# La Riduzione del Rischio

www.vincenzocalabro.it

# Indice degli argomenti

- Ridurre i rischi
- Le azioni di reazione
- Le misure
- I controlli
- La vigilanza
- La disciplina
- Il processo 231

# Ridurre i rischi

- Dopo aver completato l'attività di analisi occorre individuare le azioni idonee a ridurre i rischi individuati.
- Per meglio comprendere le attività da porre in essere occorre richiamare gli elementi che compongono i rischi cui si è già fatto cenno quando si è trattata la valutazione.
- Il rischio è composto da tre elementi:
  1. La vulnerabilità, ovvero la debolezza offerta dal bene che deve essere protetto e dall'ambiente in cui esso è collocato e gestito.
  2. La minaccia, ovvero la probabilità che il rischio si manifesti.
  3. Il danno, ovvero l'impatto che il rischio può produrre, qualora si avveri, sul bene e, per relazione, sui soggetti legati al bene.
- Le azioni di reazione ai rischi agiscono su questi elementi.

# Le azioni di reazione

- Per quanto riguarda il danno la classica azione di reazione è il “trasferimento del rischio”. Ad esempio mediante l’accensione di un polizza assicurativa che nel caso in cui il rischio si avveri, risarcisce il danno prodotto. Questa azione, evidentemente non previene né evita il rischio, non può essere presa in considerazione riguardo i rischi 231 in quanto l’art.6 co. 1 lett. a) e l’art. 7 co. 2 del D.Lgs. 231/2001 espressamente richiedono di adottare un governo di prevenzione, ovvero atto ad impedire la commissione dei reati di specie tale che le persone possano commettere il reato soltanto eludendo fraudolentemente i modelli di organizzazione e di gestione.

# Le azioni di reazione

- Per quanto riguarda la minaccia, questa è legata prevalentemente alla storicità interna ed esterna all'ente. Ovvero devono essere considerati i casi in cui reati della stessa specie sono stati già commessi dall'ente e/o da enti aventi analoghe finalità e modalità operative, e/o da altri enti nel territorio ove opera l'ente in esame.
- Ai fini della presente esposizione le minacce di origine naturale hanno trascurabile rilevanza, mentre sono importanti quelle legate agli aspetti umani sia all'interno che all'esterno dell'ente.

# Le azioni di reazione

- Il fattore esterno è importante sia per quanto riguarda le minacce di origine umana (si consideri ad esempio il rischio di infiltrazione della criminalità organizzata - - ‑ Gruppo XI-- ‑ , al fine di determinare la probabilità di accadimento è importante analizzare non solo la storicità interna dell'ente, ma anche la storicità legata al territorio ed alla tipologia dell'ente stesso), sia per quanto riguarda le minacce di origine naturale (si consideri l'importanza della giacitura rispetto, ad esempio, il rischio di perdita dati in relazione ad eventi naturali quali un terremoto).

# Le azioni di reazione

- La vulnerabilità è certamente l'elemento del rischio ove deve essere concentrata l'attenzione. Come si è detto la vulnerabilità si percepisce analizzando le componenti reali, dovendo prevenire la commissione di reati, la componente umana assume l'aspetto prioritario non solo per l'analisi, ma anche per implementare le attività di reazione. In successione le informazioni rappresentano una rilevante criticità, in quanto, come si è detto, esse possono rappresentare sia il bene offeso dal reato, che lo strumento di commissione del reato, che, infine, lo scopo per cui è commesso il reato.

# Le azioni di reazione

- Le risorse economiche ed in particolare quelle finanziarie, sono anch’esse una componente critica, sia in considerazione del fatto che in un ente esse ne costituiscono l’essenza, sia perché anche esse possono rappresentare il bene offeso, lo strumento e lo scopo del reato.

# Le azioni di reazione

- L’opera231 è uno dei più completi esempi di interdisciplinarietà, in ragione delle disomogenee tipologie dei rischi che devono essere affrontate e della pervasività delle attività che devono essere affrontate nell’ente.
- Questa caratteristica rappresenta anche la maggiore difficoltà  per chi si accinge ad operare, si tratta di un’opera di ingegneria ove devono essere organizzate le risorse professionali(team) e gli strumenti con cui operare.
- Questa difficoltà, che già appare in fase di analisi, si presenta ancor più evidente nella fase di attuazione, occorre allora individuare un metodo da seguire in modo da garantire la completezza della attività, la tracciabilità ed evidenza delle scelte operate (si rammenta che il giudizio in materia 231è un giudizio di diligenza dell’ente).

