Consiglio Nazionale dei Dottori Commercialisti ed Esperti Contabili

(CNDCEC)

SECURITY POLICY della CA

obiettivi del CNDCEC per la sicurezza e la strategia di gestione concordata per la sicurezza delle informazioni.

Obiettivi della CA

Il CNDCEC, in continuità con quanto avviato con la precedente autorità di certificazione ha stabilito i presupposti del nuovo progetto che si basa sugli stessi obiettivi qualificanti:

- Mantenimento dell'Autorità di Certificazione Autonoma accredita presso l'AGid
- Inserimento all'interno del Certificato di sottoscrizione del Ruolo Professionale (come previsto dall'Art. 2 della finanziaria 2004)
- Emissione smart card in formato tesserino dell'Ordine con presenza della banda magnetica utilizzabile per applicazioni specifiche (es. rilevazione presenze ai corsi).
- Punto di riferimento del professionista rimane l'Ordine di appartenenza, il quale sancirà, tramite il suo Presidente, l'iscrizione del professionista iscritto all'albo e la permanenza dei requisiti professionali per esercitare la professione.

Nel panorama di misure adeguate definite nell'art. 32 del Regolamento U.E. 27 aprile 2016 n.679 anche se non meglio precisate sul piano tecnico, già da tempo il CNDCEC ha adottato delle normative interne – comunemente denominate policy di sicurezza o security policy – che indicano le misure organizzative e quali comportamenti debbano essere tenuti da dipendenti e collaboratori per contrastare i rischi informatici.

L'atteggiamento imprudente nell'uso di internet, di workstation e di smartphone aziendali può mettere a serio rischio tutta la struttura, con blocchi di produttività e, ora più che mai, di data breach. Non è sufficiente quindi studiare un piano di difesa informatica se un operatore disattende le procedure di sicurezza accettando volontariamente di eseguire un allegato di posta elettronica o aprire un improbabile file.
La sicurezza informatica scaturisce prima di tutto da una corretta percezione dei dipendenti e, in generale, da tutti coloro che utilizzano i servizi tecnologici messi a disposizione.

La sensibilizzazione deve ottenere un effetto formativo

Molta attenzione deve essere riposta nelle cautele volte a:

- mantenere segrete le proprie credenziali di accesso (password e/o pin);

- non lasciare libero accesso ai propri dispositivi in caso di assenza momentanea dalla propria postazione lavorativa;
- controllare l'accesso ad internet ed ai servizi di posta elettronica;
- verificare la presenza di eventuali tracce malevoli prima di utilizzare supporti rimovibili, quali pendrive e memory card;
- curare l'osservanza di backup periodici;
- evitare per l'uso di dispositivi aziendali al di fuori dell'ambito lavorativo.
- ecc.

Security Policy

La CA del CNDCEC mediante la propria organizzazione e tramite l'affidamento in outsourcing ad un fornitore qualificato dei sevizi erogati dalla CA, intende garantire:

- la riservatezza: proprietà per cui l'informazione non è resa disponibile o rivelata a individui, entità o processi non autorizzati;
- l'integrità: proprietà relativa alla salvaguardia dell'accuratezza e della completezza delle informazioni e dei beni ad esse collegati;
- la disponibilità: proprietà di essere accessibile e utilizzabile su richiesta di un'entità autorizzata.

A tale scopo sono stati definiti:

- le persone, le quali devono essere consapevoli del loro ruolo al fine di garantire la sicurezza delle informazioni;
- i processi, che devono essere conosciuti, mappati e analizzati in termini di opportunità e rischi;
- le tecnologie, che devono essere gestite e mantenute.

Al Fornitore a cui viene demandata l'erogazione dei servizi della CA in outsourcing:

- Impostazione del progetto di implementazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) al fine di determinare l'entità e le criticità del sistema di gestione e di definire le priorità, i tempi, i ruoli e le responsabilità.
- Definizione politica e contesto al fine di definire gli obiettivi di sicurezza e la definizione dettagliata del campo di applicazione in relazione al contesto interno ed esterno di riferimento
- L'analisi dello stato attuale dell'organizzazione che consente di individuare i requisiti contrattuali e normativi e le risorse informative da prendere in considerazione.
- Risk assessment per l'analisi, la valutazione e la pianificazione del trattamento dei rischi e la selezione delle contromisure rilevanti coerentemente con le linee guida riportate dalle norme ISO/IEC 27005:11 – ISO 31000. Tale analisi viene svolta sulla base degli obiettivi strategici, della politica e del campo di applicazione definiti.
- Implementazione del Sistema di gestione della sicurezza delle informazioni attraverso le attività di formazione continua, monitoraggio, misurazione audit interni, formazione e consapevolezza, gestione incidenti, riesami della direzione, miglioramento del sistema.

7 maggio 2018