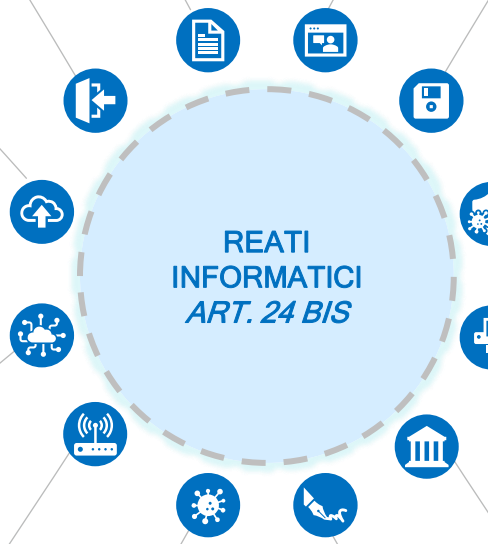
La prevenzione dei reati informatici: il documento di approfondimento di AODV231

Milano, 17 gennaio 2024

I reati informatici ex art. 24-bis del D.Lgs. 231/2001 ...



FALSIFICAZIONE DI DOCUMENTI INFORMATICI
Art. 491 bis c.p.

ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO TELEMATICO
Art. 615 ter c.p.

DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI 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.

VIOLAZIONE DELLE NORME IN MATERIA DI PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA
Art . 1 ,comma 11, D.L. 21.09.2019, n. 105 c.p.

INSTALLAZIONE DI APPARECCHIATURE ATTE AD INTERCETTARE, IMPEDIRE O INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEMATCHE
Art. 617 quinquies c.p.

DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI
Art. 635 bis c.p.

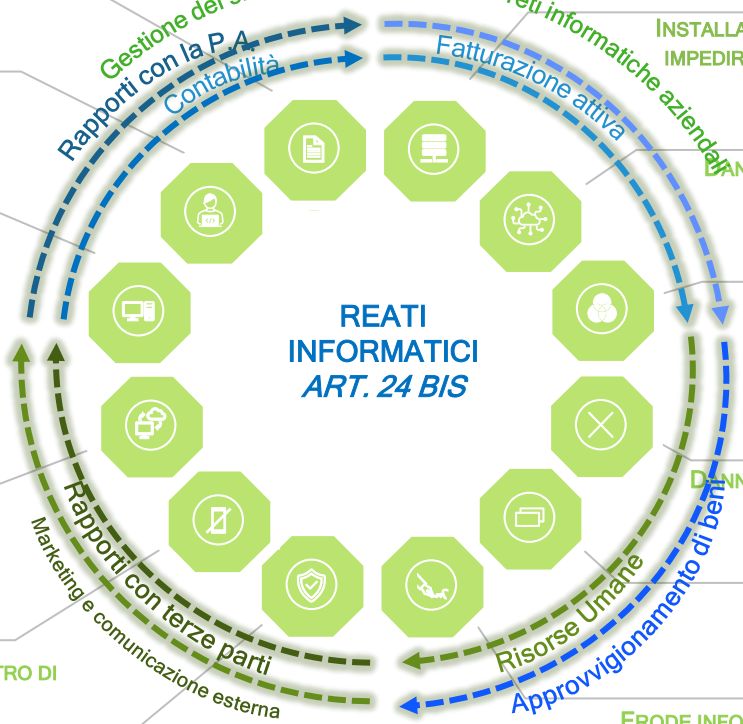
DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI UTILIZZATI DALLO STATO O DA ALTRO ENTE PUBBLICO O COMUNQUE DI PUBBLICA UTILITÀ
Art. 635 ter c.p.

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI
Art. 635 quater c.p.

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICA UTILITÀ
Art. 635 quinquies c.p.

FRODE INFORMATICA DEL CERTIFICATORE DI FIRMA ELETTRONICA
Art . 640 quinquies c.p.