# Le misure di sicurezza

- Questa attività di ordinamento deve riflettersi innanzitutto nella predisposizione delle azioni di reazione.
- Considerando il rapporto tra 231 e le norme tecniche, cui si è già accennato, occorre preliminarmente individuare le zone “buie”dell’ente ovvero, quelle zone, ove sono state collocati rischi, che non sono coperte, a livello operativo, da norme tecniche già attuate dall’ente. In queste zone occorre agire attraverso “misure di sicurezza” o “controls”. Ad esempio, se in un ente non è implementato un sistema di protezione delle informazioni, si dovrà tenere conto delle misure, anche a livello operativo, coerenti quali quelle dell’ISO/IEC 27001. Esse dovranno essere coordinate con le azioni ai piani superiori dell’ente di natura strategica, organizzativa e gestionale.

# I protocolli

- L’art. 6 Co. 2 Lett. b) del D.Lgs. 231/2001, riguardo i requisiti che devono essere soddisfatti dal MOG, testualmente prescrive: “prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire”.
- Dal tenore della norma si evince che i "protocolli 231” sono complessi di attività e risorse tra loro interagenti per la migliore organizzazione e gestione dell’ente al fine di ridurre i rischi 231. La funzione di tali attività si esplica evidentemente, con un processo top-down, secondo i piani decisionali. Essi devono fornire dunque indicazioni sia a livello strategico che organizzativo in modo che possano tradursi poi sul piano operativo.
- Si tratta di un’azione verticale rispetto ai piani dell’ente, che opera secondo i sistemi tale per cui questi ultimi possono essere adottati come elemento di classificazione dei protocolli.

# I protocolli

# I protocolli

- I “Protocolli 231”, dunque, si possono distinguere a seconda del sistema dell’ente cui appartengono e del livello da cui dipendono.
- Coerentemente alle considerazioni già svolte, al fine di garantire l’obiettività, condivisibilità e ripetibilità che deve caratterizzare ogni fase dell’opera 231 è opportuno che la scelta e la definizione dei “Protocolli 231” siano basate sulla esperienza, su standard, good practice, frame work internazionali, conosciuti e condivisi.
- I compiti e le responsabilità per la scelta, l’adozione, l’attuazione, l’aggiornamento dei protocolli devono altresì essere esplicite, chiare, precise, segnate e formalizzate in modo da poter valere nelle sedi giudiziali.
- I “Protocolli 231”, per la loro realizzazione, utilizzano sia le risorse interne che esterne dell’ente.

# I protocolli

- I protocolli così definiti non solo partecipano alla fase di reazione ma rappresentano un importante momento della analisi avanzata dei rischi.
- Infatti, la determinazione dei rischi che normalmente è svolta nel primo ciclo di analisi, determina dei valori di rischio teorici, ovvero indicativi di cricità. Questo aspetto è estremamente utile, in prima battuta quando, al fine di ottimizzare le risorse a disposizione per l'analisi, si parte da una vista d'insieme per individuare gli aspetti da sottoporre a focus. Nel ciclo di analisi successivo, però, è opportuno riscontrare quanto teoricamente accertato sulla base dei feedback che provengono dalla implementazione e dal monitoraggio, al fine di conferire maggiore realismo ai valori attributi.
- Collocando i protocolli accanto ai rischi che essi contrastano e che sono stati già individuati nell'ente, si definisce lo stato ideale cui l'ente deve tendere (se l'ente ha adottato tutti i protocolli previsti il rischio è già ridotto ai livelli desiderabili). Dalla misurazione dello stato attuale (ovvero lo stato di implementazione dei protocolli suggeriti) per differenza rispetto allo stato ideale, si misura realisticamente il livello di rischio dell'ente.
- Maggiore sarà la differenza, più alta sarà la vulnerabilità e, di conseguenza, maggiore sarà il rischio cui l'ente è esposto.

