PRIMA GIORNATA TUTORIAL DAYS CCR
EDIZIONE 2021

Normativa di riferimento

I documenti INFN che recepiscono la normativa

Silvia Arezzini

4 Documenti da tenere presenti

- Disciplinare uso risorse informatiche
- Misure Minime
- Norme privacy
  - per l'uso dei sistemi informatici destinati al trattamento di dati personali
  - per il trattamento di dati personali

POCHI documenti, ma importanti!

Disciplinare uso risorse informatiche (a)

Delibera CD 15442 - 28/2/2020 *(anche CORSO SICUREZZA)*

L'INFN si dota di un DISCIPLINARE per:

«Salvaguardare la sicurezza del proprio sistema informatico e tutelare la riservatezza, l'integrità e la disponibilità delle informazioni e dei dati, anche personali, da questo prodotti, raccolti o comunque trattati.»

Nel disciplinare vengono date indicazioni all'AMMINISTRATORE DI SISTEMA

Chi è l'amministratore di sistema?

figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati, anche personali, compresi i sistemi di gestione delle basi di dati, le reti locali e gli apparati di sicurezza

AMMINISTRATORE DI SISTEMA

Disciplinare uso risorse informatiche (b)

- 1. mantenere i sistemi al livello di sicurezza appropriato al loro uso;
- 2. verificare con regolarità l'integrità dei sistemi;
- 3. controllare e conservare i log di sistema per il tempo necessario a verificare la conservazione degli standard di sicurezza;
- 4. segnalare immediatamente al Servizio di Calcolo e Reti incidenti, sospetti abusi e_violazioni della sicurezza e partecipare alla loro gestione;
- 5. installare e mantenere aggiornati programmi antivirus per i sistemi operativi che lo prevedono;
- 6. non visionare i dati personali e della corrispondenza di cui dovessero venire a conoscenza e comunque a considerarli strettamente riservati e a non riferire, né duplicare o cedere a persone non autorizzate informazioni sull'esistenza o sul contenuto degli stessi;
- 7. in caso di interventi di manutenzione, impedire, per quanto possibile, l'accesso alle informazioni e ai dati personali presenti nei sistemi amministrati;
- 8. seguire attività formative in materie tecnico-gestionali e di sicurezza delle reti, nonché in tema di protezione dei dati personali e di segretezza della corrispondenza.

AMMINISTRATORE DI SISTEMA

Disciplinare uso risorse informatiche (c)

L'INFN, nel rispetto dei principi di libertà e dignità, non consente l'installazione di strumentazioni hardware e software mirate al controllo degli utenti e vieta il trattamento effettuato mediante apparecchiature preordinate al controllo a distanza quali:

- a) la lettura e la registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per svolgere il servizio di posta elettronica;
- b) la riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dall'utente;
- c) la lettura e registrazione dei caratteri inseriti tramite tastiera o dispositivi analoghi;
- d) l'analisi occulta di computer portatili affidati in uso.

AMMINISTRATORE DI SISTEMA

Disciplinare uso risorse informatiche (d)

Al fine di assicurare la funzionalità, disponibilità, ottimizzazione, sicurezza ed integrità dei sistemi informativi e prevenire utilizzazioni indebite, l'INFN adotta misure che consentono la verifica di comportamenti anomali o delle condotte non previste dal presente Disciplinare nel rispetto dei principi generali di necessità, pertinenza e non eccedenza sopra richiamati. A tal fine il Servizio di Calcolo e Reti può eseguire elaborazioni sui dati registrati dirette ad evidenziare anomalie nel traffico di rete o condotte non consentite dal presente Disciplinare.

AMMINISTRATORE DI SISTEMA

MISURE MINIME(a)

il documento che definisce le

Misure minime di sicurezza ICT per le pubbliche amministrazioni

https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

(Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015) pubblicata sulla GU del 5-5-2017

- “Modulo di implementazione delle misure minime di sicurezza nell'Istituto Nazionale di Fisica Nucleare” Documento in data certa depositato dalla Presidenza il 20/12/2017 (modulo_implementazione_mm_v4.pdf)
- Note redatte in ambito CCR: Implementazione Misure Minime.pdf

SECURITY

MISURE MINIME(b)

Le misure minime in parte sono già previste nel disciplinare, ma sono più dettagliate negli aspetti tecnici.

Misure: MINIME, STANDARD, ADVANCED

Non solo un obbligo, ma una guida.