… in stretta connessione con i processi aziendali



FALSIFICAZIONE DI DOCUMENTI INFORMATICI
(Art. 491 bis 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.)

VIOLAZIONE DELLE NORME IN MATERIA DI PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA
(Art. 1,comma 11, D.L. 21.09.2019, n. 105 c.p.)

INSTALLAZIONE DI APPARECCHIATURE ATTE AD INTERCETTARE, IMPEDIRE O INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEMATICHE
(Art. 617 quinquies c.p.)

DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI
(Art. 635-bis c.p.)

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.)

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI
(Art. 635-quater c.p.)

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICA UTILITÀ
(Art. 635-quinquies c.p.)

FRODE INFORMATICA DEL CERTIFICATORE DI FIRMA ELETTRONICA
(Art. 640-quinquies c.p.)

Dal diritto all'impresa: dai rischi-reato ai processi ed ai presidi

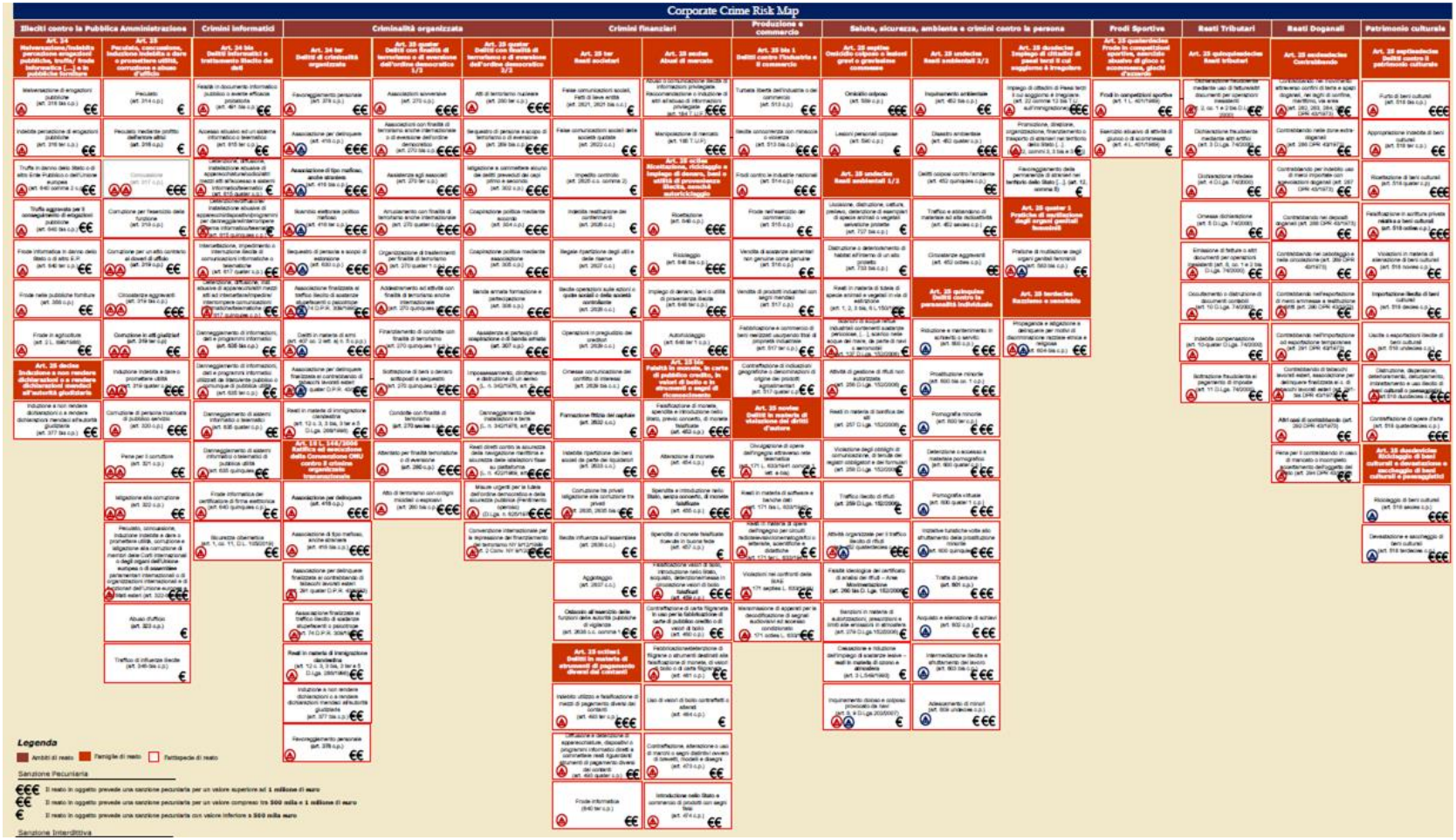
Mappatura dei rischi-reato specifici dell'organizzazione e (con particolare riferimento alle fattispecie di cui all'art. 24 bis del D.Lgs. 231/01) in coerenza con:

