INFORMEST

(Centro di Servizi e Documentazione per la Cooperazione Economica Internazionale)

Modello di organizzazione, gestione e controllo ex D.lgs. 231/2001 integrato ai sensi della legge 190/2012

PARTE SPECIALE "D" – REATI INFORMATICI E DI TRATTAMENTO ILLECITO DEI DATI

Revisione n. 00	Approvata dal C.d.A.	In data 30/01/2025

1. Le "attività sensibili" ai fini del d.lgs. n. 231/2001

L'art. 6, comma 2, lett. a) del d.lgs. n. 231/2001 indica, come uno degli elementi essenziali dei modelli di organizzazione e di gestione previsti dal decreto, l'individuazione delle cosiddette attività "sensibili" o "a rischio", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal d.lgs. n. 231/2001.

L'analisi dei processi aziendali di Informest ha consentito di individuare le attività nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate all'art. 24-*bis* del D.lgs. n. 231/2001. Qui di seguito sono elencati i processi esaminati unitamente alle attività sensibili identificate al loro interno e le funzioni/unità organizzative coinvolte di Informest:

1) ***Gestione dei sistemi informativi e della sicurezza informatica***

Principali funzioni/aree coinvolte: Legale Rappresentante, Dirigente responsabile, RPCT, ICT, tutti i soggetti che possono accedere ad un sistema informatico o telematico.

Attività inerenti i sistemi propri di Informest e, in particolare, le attività di gestione del sito internet e della rete intranet, gestione dei profili utente e del processo di autenticazione, gestione dell'hardware e del software aziendale, gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio, protezione della postazione di lavoro, gestione degli accessi da e verso l'esterno, gestione e protezione delle reti e degli output di sistema e dei dispositivi di memorizzazione nonché la sicurezza fisica (cablaggi, dispositivi di rete, ecc.).

Reati ipotizzabili:

o **Accesso abusivo a sistema informatico o telematico** (art. 615-ter c.p.)

Le fattispecie di reato potrebbero configurarsi in caso di accesso a sistemi di società di terzi protetti da misure di sicurezza per ottenere informazioni, dati, documenti riservati.

o **Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici e telematici** (art. 615-quater c.p.)

Le fattispecie di reato potrebbero configurarsi, a titolo esemplificativo, nel caso in cui un dipendente si procuri un codice di accesso che permette di introdursi da remoto nella rete aziendale di un ente o società terza, per ottenere informazioni, dati, documenti riservati.

o **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche** (art. 617-quater c.p.)

Le fattispecie di reato potrebbero configurarsi nel caso in cui un dipendente invii messaggi di posta elettronica (spam) ad un terzo al fine di rallentare o bloccare i servizi di posta elettronica utilizzati, ad esempio per partecipare ad un bando europeo, o intercetti fraudolentemente una comunicazione tra altri soggetti al fine di veicolare false informazioni o comunque alterate, ad esempio per danneggiare l'immagine del terzo.

o **Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche** (art. 617-quinquies c.p.)

Le fattispecie di reato potrebbero configurarsi nel caso in cui un dipendente detenga o installi un software (trojan horse o spyware) nel sistema di un terzo al fine di intercettare informazioni riservate. Il presente reato è assorbito in quello di cui sopra (617-quater c.p.) in quanto

l'attività di fraudolenta intercettazione di comunicazioni informatiche presuppone la previa installazione di apparecchiature atte alla realizzazione dell'intercettazione configurandosi pertanto in un'ipotesi di progressione criminosa.

o **Danneggiamento di sistemi informatici o telematici** (art. 635-bis c.p.)

Le fattispecie di reato potrebbero configurarsi, a titolo esemplificativo, nel caso in cui un dipendente invii messaggi di posta elettronica (spam) ad un terzo al fine di bloccare le reti o violare i sistemi su cui eventuali concorrenti conservino della documentazione relativa a propri progetti allo scopo di distruggere le informazioni e ottenere un vantaggio.

o **Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità** (art. 635-ter c.p.)

Le fattispecie di reato potrebbero configurarsi, a titolo esemplificativo, nel caso in cui un dipendente, attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugga, danneggi o renda, in tutto o in parte, inservibili sistemi informatici appartenenti allo Stato o ad altro ente pubblico o ad esso pertinente o di pubblica utilità, o ne ostacola gravemente il funzionamento.

o **Danneggiamento di sistemi informatici o telematici** (art. 635-quater c.p.)

