**Piano di Sicurezza Informatica**

**Inquadramento normativo**

Il **Piano di Sicurezza Informatica** è previsto dalle **Linee Guida AgID**, in attuazione del **Codice dell’Amministrazione Digitale (D.Lgs. 82/2005)** e del **Regolamento UE 2016/679 (GDPR)**.  
Costituisce parte integrante del sistema di gestione della sicurezza ICT per le organizzazioni pubbliche e private, con l’obiettivo di tutelare dati, servizi e infrastrutture critiche.

Il Piano:

* identifica i rischi,
* definisce le misure di protezione,
* stabilisce le politiche di sicurezza adeguate per garantire la protezione dei dati personali e la resilienza dei sistemi informativi.

**Il valore aggiunto: la figura del CISO**

Marco La Diega srl mette a disposizione una figura professionale **CISO (Chief Information Security Officer)** certificata, con esperienza specifica nella Pubblica Amministrazione e nel settore privato.

Il **CISO** offre:

* Supervisione e validazione del Piano di Sicurezza Informatica.
* Definizione della strategia di sicurezza ICT a medio-lungo termine.
* Coordinamento nella gestione di incidenti e nella risposta agli attacchi informatici.
* Consulenza per la protezione di dati sensibili e infrastrutture critiche.
* Supporto nella gestione della compliance normativa (GDPR, CAD, NIS2, AgID).
* Formazione del personale su temi di sicurezza informatica e gestione dei rischi.
* Affiancamento nei rapporti con l’Agenzia per la Cybersicurezza Nazionale (ACN) e altri enti di controllo.

Grazie al coinvolgimento diretto del **CISO**, il servizio garantisce non solo la conformità normativa, ma anche l’adozione di best practice di sicurezza riconosciute a livello internazional

**Obiettivo del Servizio**

Fornire assistenza qualificata per l’elaborazione e l’adozione di un **Piano di Sicurezza Informatica** personalizzato, in grado di garantire:

* la protezione dei dati e dei sistemi,
* la riduzione dei rischi residui,
* la continuità operativa,
* la conformità ai requisiti di privacy e sicurezza.

Il Piano è basato su un’analisi dei rischi che coinvolge infrastrutture, dati, documenti e procedure, tenendo conto delle direttive strategiche dell’organizzazione.

**Attività Previste**

Il servizio comprende:

* Censimento degli asset hardware e software.
* Verifica della continuità operativa e dei piani di disaster recovery.
* Controllo dell’infrastruttura fisica.
* Monitoraggio e tracciamento dei log di sistema.
* Gestione delle responsabilità e delle procedure in caso di incidente.
* Analisi delle modalità di conservazione dei documenti.
* Redazione e aggiornamento del Piano di Sicurezza Informatica.

**Aree di Intervento**

* Analisi preliminare dei fabbisogni e delle criticità.
* Raccolta dati sulla struttura organizzativa e sui sistemi IT.
* Definizione di misure preventive e correttive.
* Pianificazione della gestione degli incidenti.
* Controllo dei livelli di sicurezza fisica e logica.
* Verifica della conformità alle normative vigenti (CAD, GDPR, Linee Guida AgID).
* Supporto nella redazione e approvazione del Piano.

**Modalità di Erogazione**

* Analisi iniziale e raccolta dati.
* Redazione della bozza del Piano.
* Condivisione e approvazione con l’organizzazione.
* Incontri operativi (in presenza o da remoto) secondo un calendario definito.
* Possibilità di aggiornamento periodico del Piano in base all’evoluzione tecnologica e normativa.

**Output del Servizio**

* Piano di Sicurezza Informatica completo, aggiornato e conforme.
* Identificazione e valutazione dei rischi.
* Definizione di misure di sicurezza preventive e correttive.
* Miglioramento della resilienza dei sistemi e dei servizi.
* Riduzione del rischio di incidenti e sanzioni.
* Allineamento con le migliori pratiche e le normative vigenti.

**Destinatari**

* Pubbliche Amministrazioni.
* Enti e istituzioni pubbliche e private.
* Organizzazioni con sistemi informativi critici o trattamento di dati personali.

**Il metodo OLTRECODE**

Anche per il **Piano di Sicurezza Informatica** adottiamo il metodo **OLTRECODE**, che garantisce:

* Contatto costante e diretto con il cliente.
* Affiancamento operativo e non formale.
* Soluzioni personalizzate in base alla struttura e ai rischi specifici dell’organizzazione.
* Risposte tempestive e supporto continuativo per tutta la durata dell’incarico.

Non solo un documento formale, ma uno **strumento operativo e strategico** per la sicurezza e la resilienza digitale dell’organizzazione.

**Affidati a Marco La Diega srl per la redazione e la gestione del tuo Piano di Sicurezza Informatica, con l’affiancamento di un CISO qualificato e un approccio pratico e conforme alle normative vigenti.**  
Contattaci per maggiori informazioni: **supporto@marcoladiega.it**