- business
- dimensioni
- articolazione organizzativa
- storia dell'ente

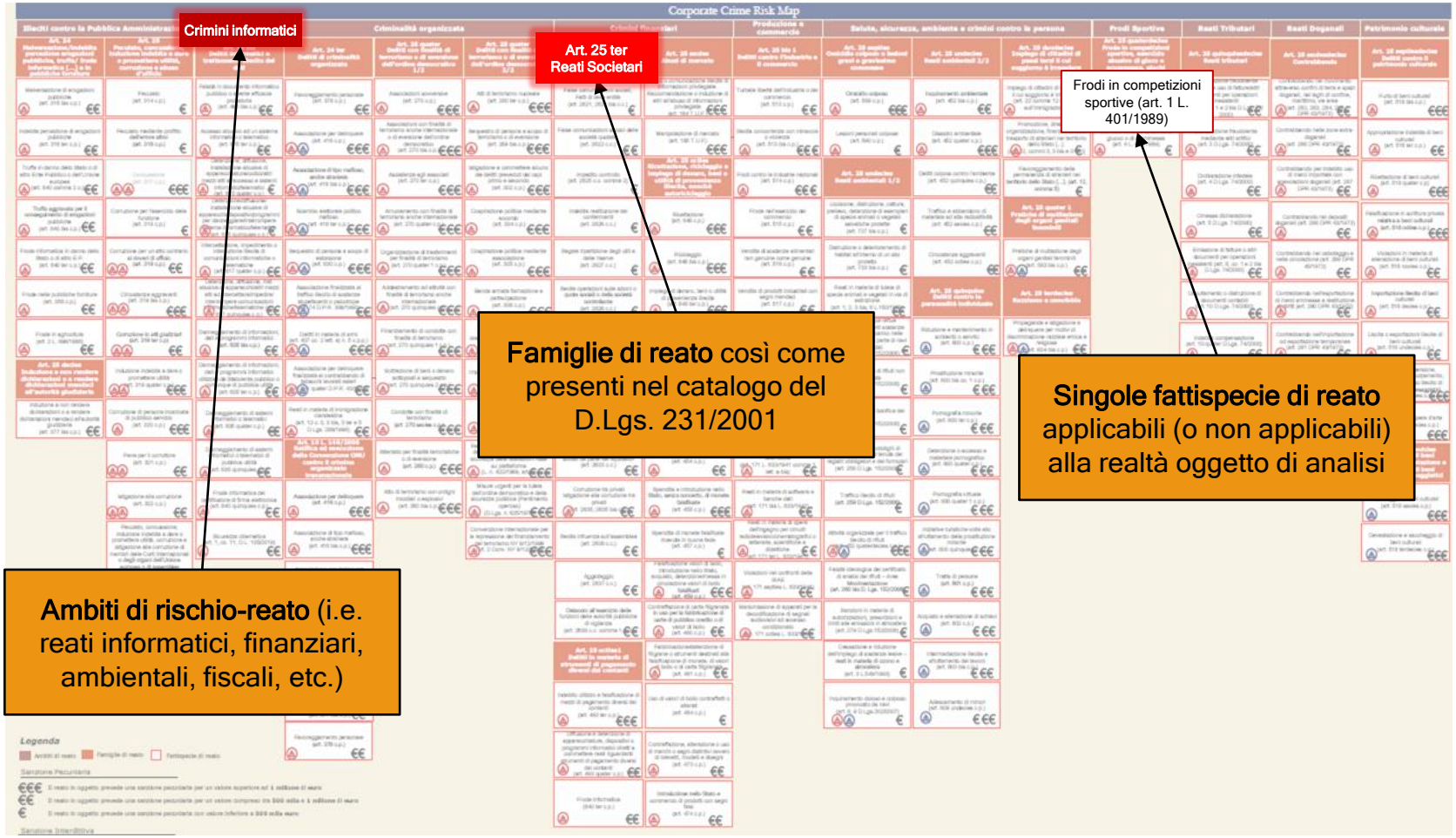
Identificazione dei **processi/attività sensibili** ai rischi-reato individuati nella fase precedente e dei **principi/presidi di controllo** atti a **prevenire** e **mitigare** i **rischi-reato** identificati

