CONTRATTI PER LA SICUREZZA INFORMATICA

(a cura di **Avv. Antonino ATTANASIO**)

INDICE DELLA PRESENTAZIONE :

Capitolo 1

Gli aspetti di sicurezza coinvolgono tutti i settori dell'informatica:

- **sicurezza logica**, volta a proteggere risorse informatiche e dati, tramite la definizione e l'implementazione di misure di carattere tecnico preventivo, supportate da adeguate procedure di configurazione e gestione;
- **sicurezza fisica**, intesa come insieme di caratteristiche e procedure per la salvaguardia delle infrastrutture utilizzate (edifici, locali, strumentazioni, ecc.);
- **sicurezza organizzativa** volta a proteggere risorse informatiche e dati attraverso la definizione di modelli di governance, l'adeguamento dei processi organizzativi agli standard di sicurezza, e l'avvio di piani di formazione per lo sviluppo delle competenze

Capitolo 1

Quanto al contenuto della sicurezza informatica, occorre adottare concretamente misure atte a:

1. **garantire la disponibilità** delle risorse, compresi i dati allorché conoscibili, e dei servizi del sistema informatico;
2. **impedire attacchi** rivolti a violare la riservatezza dei dati e delle informazioni, consentendone la fruizione soltanto a persone o sistemi informatici autorizzati;
3. **assicurare l'integrità** dei dati e delle informazioni e più in generale delle risorse, non consentendo modifiche non autorizzate.

Capitolo 1

Information security

insieme delle misure, di natura tecnologica, organizzativa e legale, volte a impedire o comunque ridurre al minimo i danni causati da eventi intenzionali (crimini, frodi) o non intenzionali (errori umani, fenomeni naturali) che violano la confidenzialità, l'integrità e la disponibilità del patrimonio informativo aziendale, indipendentemente dal modo in cui tali informazioni siano comunicate, e dal supporto fisico sul quale siano custodite.

Capitolo 1

Ict security

Ict security per essere completa deve tenere conto non solo della protezione, intesa come confidenzialità, integrità e disponibilità, del dato elementare e delle informazioni proprietarie dell'organizzazione, **ma anche della protezione delle infrastrutture e delle applicazioni Ict da attacchi o manomissioni che ne possano compromettere il regolare funzionamento**.

Capitolo 1

Ict security Governance

i responsabili dell'Ict security devono quindi garantire la giusta componente di security in ogni progetto in cui si faccia uso di soluzioni Ict e quindi, considerata la sempre maggiore pervasività dell'Ict, praticamente in tutte le attività aziendali.

Capitolo 1

Ict security Governance

obiettivo dell'Ict security governance è quello di dotare l'impresa di:

• **una strategia di Ict security ben definita, e collegata agli obiettivi di business, nonché a quelli dell'Ict;**

• **una struttura organizzativa congruente con gli obiettivi, la tipologia di attività e il carico di lavoro previsto;**

• **meccanismi di pianificazione e controllo**;

• metodologie di risk analysis/management appropriate;

• adeguate policy che comprendano tutti gli aspetti legati alla strategia, al controllo e alla regolamentazione inerente l'Ict security;

• standard di riferimento che assicurino procedure adeguate e rispetto delle policy;

• processi di monitoraggio e controllo adeguati, che assicurino feed-back tempestivi sullo stato di implementazione dei programmi, sulla loro efficacia, nonché sulla compliance alle policy e alle normative di riferimento;

• meccanismi organizzativi che consentano un aggiornamento e un miglioramento continuo delle policy e delle procedure e, quindi, una costante riduzione del livello di rischio complessivo.

Capitolo 1

Obbligazioni di mezzo o di risultato?

Obbligazioni di mezzo	Obbligazioni di risultato
Il fornitore è totalmente responsabile della gestione della sicurezza	La responsabilità è divisa tra ente appaltante e fornitore
sicurezza come eventi da contrastare	Sicurezza come protezione
Difficile verificare l'ottemperanza ai requisiti in fase di collaudo	Verificabilità dell'ottemperanza ai requisiti in fase di collaudo
Devono essere previsti valori di soglia e penali	Necessità di fissare con chiarezza compiti e responsabilità del fornitore

Capitolo 1

Leggi di rilievo

D.Lgs. 196/2003: protezione dei dati personali

D.Lgs. 231/2001: responsabilità amministrativa dell'ente

SEZIONE III - Responsabilità amministrativa per reati previsti dal codice penale

Art. 24. - Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico.

