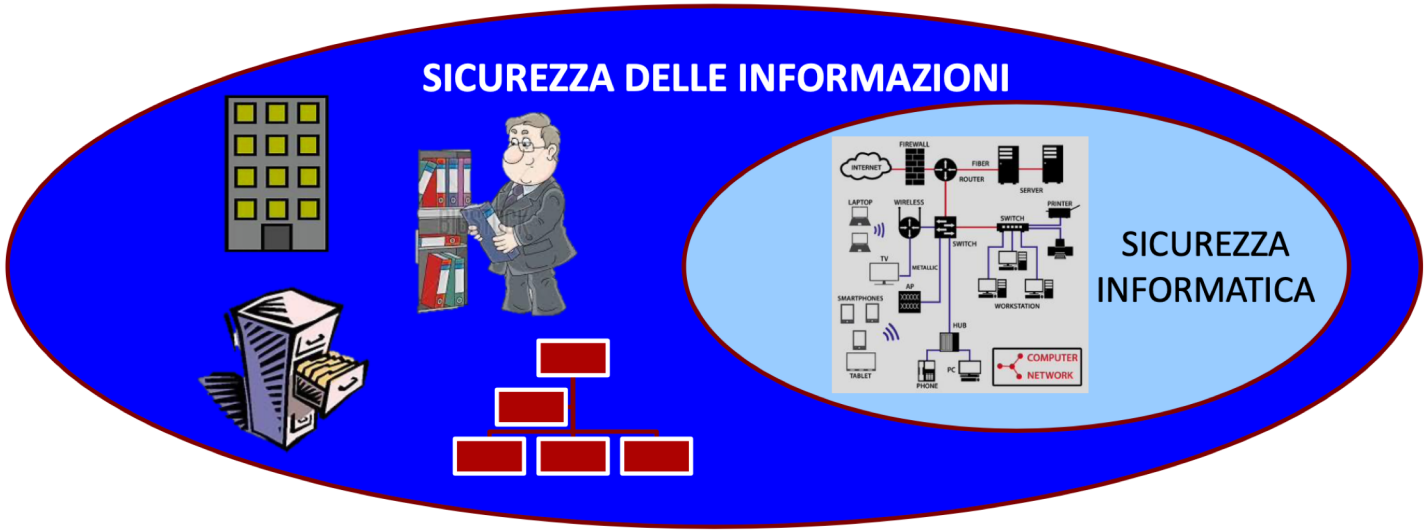
La GO integra in un "*Sistema di Gestione Aziendale*“ le principali norme in tema di salute, sicurezza, ambiente e qualità oltre che al MOG ai sensi del D.Lgs 231/01 altre norme diffuse nelle aziende quali:

- UNI 37001: 2016 *Sistemi di gestione per la prevenzione e la corruzione*;
- UNI CEI EN ISO/IEC 27001:2017 – *Tecnologie Informatiche – Tecniche di sicurezza – Sistemi di gestione della sicurezza e dell’informazione*;
- UNI EN ISO 22301: 2019 – *Sicurezza e resilienza - Sistemi di gestione per la continuità operativa*;
- UNI ISO 26001: 2010 *Guida alla responsabilità sociale*.

Ogni organizzazione deve essere in grado di garantire la sicurezza dei propri dati da crimini e attacchi informatici.

L'obiettivo dello standard ISO 27001 è quello di proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità.

Sicurezza delle informazioni (Information security): preservazione della riservatezza, integrità e disponibilità delle informazioni



Le informazioni custodite con mezzi informatici rappresentano un patrimonio aziendale la cui gestione diventa strategia per la tutela e lo sviluppo aziendale. Si tratta di garantire:

Riservatezza;

Integrità;

Accessibilità..

Esempi di incidenti

Esempi di incidenti	R	I	D
Guasto impianti tecnologici			X
Furto di password	X	X	X
Incendio		X	X
Diffusione non autorizzata dei documenti	X		
Spionaggio industriale	X		
Attacco ai sistemi informatici	X	X	X
Intrusione fisica in strutture ad accesso riservato	X	X	X

- Secondo la norma ISO 27001 la sicurezza viene vista come un processo indipendente dalla tecnologia.

- La sicurezza deve coprire tutti i processi che impattano sulle caratteristiche di security del prodotto o servizio immesso sul mercato.

- ISO 27001 è una norma internazionale che definisce i requisiti per impostare, gestire e migliorare un Sistema di Gestione sulla Sicurezza delle Informazioni e include una serie di controlli (requisiti) relativi alla sicurezza logica, fisica e organizzativa.