Redazione / Aggiornamento della Parte Speciale del **Modello 231** in coerenza con quanto emerso nella **mappatura dei rischi e dei presidi**

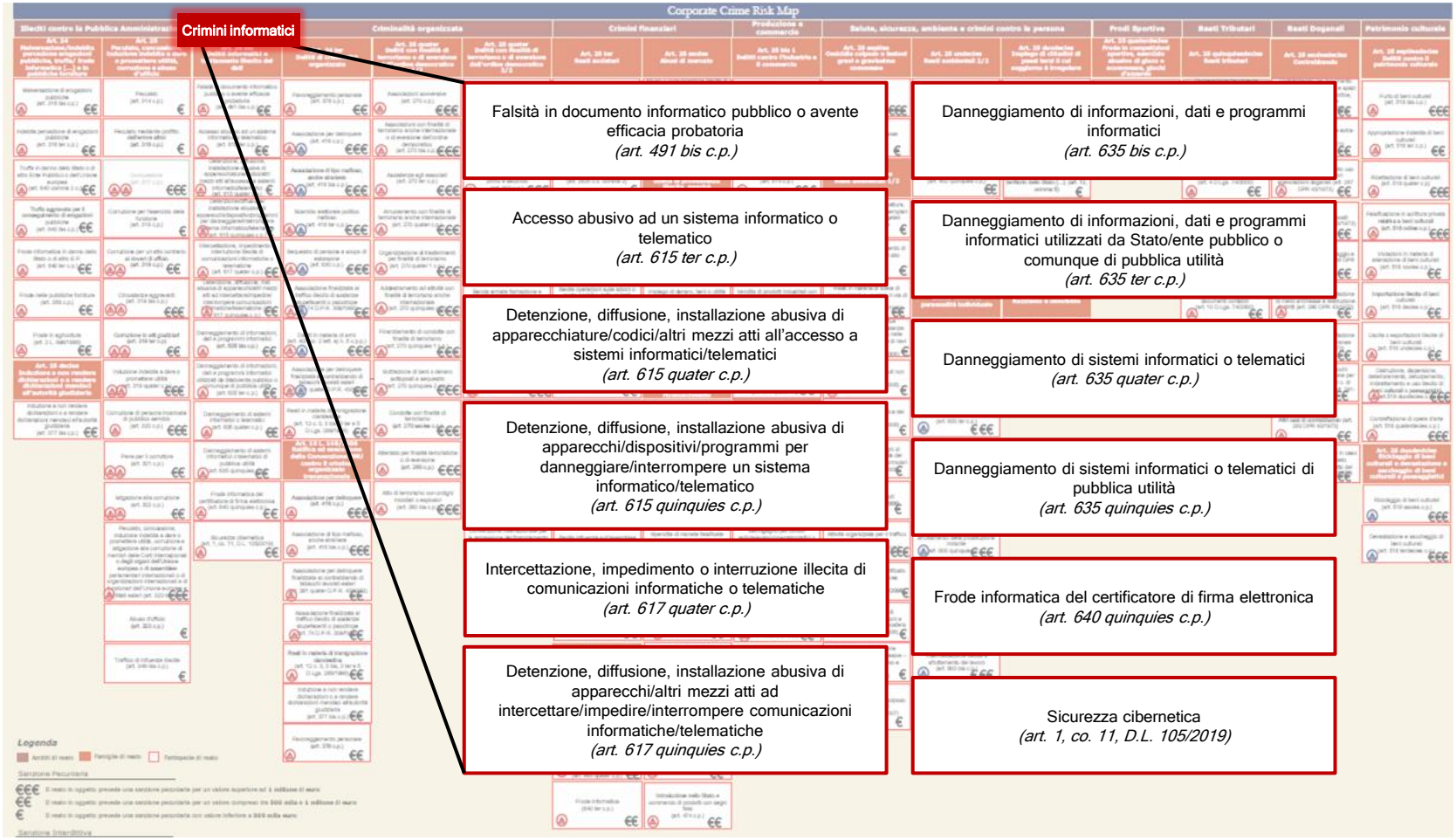
Mappatura dei rischi-reato | Corporate Crime Risk Map