SECURITY

MISURE MINIME(c)

Una lettura ragionata del Modulo di Implementazione delle Misure Minime: un framewok di security per gli amministratori di sistema (seguono alcune slide con le misure da implementare)

ABSC: Agid Basic Security Control(s) ispirati a:

CSC: Critical Security Control(s) for Effective Cyber Defense, pubblicati da:

CIS, Center for Internet Security e originariamente noti come SANS 20

SECURITY

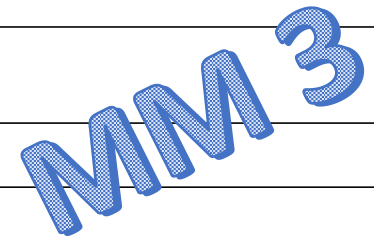
ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositi almeno l'indirizzo IP.	
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

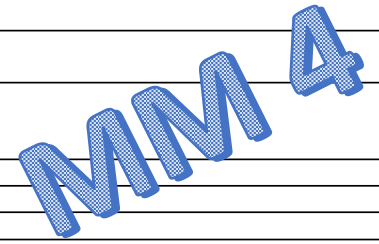
ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	MM 2
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	
2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	
3	1	2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	
3	1	3	A	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	
3	5	3	A	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	



ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	
4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	
4	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	
4	7	2	S	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	
4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	

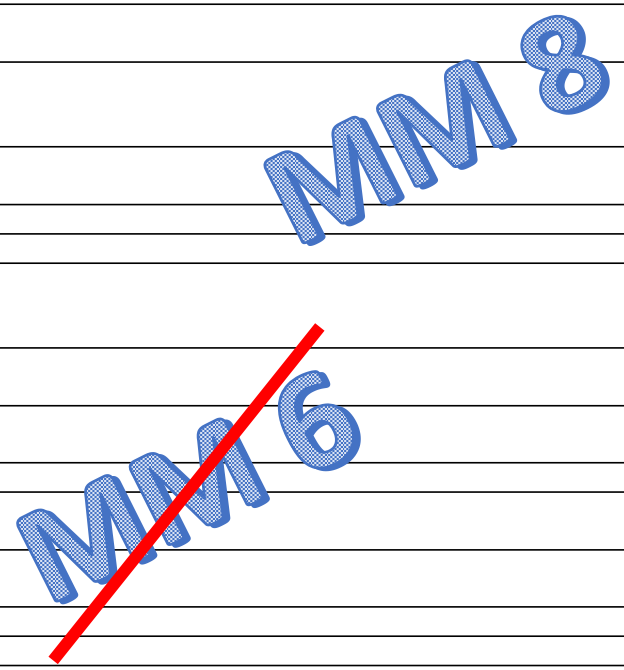


ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	
8	9	2	M	Filtrare il contenuto del traffico web.	
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	
8	11	1	S	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	



ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	MM 10
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	MM 13
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	
13	6	1	A	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	
13	9	1	A	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	

Norme privacy (a)

GDPR (Regolamento 2016/679) chiede: **misure adeguate** a proteggere i dati

INFN sceglie di considerare «adeguate» le Misure Minime, da accrescere, se necessario.

1 delibera CD e 2 documenti da non dimenticare:

- Delibera *n. 14844 del 27 Luglio 2018* : Figure e ruoli legati alla privacy
- Documento1: Norme per l'uso dei sistemi informatici destinati al trattamento di dati personali nell'INFN (allegato alla delibera)
- Documento 2: Norme per il trattamento di dati personali nell'INFN (*dicembre 2018*)

PRIVACY

Norme privacy (b)

Figure e ruoli legati alla privacy:

DPO Data Protection Officer (Responsabile Protezione Dati) delibera CD *n. 14734 del 27/4/ 2018*

Titolare: *L'Istituto Nazionale di Fisica Nucleare*

Il Direttore Generale dell'INFN, sentito il DPO, svolge funzioni di coordinamento tra i Direttori

Responsabile: Figura ESTERNA
Autorizzato: Soggetto designato dal Direttore al trattamento dei dati

PRIVACY

Norme privacy (c)

Norme per l'uso dei sistemi informatici destinati al trattamento di dati personali nell'INFN (allegato alla delibera)

Indicazioni e approfondimenti sull'applicazione misure minime:

- sistemi LINUX
- sistemi MAC-OS
- Sistemi WINDOWS

PRIVACY

Un buon punto di partenza…

L'attuazione delle presenti norme dovrà pertanto essere valutata in ciascuna Struttura ed eventualmente adattata alle particolari situazioni locali, *documentando con chiarezza* il motivo delle scelte fatte.