L'obiettivo principale dello standard ISO 27001 è proprio quello di garantire la protezione dei dati e delle informazioni da minacce di ogni tipo, al fine di

- assicurarne l'integrità;
- la riservatezza;
- e la disponibilità;
- e fornire i requisiti per realizzare un sistema di gestione della sicurezza delle informazioni adeguato alla corretta gestione dei dati critici dell'azienda.

Occorre un sistema di gestione più ampio della sicurezza delle informazioni che contribuisca alla

- creazione di valore
- ed implicito sviluppo
- e l'applicazione di policy aziendali
- e di procedure per possibili situazioni di rischio, permettendo così un adeguato controllo della sicurezza e una difesa da possibili minacce.

La sicurezza informatica riguarda tutti i settori economici e molti degli aspetti della vita quotidiana:

- dai gravi incidenti causati da carenti misure di sicurezza in fase di progettazione;
- collaudo ed esercizio di importanti infrastrutture di trasporto;
- all'e-commerce;
- la digitalizzazione dei processi aziendali e della PA;
- la sanità.

- La norma ISO 27001 può essere utilizzata da qualsiasi impresa (pubblica o privata, profit o noprofit, culturale o sociale, collettiva o individuale) che intende gestire i rischi relativi alla sicurezza delle informazioni.
- La norma è applicabile alle organizzazioni nella gran parte dei settori commerciali e industriali, come finanza e assicurazioni, servizi, trasporti, settori governativi e comunque a tutte quelle aziende che forniscono servizi informatici (sia all'interno che all'esterno dell'organizzazione).

Vantaggi di chi si certifica

- Soddisfacimento dei requisiti per la partecipazione a bandi gara;
- Conseguimento di vantaggi di natura interna (qualità e sicurezza dei processi aziendali) o esterna (competitività sul mercato);
- Minimizzazione di possibili sanzioni a fronte di violazioni di compliance;
- Possibile riduzione del premio relativo a polizza assicurative;
- Miglioramento dell'immagine verso gli stakeholders (clienti, azionisti, parti sociali);
- Motivazione e crescita professionale dei dipendenti

Vantaggi di chi si certifica

- Rafforzare le interfunzionalità delle sicurezza delle informazioni e la fiducia dei propri Partner commerciali;
- Integrare la sicurezza delle informazioni e dei sistemi nella strategia globale di gestione del rischio dell'Organizzazione;
- Soddisfare le richieste degli Stakeholders (azionisti, legislatore, clienti, personale amministrazione e comunità, dimostrando di affrontare e gestire il rischio, garantendo la sostenibilità del business;

Vantaggi di chi si certifica

- Ridurre gli incidenti che comportano responsabilità legali e contrattuali;
- Migliorare l'organizzazione e la consapevolezza dell'importanza della sicurezza delle informazioni;
- Assicurare la protezione di segreti commerciali, del know-how aziendale, della privacy garantendo il rispetto delle norme legislative e la sicurezza delle informazioni.