Mappatura dei rischi-reato | Corporate Crime Risk Map



Mappatura dei rischi-reato | focus reati informatici



Risk Assessment di dettaglio

Step successivo all'**identificazione e mappatura** strutturata dei **reati applicabili** è lo svolgimento di un Risk Assessment di dettaglio che **analizzi** puntualmente **i rischi-reato 231**, in coerenza con i requirement del *comma 2, lett. a), dell'art. 6 del Decreto*

OBIETTIVO

Comprendere se, in quali circostanze e con quali modalità, un determinato **illecito possa essere commesso nell'interesse o a vantaggio dell'ente**, nell'ambito dell'organizzazione oggetto di analisi

MODALITÀ

Coinvolgimento dei soggetti responsabili delle **aree operative**, attraverso un **approfondito assessment dei rischi-reato specifici** delle rispettive aree di competenza (eventualmente supportati da risorse interne e/o esterne esperte in materia legale, di risk management, internal auditing e sistemi di controllo interno)

OUTPUT

Matrice rischio-reato

Art. 25 quinquies D.lgs. 231/2001		ESEMPI DI ATTIVITA' "SENSIBILI"	DIREZIONI COINVOLTE	POSSIBILI FINALITA' DI REALIZZAZIONE DEL REATO	ESEMPI DI POSSIBILI MODALITA' DI REALIZZAZIONE (a titolo esemplificativo e non esaustivo)	PROCESSI SENSIBILI
Riduzione o mantenimento in schiavitù o in servitù *(art. 600 c.p.)*	59	**Gestione degli acquisti**, con particolare riferimento ad affidamento di attività che prevedono l'utilizzo di manodopera di terze parti.	✓ Service erogato da Iren S.p.A.	Approfittando di una situazione di inferiorità ovvero di una situazione di necessità, si costringe una persona al proprio esclusivo servizio promettendo denaro o altra utilità.	Utilizzo o impiego di manodopera di soggetti terzi (e.g., prestatori d'opera nell'ambito di attività di appalto), nei casi in cui questi ultimi sottopongano i propri lavoratori a condizioni di sfruttamento approfittando del loro stato di bisogno.	1. Gestione degli acquisti di beni, servizi/consulenze e lavori
Intermediazione illecita e sfruttamento del lavoro *(art. 603 bis c.p.)*	60	**Gestione del personale**, con particolare riferimento alla definizione: - dell'orario lavorativo; - delle condizioni retributive; - degli impatti in ambito salute e sicurezza e delle condizioni lavorative in senso lato.	✓ Service erogato da Iren S.p.A.	Ottenere un risparmio di costi derivante dall'affidamento delle attività in appalto a terze parti che non rispettano pienamente, nei rapporti con i propri dipendenti, le condizioni fissate dai contratti collettivi nazionali ed ulteriori regolamentazione di riferimento.		3. Selezione, assunzione e gestione del personale e del sistema premiante