Norme privacy (d)

Norme per il trattamento di dati personali nell'INFN

- Una raccolta dei principali aspetti normativi
- Individuazione delle figure rilevanti in ambito privacy INFN
- Indicazioni anche pratiche per il trattamento di dati sia in froma cartacea che elettronica
- Una guida che aiuti tutti gli autorizzati al trattamento

PRIVACY

In caso di dubbi...

DPO@infn.it

PRIMA GIORNATA TUTORIAL DAYS CCR
EDIZIONE 2021

Normativa di riferimento

Il system manager e la privacy

Silvia Arezzini

Aspetti pratici legati alla PRIVACY

- Problematiche significative, connesse alla privacy, con le quali può trovarsi a contatto chi svolge attività di system management
- Il databreach
  - Procedura di segnalazione
  - Casi di databreach sanzionati dal Garante.

Consapevolezza

Alcuni dei PRINCIPI del GDPR a cui riferirsi

- Accountability
- Minimizzazione
- Privacy by Default e by Design

Consapevolezza

File di LOG

Il log file è il tipico file contenente dati personali che il sistemista è chiamato a trattare

- Ma il sistemista è in possesso di una nomina da parte del Direttore con l'incarico a trattare i dati personali,
- Quindi il log non è un problema, ma un lavoro, una attività!

La conservazione dei log è normata dal nostro disciplinare sull'uso delle risorse informatiche:

- Viene indicato come tempo di conservazione un anno, con l'unica eccezione dei log di sessioni web e proxy che devono essere rimossi entro 7 giorni, ma si sta valutando l'eventualità di portare a 1 mese questo termine.

- Non sono elencati tutti i tipi di log ma è sensato individuare in un anno il periodo tipico di conservazione

Data Base

Ad esempio:

DataBase degli asset, con associazione di utenti

Un altro esempio tipico di file, contenente dati personali trattati dai System Manager (vedi Misure Minime).

Non l'unico esempio

Attenzione…
Privacy e accesso a dati personali

E' una preoccupazione frequente dei sistemisti:

Nel corso del mio lavoro può capitare di «vedere» dati personali degli utenti

Qui non si tratta di applicare le norme sulla privacy, ma quelle sulla deontologia professionale

RISERVATEZZA

Anonimizzazione

Le problematiche di anonimizzazione di dati non sono in generale presenti nelle attività standard del sistemista INFN. Esse possono presentarsi in situazioni particolari ad esempio nel caso di progetti in cui siano presenti casi sanitari (dati biologici o genetici o neuroimmagini ecc). In questo caso, se si è chiamati a trattare questo tipo di dati, occorre prevedere misure specifiche.

Esiste una indicazione ad hoc del garante per dati genetici

Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101 [9124510] giugno 2019

In generale: dati da trattare con grande attenzione, esclusivamente nell'ambito di progetti.

CHIEDERE al DPO: esamineremo la questione e daremo un parere.

Cosa si può fare e cosa non si può fare in base al GDPR? Cosa c'è scritto?

Il GDPR non entra nel merito di contenuti specifici…

recita che i dati devono essere trattati in maniera lecita, quindi la domanda da porsi deve essere di questo tipo: "per questo specifico trattamento è lecito richiedere questo dato".

la risposta può essere negativa o affermativa a seconda del trattamento.

Data Breach(a)

Dal sito del GARANTE:

Alcuni possibili esempi:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

Data Breach(b)

COSA FARE IN CASO DI VIOLAZIONE DEI DATI PERSONALI?

Il titolare del trattamento (soggetto pubblico, impresa, associazione, partito, professionista, ecc.) **senza ingiustificato ritardo** e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, deve notificare la violazione al Garante per la protezione dei dati personali a meno che sia **improbabile** che la violazione dei dati personali comporti un **rischio** per i diritti e le libertà delle persone fisiche.

Procedure INFN: notifica al GARANTE, al DG, al DPO

Nel secondo caso notifica solo al DG e al DPO

Data Breach(c)

- **Le notifiche al Garante effettuate oltre il termine delle 72 ore** devono essere **accompagnate dai motivi del ritardo.**
- Inoltre, se la violazione comporta un rischio elevato per i diritti delle persone, il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.
- Il titolare del trattamento, a prescindere dalla notifica al Garante, **documenta** tutte le violazioni dei dati personali, ad esempio predisponendo un apposito registro. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.