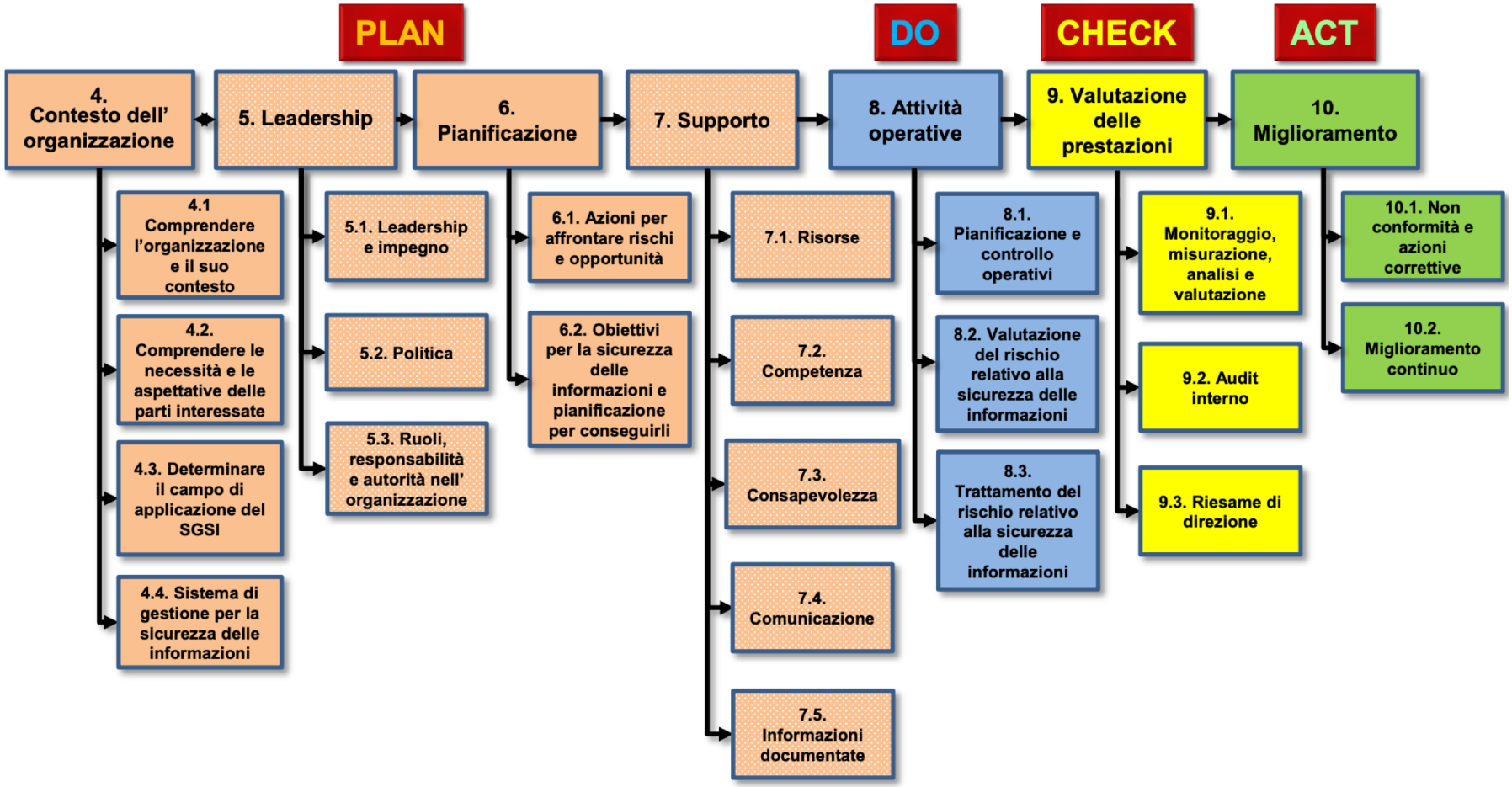
Vantaggi di chi si certifica

- Garanzia di immediata disponibilità, affidabilità e integrità delle informazioni, assicurando la protezione di segreti commerciali e del know-how aziendale;
- Attuazione sistematica della politica di gestione della sicurezza delle informazioni;
- Gestione a livello aziendale dei rischi correlati alle informazioni;

Vantaggi di chi si certifica

- Monitoraggio efficace e continuo miglioramento del livello di sicurezza;
- Assicurazione di conformità ai requisiti di legge e contrattuali;
- Promozione di un atteggiamento più fiducioso nel contatto e nelle relazioni con i propri clienti

INDICE


PLAN
DO
CHECK
ACT
4. Contesto dell' organizzazione
5. Leadership
6. Pianificazione
7. Supporto
8. Attività operative
9. Valutazione delle prestazioni
10. Miglioramento
4.1 Comprendere l'organizzazione e il suo contesto
4.2. Comprendere le necessità e le aspettative delle parti interessate
4.3. Determinare il campo di applicazione del SGSI
4.4. Sistema di gestione per la sicurezza delle informazioni
5.1. Leadership e impegno
5.2. Politica
5.3. Ruoli, responsabilità e autorità nell' organizzazione
6.1. Azioni per affrontare rischi e opportunità
6.2. Obiettivi per la sicurezza delle informazioni e pianificazione per conseguirli
7.1. Risorse
7.2. Competenza
7.3. Consapevolezza
7.4. Comunicazione
7.5. Informazioni documentate
8.1. Pianificazione e controllo operativi
8.2. Valutazione del rischio relativo alla sicurezza delle informazioni
8.3. Trattamento del rischio relativo alla sicurezza delle informazioni
9.1. Monitoraggio, misurazione, analisi e valutazione
9.2. Audit interno
9.3. Riesame di direzione
10.1. Non conformità e azioni correttive
10.2. Miglioramento continuo

La versione in vigore dello standard ISO 27001 include l'Annex A .