Reato

...fattispecie presupposto applicabili alla determinata attività sensibile

Attività sensibili

... potenzialmente esposte alla commissione del reato

Direzioni coinvolte

...che per procura o delega o responsabilità gestorie potrebbero commettere il reato

Finalità

...esemplificative di realizzazione del reato

Modalità

... esemplificative di realizzazione del reato

Processi sensibili

... in cui può verificarsi l'illecito

Dai rischi-reato ai presidi: percorso logico di analisi

PROCESSI
Identificazione dei PROCESSI SENSIBILI ai reati informatici

ATTIVITÀ SENSIBILI
Per ogni processo identificato, mappatura delle ATTIVITÀ sottostanti, SENSIBILI AL RISCHIO-REATO

PRESIDI DI CONTROLLO
Identificazione dei PRESIDI DI CONTROLLO da porre in essere al fine di MITIGARE / CONTRASTARE I RISCHI-REATO a cui è potenzialmente soggetta la società

Reati informatici: processi e attività sensibili

RILEVANZA DIRETTA

Gestione dei sistemi informativi e delle reti informatiche aziendali che sottende:

- Gestione degli accessi e dei profili di autorizzazione ed autenticazione ai sistemi informatici/telematici e alle applicazioni informative aziendali

Predisposizione e aggiornamento, con cadenza almeno annuale, di un elenco delle reti, dei sistemi informativi e dei servizi informatici (che comprenda la relativa architettura e componentistica interna)

Artt. 1, comma 11-bis L. 133/2019

Gestione della sicurezza informatica

Artt. 1, comma 11-bis L. 133/2019

Gestione delle attività on-line svolte dai dipendenti

Artt. 615 quater, 615 quinquies

Gestione delle informazioni sensibili

Artt. 491 bis, 615 ter, 635 bis, 635 quater

«STRUMENTALI»

Processi di natura operativa non direttamente rientranti nel processo di gestione delle infrastrutture tecnologiche, ma con riflessi ipotetici sullo stesso e potenzialmente rilevanti per la commissione dei reati informatici. Es.:

- Gestione acquisti di beni e servizi
- Gestione attività di ricerca e sviluppo
- Gestione attività di marketing e comunicazione esterna

