CISCO Photonics Italia S.r.l.

Modello di organizzazione, gestione e controllo
ai sensi dell'art. 6 del Decreto Legislativo n. 231/2001

Parte Speciale

Gestione dei Sistemi informatici

Testo approvato dal Consiglio di Amministrazione con delibera del 22 novembre 2017

1 FINALITÀ

La presente Parte Speciale del Modello ha la finalità di definire le regole che tutti gli "esponenti aziendali" (organi sociali, dipendenti e collaboratori della Società) coinvolti nell'ambito delle attività "sensibili" elencate nel successivo paragrafo 2 dovranno osservare al fine di prevenire la commissione dei reati previsti dal d.lgs. 231/2001 e assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- indicare i principi di comportamento e i presidi di controllo che gli esponenti aziendali devono osservare ai fini della corretta applicazione del Modello;
- fornire all'Organismo di Vigilanza ed alle altre strutture di controllo gli strumenti per esercitare le attività di monitoraggio, controllo, verifica.

In linea generale, tutti gli esponenti aziendali dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi al contenuto dei seguenti documenti:

- Modello Organizzativo;
- Codice Etico di Cisco;
- sistema di procure e deleghe in vigore;
- corpo normativo e procedurale della Società e del Gruppo Cisco;
- CCNL applicabile;
- ogni altro documento aziendale che regoli attività rientranti nell'ambito di applicazione del Decreto.

È inoltre espressamente vietato adottare comportamenti contrari a quanto previsto dalle vigenti norme di Legge.

2 LE ATTIVITÀ SENSIBILI RILEVANTI

L'utilizzo dei sistemi informatici può portare al compimento di uno spettro molto ampio di condotte illecite. In quanto mezzo di comunicazione e calcolo utilizzato trasversalmente in svariate unità dell'azienda, i sistemi informatici possono astrattamente essere utilizzati per compiere reati contro la P.A. reati societari, reati verso il commercio e l'industria, reati ambientali, ecc..

Tale riflessione è confermata ulteriormente dal fatto che i sistemi informatici non sono solo i terminali (PC, device, ecc.), ma più in generale tutta la struttura di sistemi e apparati (materiali ed immateriali) utilizzati dalla Società.

Se si seguisse pertanto un criterio che identifica le attività sensibili scaturenti dalla gestione dei sistemi informatici con tutte le attività che ne presuppongono l'uso, il novero delle attività sensibili e dei reati sarebbe elevatissimo. Tale *modus operandi* rischierebbe di essere poco efficiente, perché farebbe cadere nella presente parte speciale ogni attività che presuppone l'uso dei sistemi informatici. Ne deriverebbe una lista di attività sensibili eccessiva, che richiederebbe peraltro l'elencazione di norme di comportamento e procedure già oggetto di altre parte speciali del Modello. Una sovrapposizione inefficiente e confusionaria, divergente dall'orientamento della più recente Giurisprudenza, che predilige modelli snelli ma efficaci, rispetto a Modelli complessi ma di difficile attuazione pratica.

Per tali motivi, la scelta adottata da Cisco con riferimento alla Gestione dei sistemi informatici è stata quella di indicare come attività sensibili solo quelle attività che sono tipicamente idonee a commettere reati informatici o reati correlati all'utilizzo di sistemi informatici.

alla luce di quanto sopra, le attività che la Società considera rilevanti nell'area relativa alla gestione dei sistemi informatici sono le seguenti:

- Gestione dei rapporti con le istituzioni e/o organismi di vigilanza relativi allo svolgimento di attività regolate dal testo unico in materia di Privacy (D.Lgs. 196/2003);
- Installazione, manutenzione, aggiornamento o gestione di software di soggetti pubblici o forniti da terzi per conto di soggetti pubblici;
- Gestione del profilo utente e del processo di autenticazione;
- Gestione e protezione della postazione di lavoro;
- Gestione degli accessi verso l'esterno;
- Gestione e protezione delle reti;
- Gestione degli output di sistema e dei dispositivi di memorizzazione;
- Sicurezza fisica (sicurezza cablaggi, dispositivi di rete, ecc.);
- Organizzazione e Dimensionamento IT;
- Certificazioni e obblighi normativi;
- Progettazione funzionalità applicative
- Utilizzo dispositivi informatici e di comunicazione, anche tramite apparati wi-fi.

3 GESTIONE DELLE ATTIVITÀ SENSIBILI RILEVANTI IN TEMA DI SISTEMI INFORMATICI

3.1 I reati potenzialmente rilevanti

- Frode informatica (art. 640-ter c.p.) e truffa aggravata ai danni dello stato (art. 640 c.p.);
- Falsità riguardanti un documento informatico (art. 491-bis c.p.) in combinazione con:
- Falsità materiale commessa dal privato (art. 482 c.p.)
- Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.)
- Falsità in scrittura privata (art. 485 c.p.)
- Falsità in foglio firmato in bianco (art. 486 c.p.)
- accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.),
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)

3.2 Ambito di applicazione

I successivi principi di comportamento e presidi di controllo si applicano a:

- Responsabile IT*;*
- personale funzione IT;
- tutti i Destinatari del Modello che, in ragione del proprio incarico o della propria funzione debbano utilizzare o gestire i sistemi informativi aziendali o di terze parti.

