MISURE MINIME DI SICUREZZA ICT
PER LE PUBBLICHE AMMINISTRAZIONI

(Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015)

AG.I.D.
AGENZIA PER L'ITALIA DIGITALE

Fonte: circolare AgID 1/2017 pubblicata in Gazzetta Ufficiale

La nuova Circolare AgID 1/2017, pubblicata in Gazzetta Ufficiale il 17.03.2017, con successivo adeguamento del 18.04.2017 nr. 2/2017, contiene tutte le misure minime di sicurezza ICT per le Pubbliche Amministrazioni, basata sulla "*Direttiva del Presidente del Consiglio dei ministri del 1° agosto 2015"*, la quale impone ad ogni Pubblica Amministrazione rientrante nella definizione ex. art. 1 c.2 d.Lgs. 165/2001 di attestare il livello di adozione delle misure minime di sicurezza del proprio Sistema Informatico al fine di conservare tale attestazione da trasmettere al CERT-PA (l'acronimo di Computer Emergency Response Team Pubblica Amministrazione) in caso di incidente informatico.

La responsabilità di attuazione delle misure minime è in capo al responsabile dei sistemi informativi (definito all'art. 10 del D.Lgs. 39/1993) o, in sua assenza, al dirigente allo scopo designato che deve applicare tutte le misure minime di sicurezza adottate da AgiD, mentre il responsabile deve attestare il livello di adozione delle misure minime compilando il modulo di implementazione ABSC (Agid Basic Security Control(s))

Il modulo deve essere compilato dal responsabile e dal responsabile legale della struttura, oltre che marcato temporalmente (NB si parla di marcatura temporale, non di riferimento temporale, per cui il numero di protocollo non è idoneo; la marcatura temporale viene apposta direttamente sul documento).

La scadenza di prima adozione di tale adempimento è il 31/12/2017; c'è da osservare che, essendo il sistema informatico soggetto a continue evoluzioni, la misura di adozione potrebbe essere aggiornata anche in data successiva a tale scadenza. Sarà pertanto necessario implementare un processo opponibile a terzi di versioning di tale documento.

Le misure di sicurezza si sviluppano su 3 livelli:

- "Minimo", al di sotto il quale nessuna amministrazione può scendere;
- "Standard", che costituisce la base di riferimento nella maggior parte dei casi;
- "Alto", che potrebbe essere un obiettivo a cui tendere.

Il responsabile quindi dovrà adottare almeno le misure di livello minimo e tendere a rendere il sistema sicuro a seconda della propria situazione contingente: quello che nel codice della privacy (D. Lgs. 196/2003) si definisce "misure idonee di sicurezza".

Questo adempimento è propedeutico alla comunicazione, in caso di eventuale incidente informatico, a CERT-PA del documento sottoscritto allegato alla segnalazione dell'incidente stesso. E' importante rilevare che, **in caso di** *data breach* (cioè di violazioni di sicurezza) **di dati personali, è obbligatoria la segnalazione al garante della Privacy**: quando il nuovo regolamento Europeo di protezione dei dati personali verrà interamente applicato (la scadenza ultima è maggio 2018), il Garante svolgerà delle **ispezioni presso l'ente che ha subito l'attacco – al fine di verificare le misure di sicurezza adottate – ed eventualmente comminare delle sanzioni**, che possono essere molto salate. L'obiettivo degli enti dovrebbe essere quello di **non ripetere adempimenti simili, implementando un Sistema di Gestione della Sicurezza** in grado di ottemperare in maniera efficiente a tutti gli obblighi di legge.

L'esperienza pluriennale nel campo della sicurezza informatica e della normativa ICT, può **affiancare qualsiasi tipo di ente nel percorso di messa in sicurezza dei propri sistemi**

In questo quadro diviene fondamentale effettuare una attività specifica di consulenza ICT al fine di effettuare una discovery sul sistema informatico e, una volta identificate le anomalie/problematiche, i nostri consulenti con uno specifico intervento tecnico od organizzativo applicano gli interventi per contrastare e ridurre gli effetti di una specifica minaccia informatica. Successivamente dopo l'applicazione degli opportuni adeguamenti viene redatto il modulo, che deve essere compilato e firmato digitalmente con marcatura temporale dal Responsabile dei Sistemi Informativi di cui all'art. 10 del D.Lgs. 12/02/1993, n. 39, ovvero, in sua assenza, dal Dirigente allo scopo designato e dal Responsabile Legale della struttura. *Dopo la sottoscrizione, il modulo deve essere conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente.*

Le attività ICT previste nella nostra consulenza si basano su otto classi di intervento:

- ***ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI***
  - *Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso*
- ***ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI***
  - *Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione*
- ***ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI , LAPTOP , WORKSTATION E SERVER***
  - *Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.*
- ***ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ***
  - *Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.*
- ***ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE***
  - *Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.*
- ***ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE***
  - *Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.*
- ***ABSC 10 (CSC 10): COPIE DI SICUREZZA***
  - *Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.*
- ***ABSC 13 (CSC 13): PROTEZIONE DEI DATI***
  - *Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni*

CONTATTAMI PER RICEVERE TUTTE LE INFORMAZIONI COMMERCIALI DELLA PROPOSTA DI CONSULENZA

Scrivi a: contact@marcomoretti.net