L'Annesso A risulta particolarmente utile e importante. Contiene i controlli, cioè il catalogo delle contromisure, un elenco di controlli a cui l'azienda che intende applicare la norma deve attenersi, raggruppati in obiettivi e aree di controllo.

Appendice A Obiettivi di controllo e controlli di riferimento

A.5 Politiche per la sicurezza delle informazioni_**A.5.1** Indirizzi della direzione per la sicurezza delle informazioni;

A.6 Organizzazione della sicurezza delle informazioni_**A.6.1** Organizzazione interna; **A.6.2** Dispositivi portatili e telelavoro;

A.7 Sicurezza del personale_**A.7.1** Prima dell'impiego; **A.7.2** Durante l'impiego; **A.7.3** Cessazione e variazione del rapporto di lavoro

A.8 Gestione degli Asset aziendali_**A.8.1** Responsabilità per gli asset; **A.8.2** Classificazione delle informazioni_**A.8.3** Trattamento dei supporti;

Appendice A Obiettivi di controllo e controlli di riferimento

A.9 Controllo degli accessi_**A.9.1** Requisiti di business per il controllo degli accessi; **A.9.2** Gestione degli accessi degli utenti; **A.9.3** Responsabilità dell'utente; **A.9.4** Controllo degli accessi ai sistemi e alle applicazioni

A.10 Crittografia_**A.10.1** Controlli crittografici;

Appendice A Obiettivi di controllo e controlli di riferimento

A.11 Sicurezza fisica e ambientale_**A.11.1** Aree sicure_**A.11.2** Apparecchiature.

A.12 Sicurezza delle attività operative_**A.12.1** Procedure operative e responsabilità_**A.12.2** Protezione dal malware; **A.12.3** Backup; **A.12.4** Raccolta di log e monitoraggio; **A.12.5** Controllo del software e di produzione_**A.12.6** Gestione delle vulnerabilità teniche_**A.12.7** Considerazioni sull'audit dei sistemi informativi;

Appendice A Obiettivi di controllo e controlli di riferimento

A.13 Sicurezza delle comunicazioni_ **A.13.1** Gestione della sicurezza della rete_**A.13.2** Trasferimento delle informazioni;

A.14 Acquisizione, sviluppo e manutenzione dei sistemi_**A.14.1** requisiti di sicurezza dei sistemi informativi_**A.14.2** Sicurezza nei processi di sviluppo e supporto_**A.14.3** Dati di test;

Appendice A Obiettivi di controllo e controlli di riferimento

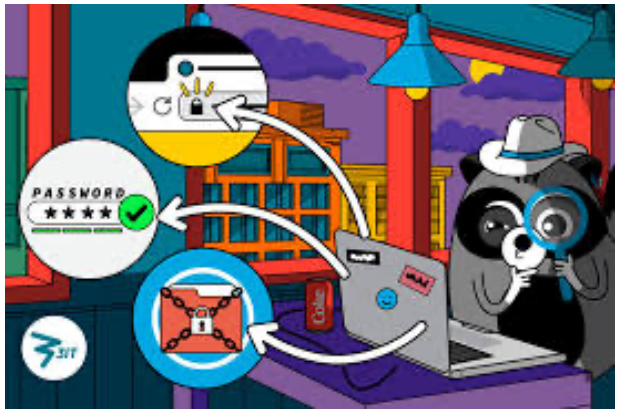
A.15 Relazioni con i fornitori_**A.15.1** Sicurezza delle informazioni nelle relazioni con i fornitori_**A.15.2** gestione dell'erogazione dei servizi dei fornitori;

A.16 Gestione degli incidenti relativi alla sicurezza delle informazioni_**A.16.1** gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramen

Appendice A Obiettivi di controllo e controlli di riferimento

A.17 Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa_**A.17.1** Continuità della sicurezza delle informaizioni_**A.17.2** Ridondanze;

A.18 Conformità_**A.18.1** Conformità ai requisiti cogenti e contrattuali_**A.18.2** Riesami della sicurezza delle informazioni.



ANALISI DELLE VULNERABILITA' E PENETRATION TEST

L'Analisi delle Vulnerabilità e i Penetration Test rientrano nel controllo **A.12.6** Gestione delle vulnerabilità tecniche della norma ISO 27001 e sono strettamente correlate con la valutazione del rischio in quanto consentono:

- Di individuare le vulnerabilità delle reti, delle applicazioni web o dei dispositivi interni;
- Di contribuire al trattamento del rischio;
- Di contribuire al miglioramento continuo.