3.3 Principi di comportamento da adottare

Tutti i dipendenti ed i collaboratori della Società, devono:

- utilizzare gli strumenti informatici assegnati ed i sistemi aziendali nel rispetto delle prassi e delle procedure aziendali in vigore per l'espletamento della propria attività lavorativa e, solo in via straordinaria e/o di emergenza, per esigenze personali;

- utilizzare la navigazione in internet e la posta elettronica esclusivamente per le attività lavorative;
- custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi utilizzati, evitando che soggetti terzi possano venirne a conoscenza, e aggiornare periodicamente le password;
- custodire accuratamente le risorse informatiche aziendali o di terze parti (es. personal computer fissi o portatili) utilizzate per l'espletamento delle attività lavorative;
- rispettare le policy o le prassi di sicurezza concordate e definite con le terze parti per l'accesso a sistemi o infrastrutture di queste ultime.

È inoltre espressamente vietato:

- detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
- entrare nella rete aziendale e nei programmi con un codice d'identificazione utente diverso da quello assegnato;
- lasciare documenti incustoditi contenenti informazioni riservate o codici di accesso ai sistemi;
- porre in essere condotte, anche con l'ausilio di soggetti terzi, miranti all'accesso a sistemi informativi altrui con l'obiettivo di acquisire abusivamente, danneggiare o distruggere informazioni o dati contenuti nei suddetti sistemi informativi;
- utilizzare abusivamente codici d'accesso a sistemi informatici e telematici nonché procedere alla
- diffusione degli stessi;
- lasciare incustodito il proprio *personal computer* sbloccato;
- rivelare ad alcuno le proprie credenziali di autenticazione (nome utente e *password*) alla rete aziendale o anche ad altri siti/sistemi;
- aggirare o tentare di eludere i meccanismi di sicurezza aziendali (*Antivirus*, *Firewall*, *Proxy Server*, ecc.) di terze parti;
- accedere ad aree riservate (quali *server rooms*, locali tecnici, ecc.) senza idonea autorizzazione, temporanea o permanente;
- distruggere o alterare documenti informatici archiviati sulle *directory* di rete o sugli applicativi aziendali e, in particolare, i documenti che potrebbero avere rilevanza probatoria in ambito giudiziario;
- danneggiare o distruggere gli archivi o i supporti relativi all'esecuzione delle attività di *backup*;
- acquisire abusivamente, danneggiare o distruggere informazioni o dati contenuti nei sistemi informativi aziendali o di terze parti;
- porre in essere condotte miranti alla distruzione o all'alterazione di sistemi informativi aziendali o di terze parti;
- porre in essere condotte miranti alla distruzione o all'alterazione dei documenti informatici aventi finalità probatoria;
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico della Pubblica Amministrazione, o intervenire senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico della Pubblica Amministrazione;
- utilizzare o installare programmi diversi da quelli autorizzati dal responsabile IT e privi di licenza;
- utilizzare i sistemi informativi a disposizione per attività non autorizzate nell'ambito dell'espletamento delle attività lavorative;
- salvare sulle unità di memoria aziendali contenuti o file non autorizzati o in violazione del diritto d'autore;
- installare, duplicare o diffondere a terzi programmi (software) senza essere in possesso di idonea licenza o superando i diritti consentiti dalla licenza acquistata (es. numero massimo di installazioni o di utenze).

3.4 Procedure e presidi di controllo da applicare

Nella gestione delle attività in oggetto tutti gli esponenti aziendali coinvolti dovranno assicurare che siano svolti e formalmente tracciati e documentati (anche ai fini delle attività di verifica di competenza dell'Organismo di Vigilanza) i seguenti presidi minimi di controllo ritenuti rilevanti al fine di mitigare potenziali rischi-reato ai sensi del d.lgs. 231/2001:

