UNIVERSITÀ DEGLI STUDI DI MILANO

DR. EMANUELE MERONI

[GESTIONE SICUREZZA]

STANDARD ISO

19011	27035	27037	27043
AUDIT	GESTIONE INCIDENTI	CATENA DI CUSTODIA	BEST PRACTICE

19011

Guida sui principi dell'attività di gestione qualità **AUDIT** (e del sistema di gestione AMBIENTALE)

ossia una VALUTAZIONE indipendente e obiettiva svolta da un AUDITOR che sulla base di

un campionamento **mira a ottenere prove**, al fine di stabilire in quale misura i criteri prefissati siano stati soddisfatti o meno.

➔ Ha un margine di errore dovuto al fatto che attesta un risultato complessivo a partire da un numero limitato di elementi selezionati. Questo è dovuto alla limitatezza delle risorse che si possono mettere a disposizione per un audit[3].

TIPI: Interni / Esterni / Coordinato / Congiunto

27035 Linee guida sugli aspetti della GESTIONE DEGLI INCIDENTI

Poc (Point of Contact) ruolo aziendale: coordinamento attività per la gestione dell'incidente informatico

CSIRT (Computer Security Incident Response Team) **IRT** (Incident Response Team)

l'information security **EVENT**, che a sua volta può causare l'**INCIDENTE** info.

27037 SI OCCUPA DELLE **FASI INIZIALI** DEL PROCESSO: non l'analisi (CATENA DI CUSTODIA)

Documentazione (logging)	Tracciabilità (chain of custody)	Priorità di intervento (plan)
Imballaggio dei reperti (protection)	Trasporto dei reperti (real/virtual)	Ruoli nel passaggio dei reperti (who & why)

DEFRs Digital evidence **FIRST RESPONDERS** qualificata per operare per primo sulla scena del crimine al fine di raccogliere e acquisire prove digitali con il compito di imballare e conservare la prova
DESs Digital evidence **SPECIALISTS** Persona che può svolgere i compiti di un DEFR e ha conoscenze, competenze e capacità specialistiche per gestire una vasta gamma di questioni tecniche

UNIVERSITÀ DEGLI STUDI DI MILANO

DR. EMANUELE MERONI

27043 promuovere le **best practices** forensi e i processi per **l'acquisizione/l'analisi** di prove digitali

PRE identificazione dell'incidente: **READINESS** strategie per garantire "prontezza" e correttezza
POST identificazione dell'incidente

FASI : raccolta, acquisizione, conservazione, analisi, interpretazione e presentazione dei dati

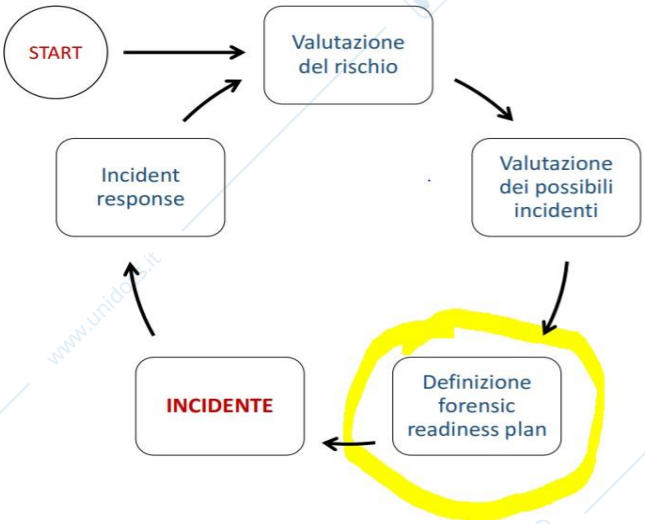
➔ **EXPERT WITNESS**: figura esperta che affianca il giudice x analizzare elementi;
Fattori chiave PERTINENZA/AUTENTICITA'

READINESS PLAN (piano di PRONTEZZA – re'diness)

MASSIMIZZARE L'EFFICACIA DELL'AZIONE IN CASO DI INCIDENTE informatico minimizzando l'effetto e costo

➔ DEFINIZIONE di SCENARI di Business,ruoli, politiche di MONITORAGGIO, modalità di GESTIONE