Differenza tra Analisi delle Vulnerabilità e Penetration Test

L'Analisi delle Vulnerabilità è un test superficiale ma ampio teso a identificare tutte le problematiche gravi e note (ad esempio, mancanza di patch, errori di configurazione più diffusi, vulnerabilità macroscopiche, ecc). È un vero e proprio check-up dei sistemi informativi e mira a far emergere possibili vulnerabilità dell'infrastruttura e della rete IT.

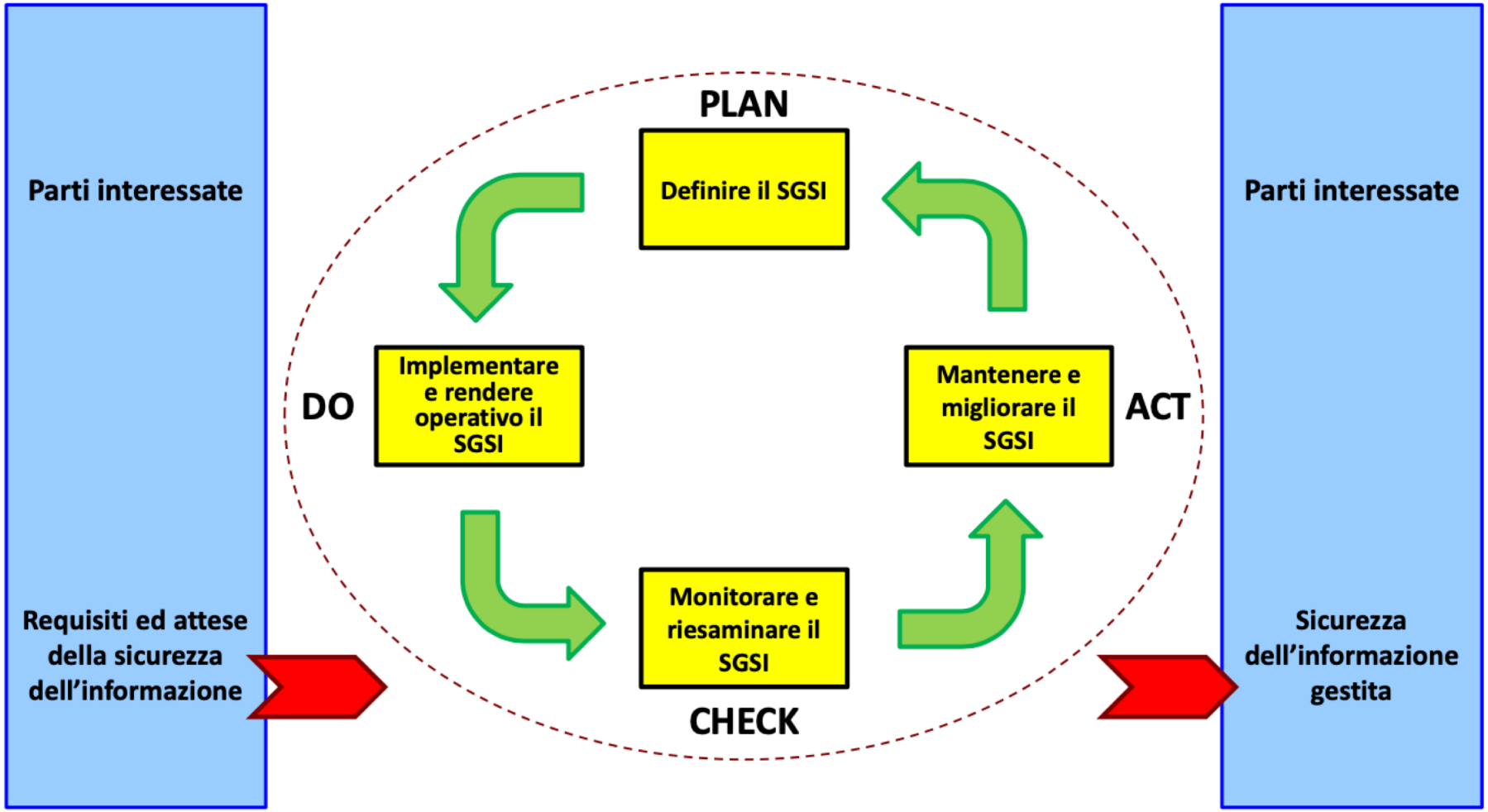
OBIETTIVO: Identificare quali parti del sistema risultano deboli a livello di sicurezza.