# I protocolli

- Da un punto di vista pratico si suggerisce di predisporre delle specifiche schede ove descrivere i protocolli. Ciascuna scheda dovrebbe identificare in modo univoco il protocollo secondo la sua azione, ovvero il sistema su cui agisce,indicando le azioni che devono essere poste in essere,le responsabilità per tali azioni, gli output documentali, le norme, standard di riferimento. Per ciascun protocollo deve essere individuato il rischio od i rischi che vengono ridotti.
- Riprendendo la similitudine tra enti ed esseri viventi, se si considerano i rischi come malanni che vogliono essere evita e prevenuti, i protocolli si comportano come “medicine” alcuni saranno mirati per alcuni rischi, altri saranno a più ampio spettro, agendo su più sistemi o sull’intero ente.

# Scheda d’esempio

| **Organizzazione** | **ICT** | **02** | Responsabilità |
|---|---|---|---|
| L’organizzazione dell’IT deve considerare i requisiti per i gruppi, le abilità, le competenze, l’affidabilità, l’autorità, i ruoli, le funzioni, i compiti, le responsabilità e la supervisione delle persone. Questa organizzazione deve essere definita e formalizzata in un framework ed in un processo che assicuri chiarezza, trasparenza e controllo.<br>Deve essere assicurato il diretto collegamento e coordinamento tra i livelli centrali e periferici dell’ente, sia geograficamente sia all’interno di unità complesse.<br>L’articolazione deve essere proporzionata alle dimensioni ed alla complessità dell’ente e del suo sistema IT. | | | |
| Piano strategico IT<br>Policy IT<br>Piani IT | Vertici<br>Alto Management | ISO 38500<br>COBIT 4.1. PO4 | |

# I protocolli

Nella scheda d'esempio che precede, nella prima cella in alto a sinistra è indicato il sistema su cui il protocollo esplica la propria azione, nella cella subito accanto è indicato il settore specifico (nell'esempio si tratta di un protocollo specifico per l'ICT ovvero il sistema informatico), nelle celle a destra è indicato un numero progressivo di identificazione ed un nome descrittivo del protocollo.

Subito sotto c'è il contenuto del protocollo, ovvero le azioni che esso prescrive.

In basso da sinistra, sono indicati gli output documentali ove il protocollo può trovare collocazione (questi variano in relazione alle specifiche caratteristiche dell'ente), quindi sono indicati coloro cui spetta la responsabilità di attuazione del protocollo, infine le norme, standard, framework da cui il protocollo è attinto.

# La vigilanza

- La vigilanza è una delle più importanti attività,prevista dal D.Lgs.231/2001 quale condizione essenziale di validità del MOG. Recita infatti l'art.6 Co.1 lett.b)"l'ente non risponde se prova che il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziava e di controllo". Generalmente questo compito è affidato all'Organismo di Vigilanza (OdV), tuttavia, in enti di modeste dimensioni e complessità tale compito può essere svolto direttamente dall'organo dirigente (Art.6 Co.4).
- La funzione di vigilanza,per essere idonea, deve soddisfare requisiti di autonomia, indipendenza, competenza ed obievità. Ciò comporta che organizzativamente tale funzione deve essere collocata in una posizione elevata della scala gerarchica, in modo da ridurre al minimo ogni possibile ingerenza da parte delle altre funzioni dell'ente. Coerentemente,come prescritto dal richiamato ISO 38500 riguardo la responsabilità, tale funzione deve essere dotata di poteri adeguati in modo da garantire lo svolgimento del compito assegnato.

# La vigilanza

- Appare opportuno che chi svolge funzioni di vigilanza non eserciti attività gestorie al fine di evitare il classico conflitto del controllore che controlla se stesso. Anche nel caso degli enti semplici, qualora il compito di vigilanza sia affidato ad un componente del Consiglio di Amministrazione, appare opportuno che questi non riceva incarichi di natura gestionale.
- Critiche per l'attività di vigilanza sono le informazioni considerate nella duplice direzione dall'OdV verso l'ente ed i suoi stakeholder e viceversa.
- L'art. 6 Co.2 Lett. d) infatti prescrive che il MOG preveda:"obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli".
- In particolare le informazioni devono soddisfare sia i criteri quantitativi di sufficienza e non eccedenza (un eccesso di informazioni paralizzerebbe la funzione di vigilanza) sia i criteri qualitativi di integrità,disponibilità, autenticità e riservatezza.

# La vigilanza

- L’ente deve quindi predisporre uno specifico piano di comunicazione da e per l’OdV, supportato da una specifica analisi dei rischi che consideri i requisiti sopra enunciati. Perché il piano funzioni, è essenziale che esso sia integrato con una coerente attività di formazione ed informazione destinata non solo ai diretti interessati (tutti coloro che operano per l’ente indipendentemente da i livelli), ma anche agli indiretti interessa (p.es. fornitori, clienti, rappresentanti di categoria, autorità).