ROI (Return of Investiment) velocità individuazione attacco



UNIVERSITÀ DEGLI STUDI DI MILANO

DR. EMANUELE MERONI

PIÙ SI FA **PREVENZIONE** **(readiness)**, MEGLIO SI RISOLVONO I PROBLEMI: phishing/PHARMING

	Incident leader	Referente IT	Referente Legale	Referente informatica forense	Referente P.R.	Management
Valutazione iniziale	**Responsabile**	Collabora		Aggiornato		
Risposta iniziale	**Responsabile**	Implementa	Aggiornato	Aggiornato	Aggiornato	Aggiornato
Raccolta evidenze informatiche	Collabora	Collaboratore	Aggiornato	**Responsabile**		
Soluzione temporanea	**Responsabile**	Implements	Aggiornato	Collabora	Aggiornato	Collabora
Comunicazioni con l'esterno	Collabora	Collabora	Collabora		Implementa	**Responsabile**
Rapporti con l'autorità giudiziaira	Aggiornato	Aggiornato	**Responsabile**	Collabora	Aggiornato	Collabora
Soluzione definitiva all'incidente	**Responsabile**	Implementa	Aggiornato		Aggiornato	Aggiornato
Valutazione dell'impatto dell'incidente e dell'operato dei vari membri	Aggiornato	Aggiornato	Collabora		Aggiornato	**Responsabile**

Definiamo **INCIDENTE** ogni situazione di **VIOLAZIONE**

(Es **HOAX** è un finto virus/messaggio che indica di cancellare un file per migliorare il sistema; in realtà il file da eliminare è una componente essenziale del S.O.)

- ➔ Tenere a mente che la casa produttrice non direbbe mai dell'esistenza del virus VIA MAIL
- ➔ Se cancelli la mail/il sw non pensare di averlo definitiv. Cancellato (CARVING)

ENISA European Union Agency for Cybersecurity

offre un progetto europeo: **TRANSITS** per formare figure CSIRT https://www.enisa.europa.eu/

Compiti di un CSIRT:

- ➔ Creazione **BOLLETTINO**: tabella in cui è presente la descrizione della vulnerabilità nel dettaglio

Identificativo bollettino	**Bollettino sulla sicurezza di Microsoft MS06-042**
Titolo del bollettino	**Aggiornamento cumulativo sulla sicurezza per Internet Explorer (918899)**
Sintesi	Questo aggiornamento risolve diverse vulnerabilità presenti in Internet Explorer che potrebbero consentire l'esecuzione di codice da remoto.
Valutazione della gravità massima	Critico
Impatto della vulnerabilità	Esecuzione di codice da remoto
Software colpito	**Windows, Internet Explorer.** Per ulteriori informazioni, cfr. la sezione Software colpito e locazioni per il download.

UNIVERSITÀ DEGLI STUDI DI MILANO

DR. EMANUELE MERONI

CASI DI STUDIO

PERIZIA: Analisi tecnica redatta da un esperto al fine di scrivere una

DICHIARAZIONE **PERITALE**: un verbale in cui è descritto il dettaglio in caso (Certificazione SW)

INCIDENTE: CSIRT

GESTIONE DEGLI INCIDENTI INFORMATICI

CATENA DI CUSTODIA

Data e ora di creazione:
Identificativo reperto (codice progressivo aziendale):
Tipo di reperto:
Descrizione dettagliata reperto (s/n, marca, modello, dimensione…):
Modalità di raccolta:
Data e ora di raccolta:
Luogo di raccolta:
Modalità di acquisizione:
Data e ora di acquisizione:
Luogo di acquisizione:
Strumento utilizzato per l'acquisizione:
Descrizione dettagliata dispositivo contenente la copia forense (s/n, marca, modello, dimensione…):

Passaggi di consegne

Data, ora e luogo:
Da (nome, ruolo e organizzazione):
Firma
A (nome, ruolo e organizzazione):
Firma
Motivazione:

Data, ora e luogo:
Da (nome, ruolo e organizzazione):
Firma
A (nome, ruolo e organizzazione):
Firma
Motivazione:

+ LOG comunicazione incid. + ripristino/Back Up

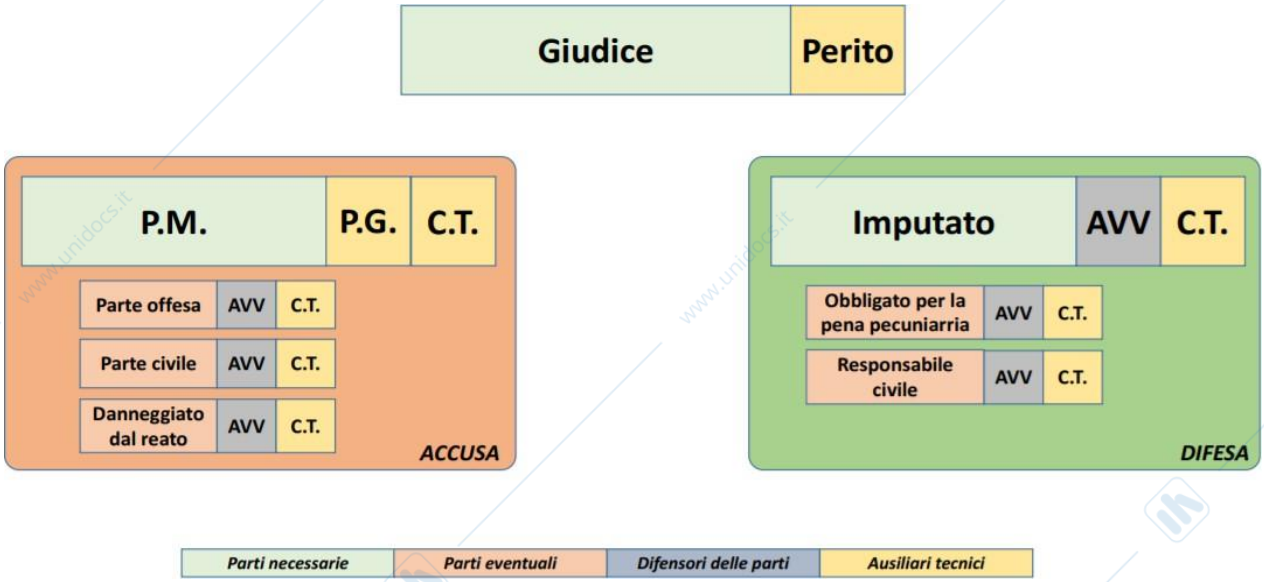
CHERRY PICKING 🍒 fallacia logica che si esplica nel selezionare le sole prove a sostegno della propria tesi, ignorando le prove che la smentiscono

UNIVERSITÀ DEGLI STUDI DI MILANO

DR. EMANUELE MERONI

PARTI PROCESSUALI procedimento penale: ATTORI

successione di atti e/o comportamenti che da un evento (notizia di reato: La notitia criminis)
giungono ad una decisione (sentenza)



GIUDICE:

- G.**I**.P. Indagini Preliminari
- G.**U**.P **Udienza** Preliminare (Non sempre presente)
- GIUDICE del DIBATTIMENTO

PERITO: Nominato dal giudice x ausilio (COADIUVA) LEALTA' CORRETTEZZA TRASPARENZA BUONA FEDE

P.M. = PUBBLICO MINISTERO "**dominus** (ha il potere di decidere) **dell'azione penale** **ACCUSA**

P.G. = Polizia GIUDIZIARIA

C.T. = Consulente TECNICO
Parte OFFESA può non presentarsi: eventuale

IMPUTATO può non presentarsi: CONTUMACE obbligatorio la presenza di un **DIFENSORE;**

FASI:

- **Indagini** prelim(P.M. richiesta archiviazione/offesa opposizione)
- **Udienza** pre. (Non luogo a procedere/decreto dispone di GIUDIZIO se P.M. raccoglie suff. Prove per sostenere un'accusa)

UNIVERSITÀ DEGLI STUDI DI MILANO

DR. EMANUELE MERONI

- **Dibattimento** decisione su istanze probatorie delle parti: testi, perizie
- Decisione con **SENTENZA**