Art. 25 - Concussione e corruzione

Art. 25-bis - Falsità in monete, in carte di pubblico credito e in valori di bollo

Art. 25-ter - Reati societari

Art. 25-quater - Delitti con finalità di terrorismo o di eversione dell'ordine democratico

Art. 25-quinques - Delitti con finalità di terrorismo o di eversione dell'ordine democratico

Art. 25-sexies - Abusi di mercato

Art. 25-septies - Omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro

Capitolo 2

Le trattative

Le parti nello svolgimento delle trattative e nella formazione del contratto devono comportarsi secondo buona fede

le parti contrattuali devono comportarsi, ciascuna nei confronti dell'altra, con lealtà, correttezza onestà e solidarietà.

A titolo esemplificativo, in fase di trattative, potrebbe concretizzarsi nell'obbligo di fornire tutte le informazioni possibili, riguardanti un determinato affare per non far interrompere le trattative stesse in modo ingiustificato, o in fase esecutiva del contratto potrebbe sostanziarsi nell' attitudine volta a permettere alla controparte di adempiere alla propria obbligazione etc.

Capitolo 2

Le trattative

I contratti di sicurezza

I contratti di sicurezza sono una tipologia contrattuale comprendente tutti quegli accordi attraverso i quali un committente, di regola un'impresa, incarica un fornitore di servizi informatici di approntare un sistema di sicurezza in grado di proteggere i propri archivi aziendali

Capitolo 2

Le trattative

Obiettivo:

assicurare l'efficace svolgimento dei processi che si basano sui beni o servizi oggetto della fornitura, creando i presupposti affinché i risultati risultino conformi alle aspettative

Capitolo 2

Le trattative

Requisiti di qualità:

hanno lo scopo di fare in modo che i risultati dei processi siano aderenti alle specifiche di progetto

Requisiti di sicurezza:

si riferiscono a situazioni eccezionali ed hanno l'obiettivo di evidenziare i possibili casi di "deragliamento" del processo produttivo fondamentale e prevedere soluzioni alternative

Capitolo 2

Le trattative

per qualunque fornitura di beni o servizi bisogna considerare le casistiche relative al processo normale e a quello eccezionale (elementi che incidono sull'efficienza ed efficacia di tale processo), anche se l'importanza che assume la gestione dei diversi casi ed il livello di dettaglio con cui è opportuno definire ciascuna casistica dipendono fortemente dalla natura della fornitura e dal contesto in cui essa si colloca.

Capitolo 2

Le trattative

A questo punto è bene una ricognizione generale di tutto il processo che ha portato alla stipula del contratto

Redazione di una check list dei punti concordati allo scopo di trasformarla in un regolamento condiviso che avrà forza di legge tra le parti

Capitolo 3

La stesura del contratto: premesse e oggetto

Le premesse sono una parte importantissima del contratto. Servono:

- a esplicitare i motivi che hanno spinto le parti a contrattare
- a chiarire il significato dei termini usati
- a indicare gli obiettivi a cui tende il contratto

In generale a rendere esplicite tutte quelle ragioni che le parti ritengono parte integrante del contratto

In questo modo la premessa integra il contenuto del contratto

Capitolo 3

La stesura del contratto: premesse e oggetto

È il bene materiale o immateriale per conseguire il quale le parti porgono in essere il contratto

Bene materiale: un personal computer, accessori

Bene immateriale: una licenza sw,un servizio

Distinguere vendita, fornitura, appalto

L'oggetto deve essere possibile, lecito, determinato o determinabile

Capitolo 3

La stesura del contratto: premesse e oggetto

•contratti relativi a beni e servizi informatici, in cui la sicurezza è un elemento qualificante come, ad esempio, fornitura di sistemi elaborativi, servizi di comunicazione, outsourcing della gestione del sistema informativo, ecc.