Differenza tra Analisi delle Vulnerabilità e Penetration Test

Il Penetration Test è un vero e proprio attacco informatico controllato al sistema informatico e sfrutta una e una sola vulnerabilità di sistema, la più efficace e diretta per riuscire a bucare la rete.

OBIETTIVO: dimostrazione pratica dell'esistenza e delle conseguenza di una particolare vulnerabilità.

Schema del modello di gestione (PDCA)

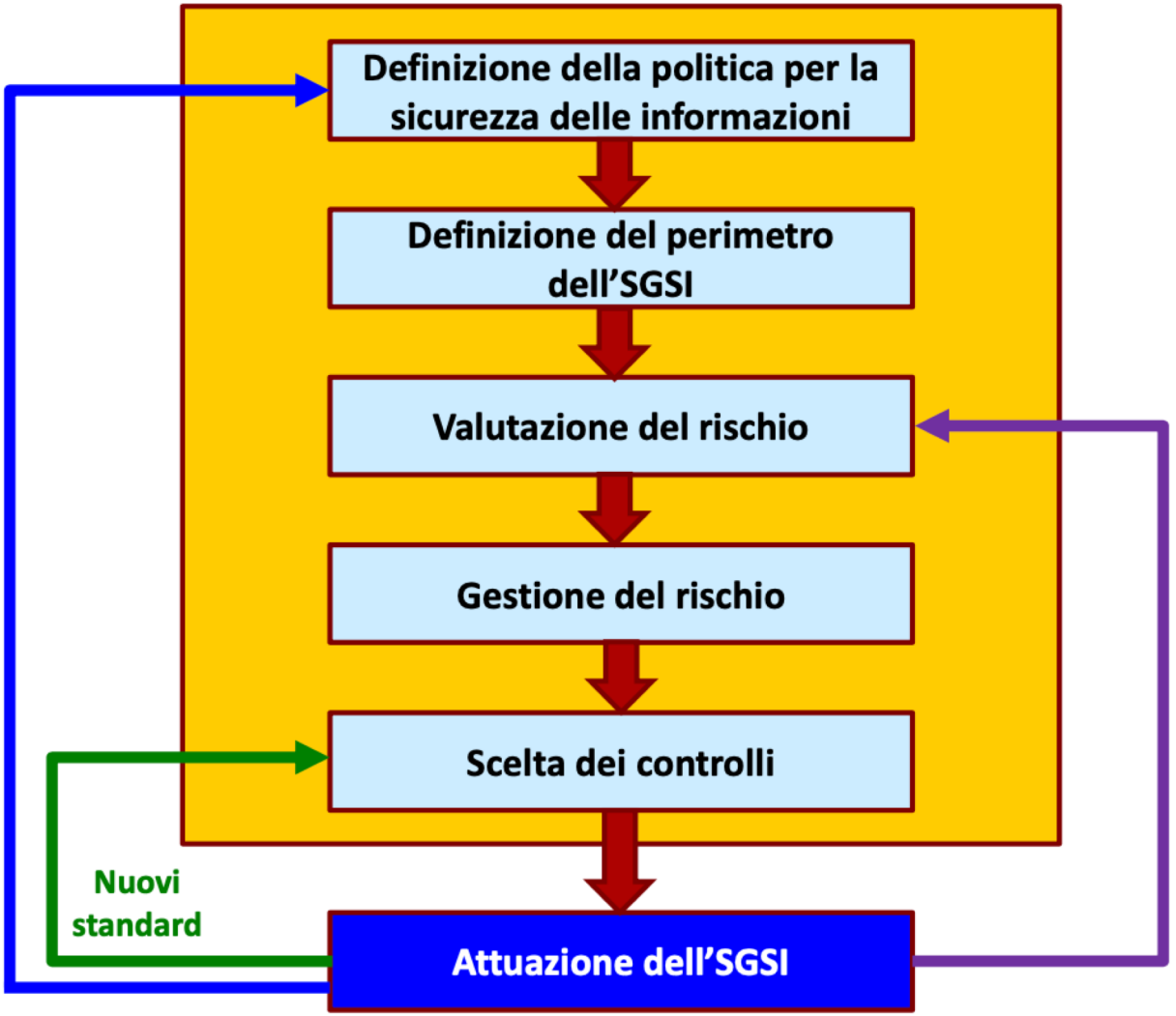


PLAN	DO
Definizione dell'ambito di applicazione del SGSI	Formulazione di un piano di trattamento dei rischi
Definizione di una politica di sicurezza di alto livello	Implementazione del piano
Definizione di un approccio sistematico per l'analisi dei rischi	Implementazione delle contromisure selezionate
Identificazione dei rischi	Svolgimento dei programmi di informazione e formazione