PROCESSO solo quando P.M. esercita azione penale

RACCOLTA PROVE: ISPEZIONE tutte la slide

*****VOCABOLARIO*****

Dirimere = solvere, per lo più con una decisione autorevole / dividere
Ricusare = respingere
Obbligo Deontologico = insieme regole morali
Coatta = imposto
Esiguo = modesto
Contenzioso = contesa/controversia giudiziaria
Probatoria = prove
FIDEFACENTE = ausiliare del NOTAI: attesta l'IDENTITA' delle parti

PROCEDIMENTO CIVILE

ATTORE agisce in giudizio **chiama**ndo un'altra parte in processo

CONVENUTO parte che si **difende** dall'altrui chiamata in giudizio con la **COMPARSA DI RISPOSTA** (raccolta di prove)

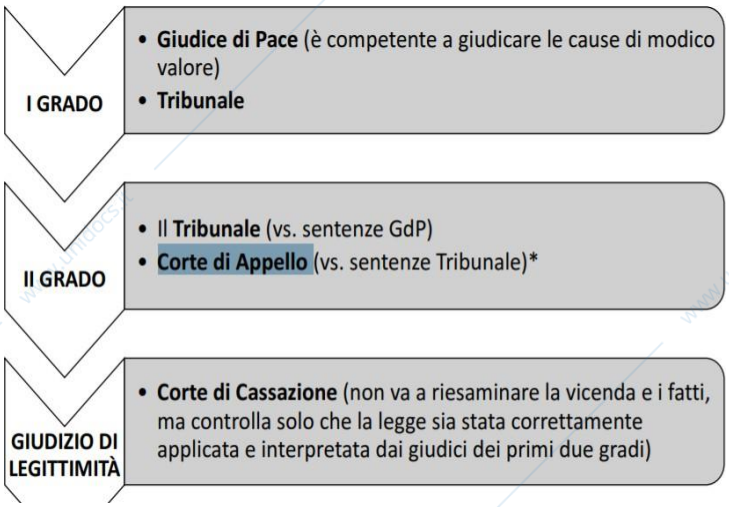
C.T.P. Consulente Tecnico di Parte DIFENSIVA non ricusabile
C.T.U. Consulente Tecnico di Ufficio coadiuva il GIUDICE

UNIVERSITÀ DEGLI STUDI DI MILANO

DR. EMANUELE MERONI

Forme di GIURISDIZIONE con fasi: Introduttiva,Istruttiva, Decisoria + procedimenti SPECIALI

- COGNIZIONE chiedere un accertamento
- CAUTELARE conservi il bene in attesa del giudizio
- ESECUTIVA esecuzione forzata dei propri diritti
- VOLONTARIA controllare attività es: affidare minore



perché nel processo civile vige il principio di TIPICITA' delle PROVE (= il giudice usa quelle e soltanto quelle prove stabilite dalla legge), mentre in quello penale vale la regola dell'ATIPICITA' delle PROVE (=manca elenco tassativo di strumenti probatori)

	Definizione	Valore probatorio	Esempi
Firma Elettronica	Insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica	Efficacia probatoria valutabile dal giudice caso per caso	*Pin*, firma biometrica
Firma Elettronica Avanzata	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati	Efficacia probatoria della scrittura privata integra la forma scritta *ad substantiam* tranne che per i contratti immobiliari	Firma su *tablet*
Firma Elettronica Qualificata	Particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma	Efficacia probatoria della scrittura privata integra la forma scritta *ad substantiam*	*Smart-card, token*
Firma Elettronica Digitale	Particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici	Efficacia probatoria della scrittura privata integra la forma scritta *ad substantiam*	*Smart-card, token*

UNIVERSITÀ DEGLI STUDI DI MILANO

LAUREA MAGISTRALE
Dr. EMANUELE MERONI

D.Lgs. 231/2001 per la disciplina della **responsabilità amministrativa degli enti** dipendente da reato commesso da un soggetto appartenente ad essi (APICALI)

JOBS ACT riforma del diritto del lavoro in Italia volta a flessibilizzare il mercato del lavoro nell'intento di ridurre la disoccupazione