• contratti relativi a servizi o prodotti per la sicurezza come, ad esempio, firewall, servizi gestiti, auditing/assessment, ecc.

Capitolo 4

Obblighi delle parti

Parliamo di obblighi funzionali al conseguimento dell'oggetto del contratto

La complessità dell'oggetto informatico ha come conseguenza la necessità di articolare e rendere esplicite le attività necessarie per realizzare l'oggetto del contratto stesso

È buona norma mettere sempre prima gli obblighi del Fornitore.

Psicologicamente il Committente "vede" che il Fornitore è tenuto a fare qualcosa per garantire il conseguimento dell'oggetto e si sente garantito.

Capitolo 4

Obblighi delle parti

Parliamo di obblighi funzionali al conseguimento dell'oggetto del contratto

La complessità dell'oggetto informatico ha come conseguenza la necessità di articolare e rendere esplicite le attività necessarie per realizzare l'oggetto del contratto stesso

È buona norma mettere sempre prima gli obblighi del Fornitore.

Psicologicamente il Committente "vede" che il Fornitore è tenuto a fare qualcosa per garantire il conseguimento dell'oggetto e si sente garantito.

Capitolo 4

Obblighi delle parti: clausole

Prodotti informatici:

- La rispondenza del prodotto alle specifiche può essere attestata con certificazione tipo “common criteria”
- Possibilità di accedere al codice sorgente
- Impegno del produttore a sviluppare e mantenere prodotti con elevati livelli di qualità e ridotte vulnerabilità
- Clausola di non diffusione di informazioni
- Distruzione o restituzione dei dispositivi contenenti dati rimossi o sostituiti per attività di manutenzione
- Regole e restrizioni relativamente alla possibilità di eseguire attività di manutenzione da postazioni di lavoro remote
- Procedure a cui il fornitore deve attenersi per attività di manutenzione e politiche di sicurezza da seguire

Capitolo 4

Obblighi delle parti: clausole

Servizi:

a) Il contratto deve specificare gli obblighi del fornitore in merito a un elenco di situazioni anomale che possono verificarsi e chiarire quali devono essere le caratteristiche del servizio a seguito di tali eventi

b) Il contratto deve esprimere i requisiti di sicurezza in termini di misure tecniche ed organizzative che il fornitore dovrà mettere in atto. L'esatta esecuzione della prestazione consiste nel comportamento diligente da parte del fornitore, il quale si impegna ad impiegare tutti i mezzi idonei affinché si realizzi un risultato conforme a quanto specificato nei requisiti, a prescindere dall'effettivo raggiungimento degli obiettivi.

Capitolo 4

Obblighi delle parti: clausole

Il Committente si impegna a fornire al Fornitore le istruzioni chiare e dettagliate necessarie per la realizzazione dell'oggetto, assicurando che tutte le informazioni e i dati relativi ai propri prodotti e/o servizi forniti al Fornitore sono veritieri e in nessun caso ingannevoli.

Il Committente si impegna, nel predisporre il materiale e le informazioni necessarie per lo sviluppo del PROGETTO, a non violare diritti di terzi e ad attenersi alle norme di legge.

La responsabilità in ordine alle eventuali violazioni di diritti di terzi e/o ad infrazioni alle normative tutte di cui sopra farà carico esclusivamente al Committente, il quale si impegna a tenere totalmente manlevato il Fornitore per qualsiasi pretesa e/od azione di terzi e/o conseguenza comunque dannosa o pregiudizievole derivante dall'attività pubblicitaria contenente il materiale pubblicitario o da questi comunque approvate.

Ferma in ogni caso la suddetta responsabilità del Committente, è riconosciuta al Fornitore la facoltà di rifiutare il materiale che fosse ritenuto non conforme alle disposizioni di legge.

Capitolo 4

Obblighi delle parti: reportistica/stato avanzamento lavori

A fronte dei servizi sopra descritti e per ogni attività conclusa in essi rientrante il Fornitore elabora una scheda di lavoro recante le attività da svolgere ed i compensi richiesti e la comunica al Committente per approvazione.