PLAN	DO
Valutazione dei rischi	Gestione delle operazioni connesse con la fase
Identificazione delle opzioni per il trattamento (eliminazione, cessione, riduzione, accettazione) dei rischi	Implementazione di procedure e altre misure che assicurino la rilevazione e le opportune azioni in caso di incidenti relativi alla sicurezza
Selezione delle contromisure per il controllo dei rischi	
Redazione della dichiarazione di applicabilità, comprendente l'esplicitazione delle ragioni che hanno portato alla selezione delle contromisure e alla non applicazione di misure indicate nell'Appendice A della norma	

CHECK	ACT
Esecuzione delle procedure di monitoraggio del SGI	Implementazioni delle azioni migliorative del SGSI identificate
Esecuzione di revisioni per l'accertamento del rischio residuo	Implementazione delle azioni correttive e preventive
Conduzione di audit interni al SGSI	Comunicazione dei risultati
Esecuzione di review al massimo livello dirigenziale del SGSI	Verifica che i miglioramenti raggiungano gli obiettivi identificati alla loro base
Registrazione delle azioni e degli eventi che potrebbero avere impatti sulla sicurezza o sulle prestazioni del SGSI	

CICLO DI VITA DI UN SGSI: ISO/IEC 27001

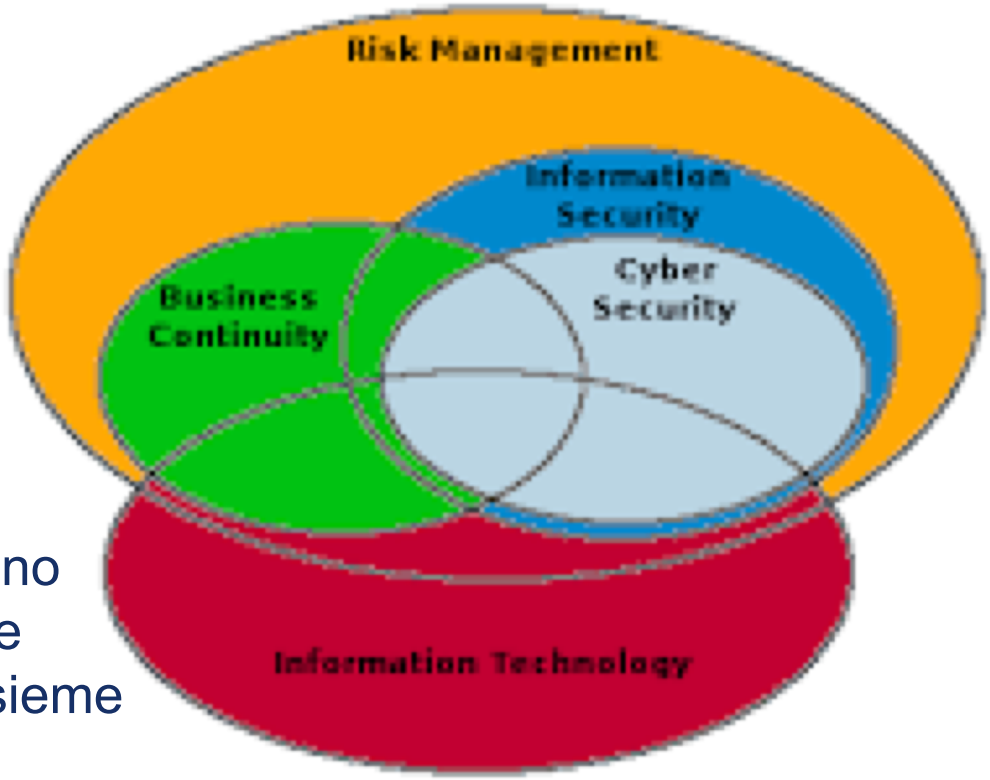


Alcuni aspetti qualificanti della norma ISO/IEC 27001

Gestione del Rischio

La ISO/IEC 27001 si basa sulla gestione del rischio relativo alla sicurezza delle informazioni. Uno dei modi più diretti per effettuare un trattamento del rischio è quello di ridurlo ad un livello accettabile adottando opportuni controlli di sicurezza.