Le fattispecie di reato potrebbero configurarsi, a titolo esemplificativo, nel caso in cui un dipendente, attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugga, danneggi o renda, in tutto o in parte, inservibili sistemi informatici appartenenti a terzi o ne ostacola gravemente il funzionamento.

o **Falsità in un documento informatico pubblico o avente efficacia probatoria** (art. 419-bis c.p.)

Le fattispecie di reato potrebbero configurarsi, a titolo esemplificativo, nel caso in cui un dipendente ottenga indebitamente una smart card/ token necessario per l'utilizzo della firma digitale certificata, al fine di modificare un documento informatico avente valore legale; cancelli o alteri informazioni a valenza probatoria presenti nei sistemi dell'Ente o di un terzo allo scopo di eliminare le prove di un reato; falsifichi documenti destinati alla PA per ottenere un vantaggio.

2. Il sistema dei controlli

Il sistema dei controlli, individuato da Informest sulla base delle indicazioni fornite da ANAC, prevede con riferimento alle attività sensibili e ai processi strumentali individuati:

- principi generali di comportamento relativi alle attività sensibili,
- protocolli di controllo specifici applicati alle singole attività.

I protocolli di controllo sono fondati sulle seguenti regole generali che devono essere rispettate nell'ambito dell'attività sensibile individuata:

• **Segregazione dei compiti**: preventiva ed equilibrata distribuzione delle responsabilità e previsione di adeguati livelli autorizzativi, idonei ad evitare commistione di ruoli potenzialmente incompatibili o eccessive concentrazioni di responsabilità e poteri in capo a singoli soggetti. In particolare, deve essere garantita la separazione delle attività e responsabilità tra chi autorizza, chi esegue e chi controlla una determinata operazione nelle attività sensibili.

• **Norme**: esistenza di disposizioni interne e/o di procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante.

• **Poteri autorizzativi e di firma**: i poteri autorizzativi e di firma devono essere: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all'interno di Informest.

• **Tracciabilità**:
(i) ogni operazione relativa all'attività sensibile deve essere, ove possibile, adeguatamente registrata;
(ii) il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile *ex post*, anche tramite appositi supporti documentali;
(iii) in ogni caso, deve essere disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate.

2.1 Principi generali di comportamento prescritti nelle attività sensibili

Divieti

La presente Parte Speciale prevede l'espresso divieto a carico degli Esponenti dell'Ente in via diretta, ed a carico dei Collaboratori e fornitori di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 24-bis del d.lgs. 231/2001);
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarle.

In particolare, è fatto divieto:

- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico messo a disposizione dalla Regione Autonoma Friuli Venezia Giulia o altri partner con cui Informest intrattiene rapporti nell'ambito della propria attività al fine di alterare, cancellare dati o informazioni;
- detenere e/o utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico della Regione Autonoma Friuli Venezia Giulia o altri partner con cui Informest intrattiene rapporti nell'ambito della propria attività al fine di acquisire informazioni riservate;
- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico della Regione Autonoma Friuli Venezia Giulia o altri partner con cui Informest intrattiene rapporti nell'ambito della propria attività al fine di acquisire informazioni riservate;
- svolgere abusivamente attività di modifica e/o cancellazione di dati, informazioni o programmi della Regione Autonoma Friuli Venezia Giulia o altri partner con cui Informest intrattiene rapporti nell'ambito della propria attività;
- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;

• trasferire all'esterno di Informest e/o trasmettere file, documenti, o qualsiasi altra documentazione riservata di proprietà di Informest, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni;
• lasciare accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (parenti, amici, ecc.);
• utilizzare abusivamente password di altri utenti aziendali, neppure per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Dirigente responsabile e solo per finalità urgenti e non derogabili;
• utilizzare strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici.

Doveri

Ai fini dell'attuazione dei comportamenti di cui sopra indicati nella presente parte speciale, i soggetti sopra richiamati, devono:

• conoscere e rispettare tutte le misure atte a garantire l'affidabilità del sistema tenendo conto anche dell'evoluzione tecnologica per quanto riguarda la sicurezza dei dati trattati, il rischio di distruzione o di perdita degli stessi ed il rischio di accesso non autorizzato o non consentito.

È inoltre tassativamente imposto di:
• tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure interne di Informest;
• assicurare un pieno rispetto delle norme di legge e regolamenti, nonché delle procedure interne di Informest, nell'acquisizione, elaborazione e comunicazione di dati e informazioni, sia ai fini interni che nello svolgimento delle attività presso altri enti o PP.AA.;
• effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità Pubbliche con particolare attenzione a quelle destinate all'Autorità Garante della Privacy, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate;
• predisporre efficaci piani di sicurezza e sistematici monitoraggi della rete interna (intranet) di Informest al fine di evitare la commissione di reati.