1. L'accesso alle informazioni che risiedono sui *server* e sulle banche dati aziendali e di terze parti, deve essere limitato da idonei strumenti di autenticazione implementati dal Responsabile IT, tra cui a titolo esemplificativo e non esaustivo:
   - utilizzo di *account* e *password*;
   - accessi profilati alle cartelle di rete.
2. La creazione, modifica e disattivazione degli utenti e dei relativi profili deve essere effettuata dal Personale della Funzione IT, sulla base delle informazioni fornite dal Responsabile della Funzione Human Resources, in particolare:
   - il Personale della Funzione IT deve gestire le abilitazioni degli utenti sul server e l'abilitazione e la disabilitazione delle utenze in base alle necessità delle singole Funzioni (ad esempio, l'accesso al sistema di contabilità deve essere garantito al solo personale della Funzione Amministrazione, Finanza e Controllo)
   - almeno due volte all'anno, il Responsabile IT deve effettuare una revisione degli utent e dei profili abilitativi, confrontando la definizione d'utenza con i dati in possesso della Funzione Human Resources;
   - in caso di dimissioni dell'utente, il personale della Funzione HR deve comunicare, tramite apposito *form*, le dimissioni al personale della Funzione IT, che deve provvedere a disabilitare l'utente in tutti i *server*.
3. L'accesso tramite *VPN* è consentito, tramite l'utilizzo di appositi *eToken* secondo le modalità definite dal Responsabile IT.
4. Tutte le informazioni aziendali che risiedano sui *server* e sulle banche dati centrali, devono essere sottoposte a regolare procedura di *backup* da parte del Responsabile IT. In particolare, deve essere effettuato:
   - un *backup* incrementale giornaliero
   - un *backup* totale alla fine della settimana, alla fine del mese e alla fine dell'anno.
5. Il Responsabile IT deve assicurare che le procedure di salvataggio siano adeguate e provvedere al corretto mantenimento dei *file di log* generati dai sistemi.
6. Il Personale della Funzione IT deve effettuare il salvataggio periodico dei dati e la relativa archiviazione sui *server* locali e, in copia, nelle copie di *backup* e su nastro.
7. Il Disaster Recovery delle principali applicazioni aziendali e dei relativi dati deve essere garantito da copia degli stessi su un sito remoto.
8. Tutti i sistemi aziendali devono essere sottoposti, da parte del Responsabile IT, ad una preliminare attività di "hardening" prima del loro utilizzo; si deve assicurare che le risorse informatiche assegnate agli utenti siano correttamente configurate sotto il profilo della sicurezza.
9. Tutti i sistemi aziendali o i sistemi mediante i quali sono trasmesse o trattate le informazioni (dispositivi, apparati di rete, server, banche dati, applicazioni e laptop), devono essere sottoposti, da parte del Responsabile IT, a periodiche attività di risk assessment al fine di valutare eventuali vulnerabilità per le informazioni; si deve, inoltre, assicurare che l'aggiornamento dei sistemi e degli apparati di protezione sia in linea con le più recenti conoscenze tecnologiche, al fine di mitigare i rischi che incombono sulle informazioni.
10. Tutti i server e le postazioni di lavoro devono essere aggiornati periodicamente, da parte del Responsabile IT, sulla base delle *patch* rilasciate dai produttori dei sistemi operativi e degli applicativi. Deve essere assicurato l'aggiornamento periodico di tutti i sistemi in linea con gli aggiornamenti messi a disposizione dai produttori di software.
11. Tutti i supporti rimovibili, ivi inclusi gli hard disk del personale prima del loro riutilizzo o dismissione devono essere resi, da parte del Responsabile IT, tecnicamente non intelligibili.

12. L’attività di installazione software sulle postazioni di lavoro dei dipendenti/collaboratori deve essere consentita solamente al personale della Funzione IT nel momento di acquisto dell’hardware.
13. Il Responsabile IT deve verificare periodicamente la presenza sui terminali di solo SW autorizzato e deve monitorare le licenze del SW attraverso l’uso di un registro elettronico dei PC, mantenuto dal Responsabile IT.
14. Annualmente, il Responsabile IT deve effettuare il controllo dei software installati sui server.
15. Il censimento di tutti i flussi di trasferimento dei dati da e verso enti esterni ed enti pubblici, e di tutti gli accessi di tipo interattivo deve essere realizzato periodicamente, con il supporto dei Responsabili di Funzione, al fine di mitigare il rischio che i canali telematici attivi per tali flussi vengano utilizzati per accessi di tipo abusivo.
16. Per i principali sistemi informativi, il Responsabile IT deve assicurare che gli ambienti di sviluppo e test siano fisicamente e/o logicamente separati dall'ambiente di produzione.
17. La rete di trasmissione di dati aziendale deve essere protetta da adeguati strumenti di monitoraggio, gestiti dal Responsabile IT, contro il rischio di accesso abusivo.
18. I server e le workstation della Società devono essere protetti da software antivirus e antispam e firewall, con le impostazioni di aggiornamento automatico.
19. L’accesso ad internet deve essere controllato da proxy server che deve inibire la navigazione verso i siti considerati non di lavoro o con contenuti illeciti.
20. Il Responsabile IT deve effettuare periodicamente delle attività di vulnerability assessment.
21. L’accesso fisico alle sale CED deve essere gestito da un giornale d’accesso e attraverso apposite chiavi, consegnate al solo personale autorizzato, secondo quanto previsto dal Responsabile IT.
22. I server devono essere protetti con i principali sistemi di sicurezza (impianti di rilevazione e spegnimento incendi, sistemi di antintrusione, sistemi di condizionamento, gruppi di continuità, ridondanza dei sistemi, impianti di rilevazione gas, etc).
23. All’atto dell’assunzione, ogni dipendente deve ricevere il regolamento tecnologie informatiche Cisco.

***