# I rapporti tra le vigilanze

Questione particolarmente delicata assume il rapporto tra l'OdV, gli altri organismi di controllo  e le altre funzioni dell'ente.

I rapporti tra le funzioni di controllo è opportuno che siano definiti e coordinati in special modo quelli tra organismi dotati di autonomia ed indipendenza quali il Collegio Sindacale ed il Collegio dei Revisori dei Conti. Tali organismi in virtù della loro indipendenza ed autonomia che si fonda direttamente nelle leggi godono di un rango paritario e dividono le attività in ragione della loro specializzazione.

Le diverse funzioni di controllo quali ad es. il controllo di gestione, l'internal audit, il security officer, il privacy officer, occupando un rango inferiore prestano il loro supporto e collaborazione alle richieste dell'OdV.

In ogni caso si ribadisce che l'OdV non può e deve svolgere attività diverse dalla vigilanza e ciò anche quando parrebbe che la norma gli affida tali compiti (ad esempio la cura dell'aggiornamento del MOG); questa posizione, super partes, si riflette negli output dell'OdV che, ad esempio, riguardo la cura del MOG fornirà le propri indicazioni e prescrizioni alle altre funzioni dell'ente cui spetterà l'attuazione.

# La disciplina

- L’art.6  Co.2 Lett.e) del D.Lgs.231/2001, riguardo la responsabilità che discende da reati commessi dalle figure apicali, stabilisce che il MOG deve rispondere alla seguente esigenza: “introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello”.
- Nel successivo art.7 co.4 lett.b), riguardo la responsabilità derivante da i reati commessi dai sottoposti, nel prevedere i requisi per l’efficace attuazione del MOG, ribadisce la necessità di “un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello”.
- La disciplina è dunque uno degli elementi portanti del MOG, anche per essa è critica la gestione delle informazioni secondo due aspetti.
- Il primo aspetto è legato strettamente alle funzioni di controllo ed alla qualità delle informazioni che sono prodotte da questo apparato, infatti i provvedimenti disciplinari sono reazioni a comportamenti scorretti la cui rilevazione è appunto legata alle attività di controllo. A tal proposito è essenziale che le informazioni raccolte dalle attività di controllo e destinate ad essere utilizzate ai fini di disciplina siano quantitativamente e qualitativamente di alti livelli, con particolare considerazione ai requisiti previsti dalla legge quale valenza probatoria nei giudizi.

# La disciplina

- Il secondo aspetto è invece legato alla espressa previsione tra le ipotesi che configurano illecito disciplinare dei comportamenti scorretti inerenti all'uso delle informazioni.
- L'individuazione dei comportamenti scorretti è strettamente legata alla governance del sistema informavo in quanto presuppone una chiara definizione di compiti e responsabilità da cui evincere e valutare i comportamenti scorretti che devono essere oggetto di valutazione e d'azione disciplinare.
- La chiara, espressa e formale previsione di compiti e responsabilità oltre a costuire un prerequisito logico, costituisce anche requisito di legimità dell'azione disciplinare secondo il principio in base al quale non può essere contestato ciò che non è stato richiesto.
- Da un punto di vista pratico spesso gli enti offrono gravi carenze sotto questo profilo che vanificano di fatto il MOG infatti:
  - Per quanto riguarda i lavoratori subordinati spesso si limitano a rinviare alla CCNL che, riguardo alle specifiche ipotesi legate ai sistemi informavi, è vaga se non esistente.
  - Per quanto riguarda le funzioni dirigenziali ed i vertici la situazione è ancor più carente (chi punisce l'Amministratore Delegato?).
  - Per quanto riguarda infine le collaborazioni, lavoratori autonomi, partnership, le lacune sono spesso presenti ove non esiste un corpus di clausole contrauali dedicate al corretto trattamento delle informazioni.

# Il processo 231

Dalla panoramica sin qui svolta appare evidente che estremamente complessa è l'opera legata alla conformità al D.Lgs. 231/2001, tanto che è opportuno raccogliere ed organizzare le singole attività in un processo specifico che può essere denominato "Processo 231".