La scheda di lavoro si considera parte integrante del presente contratto.

Capitolo 4

Obblighi delle parti: reportistica/stato avanzamento lavori

Livelli di servizio e parametri quantitativi: SLA service level agreement

Livelli di servizio che il Committente assicura al Fornitore sulla propria infrastruttura e/o servizio: OLA operation level agreement

Capitolo 4

Obblighi delle parti: collaudo

è opportuno prevedere la possibilità di eseguire verifiche anche dopo l'avvio della fornitura, prolungando il collaudo oltre l'inizio della fase di esercizio e che il collaudo positivo sia condizionato all'assenza di manifeste vulnerabilità.

Un altro aspetto che è importante disciplinare contrattualmente è la possibilità di eseguire test o verifiche a seguito di particolari condizioni (ad esempio sospetto di compromissione del sistema di sicurezza) o periodicamente.

In generale è consigliabile introdurre comunque nel contratto la possibilità di verifiche.

In questo caso il contratto dovrà anche chiarire quale parte debba sostenere i costi della verifica, compresi i costi che il fornitore dovrà sostenere per soddisfare le relative richieste.

Capitolo 5

Clausola penale e causa di risoluzione

La penale è una prestazione dovuta in caso di inadempimento o parziale adempimento e ha la funzione di limitare il risarcimento alla prestazione stessa, salvo che sia convenuta la risarcibilità del danno ulteriore

Capitolo 5

Clausola penale e causa di risoluzione

Art. 1456: clausola risolutiva espressa. Se una parte non adempie le proprie obbligazioni l'altra può chiedere la risoluzione del contratto, salvi i danni

Tipicamente il mancato pagamento del corrispettivo è giusta causa di risoluzione del contratto.

Le parti però possono prevedere altre cause legate all'importanza degli obblighi legati al Committente o al Fornitore

Capitolo 5

Clausola penale e causa di risoluzione

Art. 1456: clausola risolutiva espressa. Se una parte non adempie le proprie obbligazioni l'altra può chiedere la risoluzione del contratto, salvi i danni

Tipicamente il mancato pagamento del corrispettivo è giusta causa di risoluzione del contratto.

Le parti però possono prevedere altre cause legate all'importanza degli obblighi legati al Committente o al Fornitore

Capitolo 6

Responsabilità

Art. 2236: se la prestazione implica la soluzione di problemi tecnici di speciale difficoltà, il prestatore d'opera non risponde dei danni se non in caso di dolo o colpa grave

Art. 1229: è nullo qualsiasi patto che esclude preventivamente la responsabilità del debitore per dolo o colpa grave

La definizione delle responsabilità inerenti la sicurezza ha impatti di natura legale, organizzativa ed economica.

Capitolo 7

Risoluzione delle controversie

Procedura conciliativa

Ricorso all'autorità giudiziaria ordinaria
(problemi: lentezza della procedura e prima sentenza non meno di due anni dall'inizio)

Ricorso all'arbitrato (massimo 90 giorni dall'accettazione dell'ultimo degli arbitri, possibilità di decidere secondo equità)

Capitolo 8

Profili fiscali

Il software costituisce un bene immateriale che partecipa alla produzione del reddito d'impresa; la sua utilità del software si distribuisce su più esercizi .

Il software viene distinto in:

a) software di base: insieme delle istruzioni indispensabili per il funzionamento dell'elaboratore (hardware);

b) software applicativo: insieme delle istruzioni che consentono l'utilizzo di funzioni del software di base al fine di soddisfare specifiche esigenze dell'utente.

La distinzione è importante, perché il software di base è un accessorio indispensabile e complementare per il funzionamento dell'hardware e quindi perde il requisito di bene immateriale, seguendo la natura dell'hardware, con assoggettamento alla relativa disciplina civilistica e fiscale.

… grazie per l'attenzione …

antonino.attanasio@studioact.it

antonino.attanasio@tin.it

Id. skype: studio_attanasio
Id MSN: studio_attanasio@hotmail.com