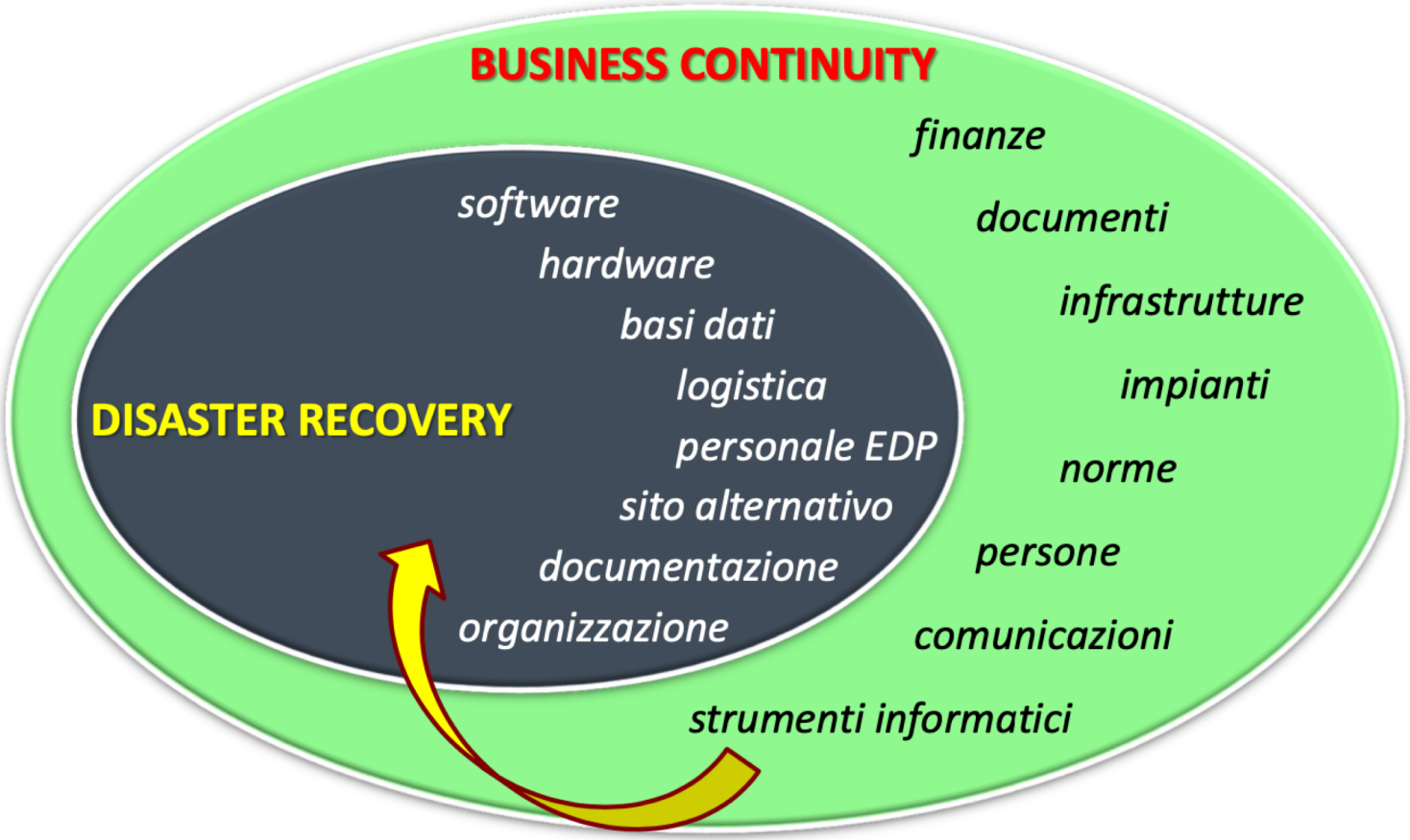
BUSINESS CONTINUITY E DISASTER RECOVERY



La Business Continuity (BC) è la capacità di un'organizzazione di mantenere la funzionalità operativa a seguito di eventi che ne minaccino le funzionalità a qualunque livello, non solo tecnologico.

Nel caso di eventi che compromettano l'infrastruttura tecnologica interviene il Disaster Recovery (DC) che è l'insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business.

Differenza tra Business Continuity e Disaster Recovery



SGSI ISO 27001 e GDPR

- ❑ Valutazione del rischio
- ❑ Conformità
- ❑ Notifica delle violazioni
- ❑ Gestione degli asset
- ❑ Privacy by design
- ❑ Rapporti con i fornitori

Thank you

Adriano Russo

ing.adrianorusso@gmail.com