Si tratta di un processo ciclico, sia perchè la norma espressamente prevede che il MOG sia mantenuto aggiornato (Art. 6 Co.1 Lett. b) D.Lgs. 231/2001), sia per la caratteristica dinamica del Decreto che, come si è detto, si comporta come un contenitore aperto che si arricchisce nel tempo di nuove ipotesi di reato, sia infine per la caratteristica degli enti, che, in quanto organismi vivi, nella loro storia si modifica continuamente per adattarsi all'ambiente in cui vivono.

# Il processo 231

Essendo il processo "231" orientato al miglioramento continuo, ben può essere utilizzato il noto ciclo di Deming che struttura in quattro fasi l'andamento delle attività.

PLAN – Pianificare, il processo deve essere avviato da una attività di pianificazione che determini gli obiettivi ed organizzi le attività.

DO – Attuare, l'attività di pianificazione deve filtrare dalla strategia alla tattica sin fino all'operatività per dar luogo all'efficace attuazione di quanto adottato (Art. 6 Co.1 Lett.a) D.Lgs. 231/2001.

CHECK – Controllare, l'andamento del processo deve essere monitorato ed infine verificato per stabilirne l'efficacia.

ACT – Reagire, sulla base delle informazioni di controllo occorre individuare le azioni proattive e reattive necessarie ed opportune. Queste costituiranno la base per la pianificazione che avvierà i cicli successivi. Traslando la figura su un piano tridimensionale la cui altezza esprime il tempo, il cerchio assumerà la forma di una spirale che si avvita verso l'alto restringendosi sempre più per effetto del miglioramento continuo.

Questa spirale non si chiuderà mai perchè i rischi, seppure ridotti a livelli infinitesimali, continueranno comunque a sussistere secondo il principio per cui non è possibile la sicurezza assoluta.

# Il processo 231

Se il processo può essere definito come il "complesso di attività e risorse tra loro organizzate al fine di mantenere conforme ed allineato l'ente alle disposizioni prescritte dal D.L.vo 231/2001 e successive modifiche od integrazioni", l'obiettivo primario è la conformità al D.L.vo 231/2001 al fine di mantenere indenne l'ente dalle responsabilità amministrative previste dalla norma.

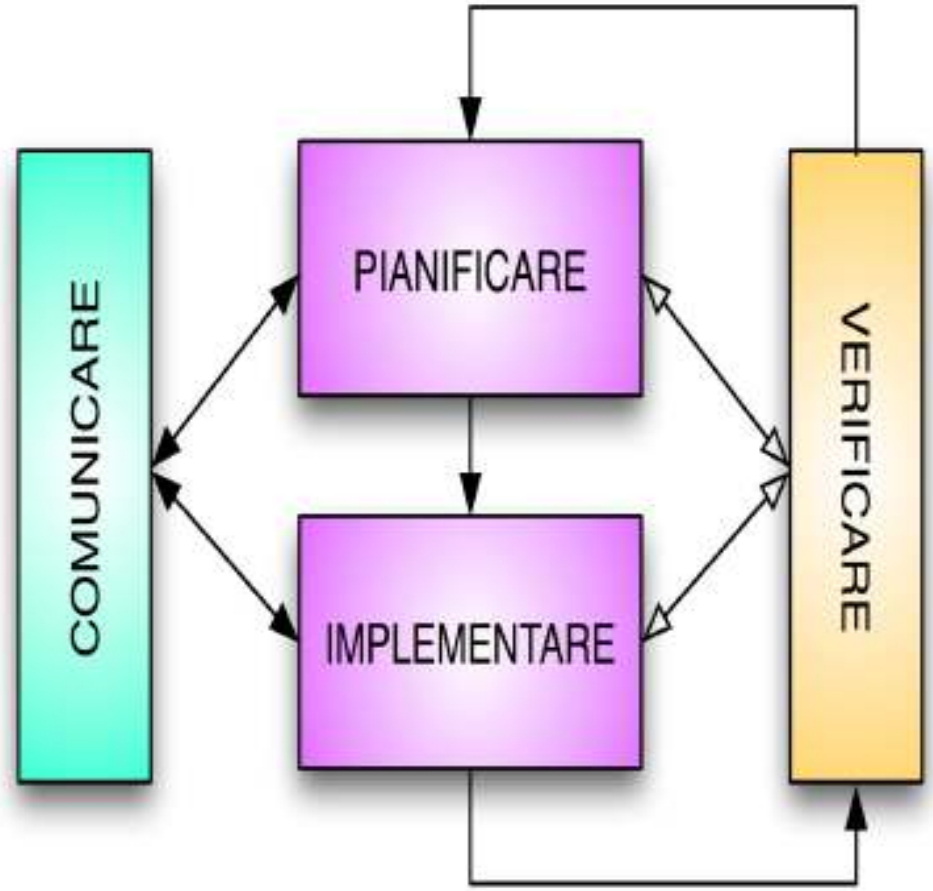
La responsabilità del processo spetta al vertice amministrativo dell'ente cui la norma affida il compito di "adottare ed efficacemente attuare" il MOG (Art.6 Co. 1 Lett. a) D.Lgs. 231/2001.