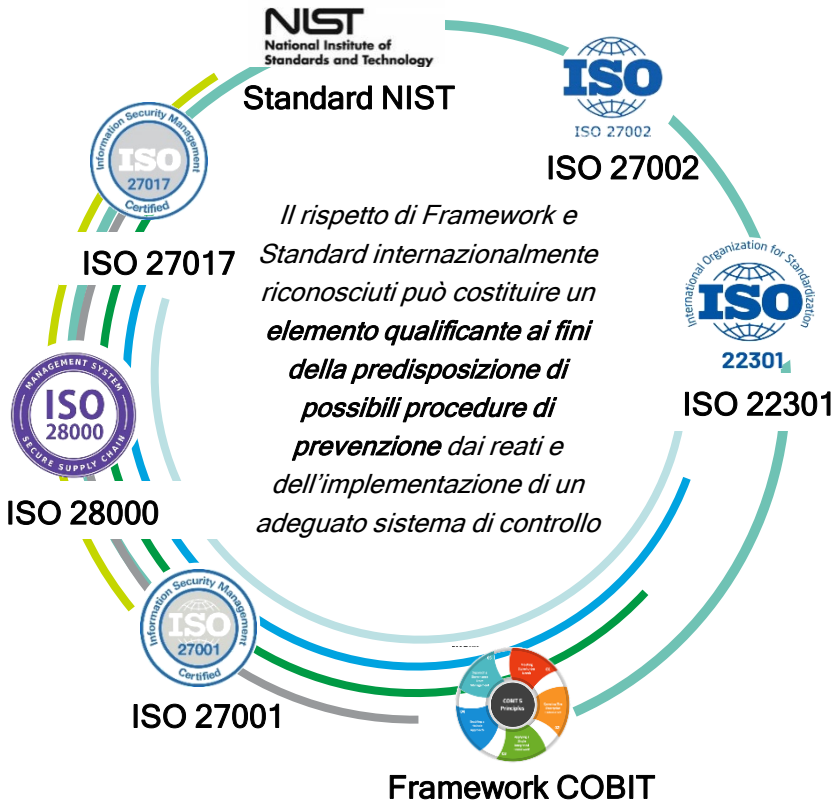
Reati informatici: presidi di controllo - introduzione

Per quanto il rischio, in astratto, non possa essere mai eliminato integralmente, l'**obiettivo prevenzionistico dell'ente** ai sensi del Decreto deve essere finalizzato a **contenerlo nel proprio risvolto di responsabilità penale** attraverso un **efficace ed efficiente** SISTEMA DI CONTROLLO INTERNO e l'adozione di specifici PRESIDI DI CONTROLLO

Il **Modello 231 deve arginare il rischio-reato** in una misura per cui l'agente non solo dovrà volere la commissione del reato, ma potrà attuare il proprio proposito criminoso soltanto AGGIRANDO FRAUDOLENTEMENTE le **prescrizioni dell'ente** e il relativo **sistema normativo interno**

Reati informatici: presidi di controllo - riferimenti

STANDARD E FRAMEWORK



LINEE GUIDA CONFINDUSTRIA

Nuove Linee Guida di Confindustria
per la costruzione dei Modelli di Organizzazione Gestione e Controllo
ai sensi del D.Lgs. 231/01

Le Linee Guida Confindustria forniscono alle imprese **indicazioni metodologiche** utili per l'elaborazione dei modelli, fornendo esempi dei principali processi/attività sensibili, dei relativi rischi-reato e dei presidi di controllo a mitigazione dei rischi

Reati informatici: presidi di controllo – esemplificazioni

ESEMPLIFICATIVO

PRINCIPALI PRESIDI DI CONTROLLO

GESTIONE DEI SISTEMI INFORMATIVI E DELLE RETI INFORMATICHE AZIENDALI

- Gestione delle informazioni sensibili (di business e/o personali)
- Gestione e protezione delle reti
- Gestione degli accessi da e verso l'esterno
- Gestione dei profili utente e del processo di autenticazione
- Gestione delle attività on-line svolte dagli utenti