Le condotte di ordine generale sopra descritte integrano e non sostituiscono i principi previsti dal Codice Etico, nonché le eventuali procedure di maggiore tutela previste all'interno di Informest e relative alle attività sensibili.

2.2 Standard di controlli specifici

Di seguito sono riportati i protocolli di controllo specifici relativi alle singole attività sensibili individuate:

1) ***Gestione dei sistemi informativi e della sicurezza informatica***

L'Ente ha posto in essere i seguenti presidi e controlli di cui ne chiede il rispetto:

- è stato predisposto il "Regolamento per l'utilizzo dei sistemi informatici" (Allegato 6 – Regolamento utilizzo sistemi informatici);
- l'Ente analizza i rischi e prevede controlli al fine di prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature attraverso:

    - monitoraggio dei luoghi fisici ove risiedono le infrastrutture,
    - previsione di credenziali fisiche di accesso ai siti ove risiedono i sistemi informativi e le infrastrutture IT,
    - limitazione all'accesso della documentazione archiviata in base alle funzioni del personale;
- sono state implementate procedure e istruzioni operative che prevedono:
    - per ogni utente i diritti di accesso alle infrastrutture ICT attraverso autenticazioni per mezzo dell'account personale del dipendente,
    - il dipendente che si colleghi in rete viene abilitato alla fruizione dei servizi corrispondenti al proprio ambito di operatività,
    - per ogni utente è prevista un'autenticazione individuale sul dominio tramite codice identificativo e password che consente anche di identificare il "profilo utente" e di verificare le attività, anche in rete, riconducibili a ciascun utente, indipendentemente dal terminale utilizzato,
    - il sistema informatico indica le modalità idonee di elaborazione e richiede un periodico aggiornamento delle "password" di autenticazione,
    - il sistema informatico prevede un limite nel numero di tentativi per il corretto inserimento della password in un determinato lasso di tempo (4 tentativi in 15 minuti), con conseguente blocco dell'accesso informatico in caso di errore per 15 minuti. Nel caso in cui si sia dimenticata la password, l'utente può reimpostarla autonomamente se ha configurato correttamente l'autenticazione a più fattori (MFA). In caso contrario è necessario richiedere assistenza all'amministrazione di sistema per la riabilitazione dell'utente,
    - ogni utente è tenuto ad adottare tutte le cautele necessarie per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo,
    - l'ufficio del personale informa l'amministratore di sistema di ogni modifica del rapporto lavorativo o del ruolo aziendale al fine di modificare di conseguenza le autorizzazioni e i diritti di accesso agli applicativi;
- l'Ente ha comunque previsto:
    - sistemi di protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono virus, con l'adozione di misure idonee e costante aggiornamento di programmi "antivirus" e "firewall",
    - scansioni automatizzate o semi automatizzate non invasive per rilevare la presenza di vulnerabilità,
    - saltuari controlli svolti da un soggetto esterno (vulnerability assessment) per valutare le vulnerabilità di un sistema e la sua capacità di resistere a tentativi intenzionali di comprometterne la sicurezza,
    - sistemi di controllo e protezione della posta elettronica in ingresso e uscita e sistemi di protezione della navigazione web,
    - tracciamento degli asset informatici,
    - archiviazione dei flussi autorizzativi dei vari processi,
    - sistemi che assicurano la continuità operativa dell'infrastruttura;
- vengono organizzate specifiche attività di formazione e aggiornamento periodico sulle procedure interne di sicurezza informatica per i dipendenti e, se del caso, per i terzi:
    - viene effettuata una valutazione (prima dell'assunzione o della stipula di un contratto) dell'esperienza delle persone destinate a svolgere attività IT, con particolare riferimento alla sicurezza dei sistemi informativi, e che tiene conto della normativa applicabile in materia, dei principi etici e della classificazione delle informazioni a cui i predetti soggetti avranno accesso,
    - adeguata formazione in base al ruolo,

- devono essere osservati gli obblighi previsti e già disciplinati all'interno del "Regolamento per l'utilizzo dei sistemi informatici" (Allegato 6 – Regolamento utilizzo sistemi informatici).
- è necessario altresì attenersi alle istruzioni impartite dalla normativa vigente in tema di trattamento dei dati personali (D.lgs. 196/2003 e Regolamento UE 2016/679)

La verifica circa l'efficacia e l'efficienza della gestione della sicurezza informatica è affidata all'Amministratore di sistema che, previa richiesta dell'OdV, ne stila una relazione sullo stato dell'infrastruttura.