Naturalmente il vertice può delegare compiti relativi al processo a soggetti che per esperienza, affidabilità e competenze offrano le massime garanzie di miglior adempimento, mantenendo le funzioni di indirizzo e l'obbligo di vigilarne, sotto la propria responsabilità, la corretta opera.

E' opportuno che la delega dei compiti sia scritta ed indichi specificamente e chiaramente i compiti e le responsabilità delegate.

# Il processo 231

In ossequio alla caratteristica ciclicità del processo, questo, anche grazie al supporto delle funzioni funzione di cura ed aggiornamento del MOG affidate all'OdV (Art. 6 Co.2 Lett.b) D.Lgs. 231/2001), deve essere regolarmente revisionato almeno una volta l'anno e, straordinariamente, ogni volta che si verifichino importanti e rilevanti mutamenti organizzativi dell'ente ovvero della normativa di riferimento, ovvero si sia verificato un grave incidente. Semplificando ed adattando il ciclo di Deming il processo potrebbe essere illustrato come a lato.



# Il processo 231

Nella fase di pianificazione:

- sono individuati e formalizzati gli obiettivi ed i limiti del processo,
- è definita la strategia per il loro raggiungimento,
- sono definite ed individuate le risorse per l'attuazione del processo,
- sono definiti i ruoli ed assegnate le responsabilità,
- sono definite le direttive in base alle quali le risorse dovranno essere gestite,
- sono definiti i tempi di attuazione,
- sono individuati i soggetti destinatari del piano di comunicazione.

Nella fase di implementazione sono attuate le direttive definite nella fase precedente.

La verifica si sviluppa secondo due diversi aspetti:

- durante l'esecuzione delle fasi di "pianificazione" ed "implementazione" quale complemento di queste attraverso il monitoraggio delle fasi stesse (frecce con la punta bianca). Il monitoraggio deve essere effettuato in modo da guidare le attività in modo da garantire costantemente il rispetto della strategia definita e dei tempi assegnati.
- al termine della "implementazione" quale autonoma fase di verifica dell'efficacia ed efficienza di quanto attuato. Periodicamente è opportuno che la verifica venga effettuata da un soggetto esterno all'ente al fine di garantire l'efficienza ed obiettività della verifica effettuata dagli organismi interni.

Contemporaneamente all'esecuzione delle fasi centrali (pianificazione ed implementazione) deve essere mantenuto attivo un sistema di comunicazione tra i soggetti che conducono il processo, l'ente, i referenti e gli stakeholder rilevanti , in modo da renderli partecipi e consapevoli delle attività in corso, guadagnandone la collaborazione e beneficiando degli eventuali feedback.

# Il processo 231

La formazione “231” chiude il processo costituendone un elemento essenziale perchè attraverso di essa si costruisce l’ambiente “sano” che consente l’efficace attuazione del MOG.

Essa, infatti, è condizione preliminare per garantire i corretti comportamenti e correggere quelli scorretti ed è importante elemento di valutazione ai fini della vulnerabilità dell’ente.

Deve essere predisposto annualmente un programma di formazione differenziato nei contenuti e modi a seconda dei destinatari.

Devono essere stabiliti i ruoli e le responsabilità per l’implementazione ed i controlli.

Le attività di formazione devono essere verificate per misurarne l’efficacia.

Sotto il profilo strettamente legato alle informazioni è opportuno che tale attività (con particolare riferimento alla analisi che ne costituisce il presupposto) sia documentata secondo i medesimi livelli previsti per il MOG in quanto elemento determinante per la valutazione di idoneità, efficacia ed adeguatezza.

# Grazie

www.vincenzocalabro.it