- **Adozione di regolamenti e procedure** aventi ad oggetto il corretto utilizzo delle risorse informatiche aziendali, la sicurezza informatica/telematica, la protezione dei dati sensibili
- **Predisposizione di strumenti di protezione** volti a garantire la **sicurezza** nello **scambio di informazioni sensibili**, per l'azienda e per gli individui
- Adozione e implementazione di **procedure per la classificazione ed il trattamento delle informazioni**, per l'**utilizzo di sistemi crittografici** in relazione alla trasmissione in rete di documenti informatici, per i controlli tesi a **rintracciare eventuali falle o debolezze dei sistemi** (es. *vulnerability assessment* e *penetration test,* finalizzati a valutare la tenuta del sistema a fronte di eventuali attacchi esterni)
- Definizione di formali **requisiti di accesso e autenticazione al sistema**, dei criteri e delle modalità di **creazione ed utilizzo delle password**, di procedure per la **concessione** o la **revoca** degli **accessi** ai sistemi informativi;
- **Tracciatura e registrazione delle attività eseguite su sistemi, applicazioni e reti**, potenzialmente lesive per la sicurezza;
- **Verifica periodica delle modalità di accesso ai sistemi**, dei **log di registrazione** delle attività sui sistemi, delle **eccezioni e degli eventi** concernenti la **sicurezza**
- **Definizione** e **regolamentazione** delle **attività di gestione e manutenzione dei sistemi**
- **Adozione di meccanismi di protezione da software pericolosi** e procedure di controllo della installazione di software sui sistemi operativi
- Etc.

Reati informatici: presidi di controllo – esemplificazioni

PRINCIPALI PRESIDI DI CONTROLLO

ESEMPLIFICATIVO

RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

Gestione del processo di creazione, trattamento e archiviazione di documenti elettronici con valore probatorio

Gestione dei pagamenti elettronici da e verso l'esterno (ivi inclusi quelli dovuti alla P.A.)

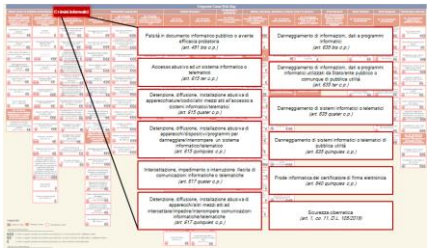
Gestione dei certificati digitali rilasciati da parte di un ente certificatore

Gestione sicurezza fisica e logica dei dati

- **Adozione e implementazione di specifiche misure** che prevedano:
  - individuazione di **ruoli e responsabilità** di documenti, dati ed elenchi
  - definizione delle **modalità** di **raccolta e approvazione della documentazione** da trasmettere alle autorità pubbliche
  - definizione di **attività di monitoraggio** per la **completezza delle informazioni** da comunicare
  - definizione e adozione di **misure tecniche per garantire adeguati livelli di sicurezza/ riservatezza** nel trattamento delle informazioni
  - individuazione delle **modalità comportamentali operative in caso di effettuazione di attività ispettive/vigilanza** da parte delle autorità preposte, etc.
- Definizione di **modalità di accesso ai sistemi informatici aziendali** mediante procedure di autorizzazione (es. concessione dei diritti di accesso ad un soggetto soltanto a seguito della verifica dell'esistenza di effettive esigenze)
- Adozione di **procedure di validazione delle credenziali** complesse e previsione di **modifiche periodiche**
- Adozione di **misure di protezione dell'integrità delle informazioni** messe **a disposizione** su un **sistema pubblico** per prevenire modifiche non autorizzate
- Implementazione di **misure di protezione dei documenti elettronici** (es. firma digitale)
- Etc.

Redazione / aggiornamento Parte Speciale MOG231

…. in coerenza con quanto emerso dalla mappatura di rischi e presidi



Crime Risk Map
reati applicabili

Attività sensibili e processi
Risk Assessment di dettaglio

PO-029-02	CONTROLLI SU FORNITURE UTENZE
PO-123-00	GESTIONE DELLE OPERAZIONI ATTIVE E PASSIVE CON SOGGETTI NON RESIDENTI IN ITALIA
PO-124-00	TASSAZIONE DEI REDDITI C.D. "PASSIVE INCOME" (DIVIDENDI, INTERESSI E ROYALTIES) CORRISPOSTI A SOGGETTI NON RESIDENTI
PO-097-02	GESTIONE DELL A CASELLA DI POSTA ELETTRONICA CERTIFICATA AZIENDALE (PEC)

Presidi di controllo
Elenco SOP / istruzioni operative aziendali