Procedure INFN: un unico Registro delle violazioni, a cura del DPO

Data Breach(d)

COME INVIARE LA NOTIFICA AL GARANTE?

A partire dal 1° luglio 2021, la notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica.

Procedure INFN: la procedura telematica del GARANTE non è ancora completamente in funzione. Seguire le istruzioni sul sito DPO.

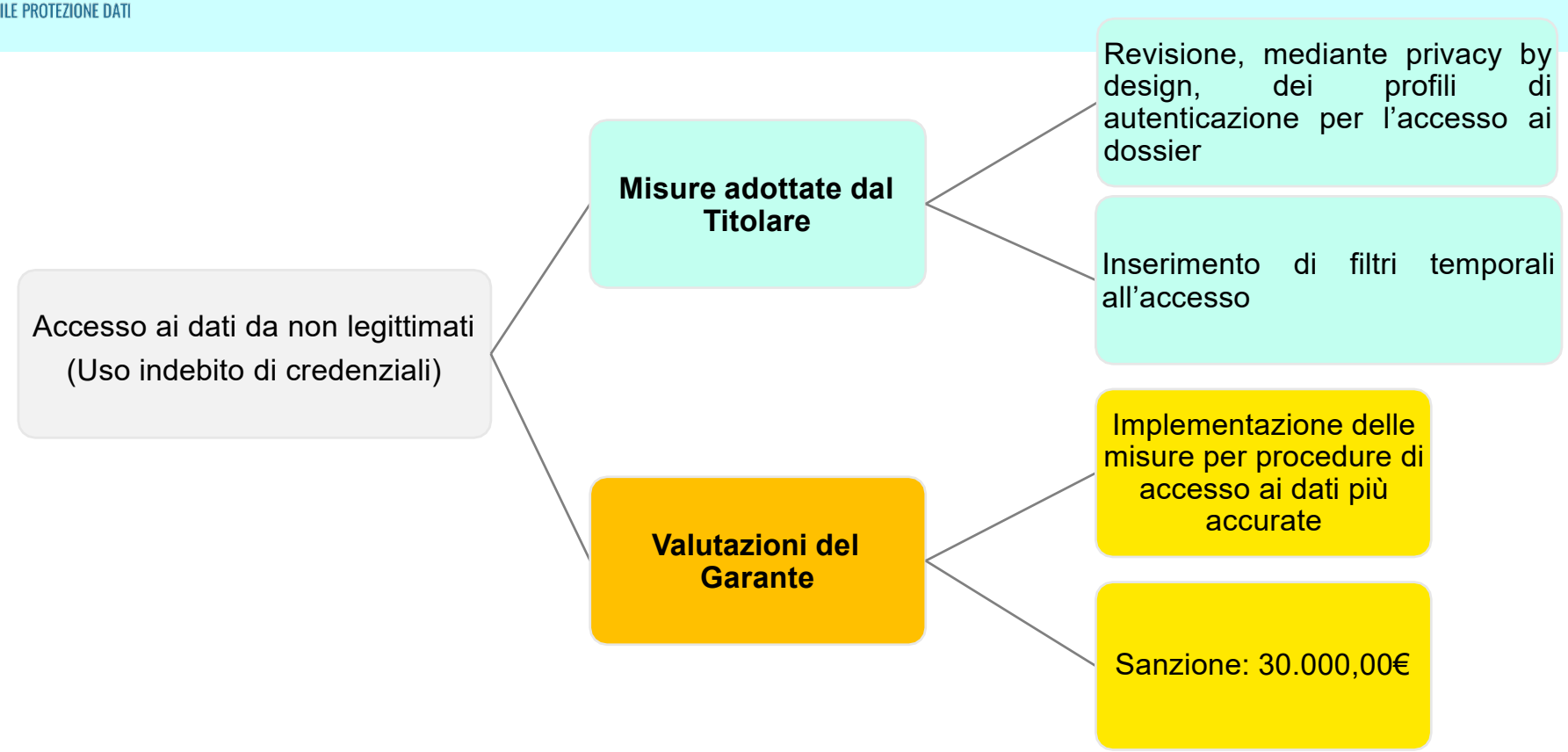
Data Breach(e)

Alcuni esempi di data breach sanzionati dal GARANTE

Sono stati presentati da Eleonora Bovo ad un recente corso del DPO destinato agli Amministratori di Sistema.

Attenzione a ciò che SEGNALA e SANZIONA il Garante!

Conseguenze delle violazioni



Autore E.Bovo

Conseguenze delle violazioni

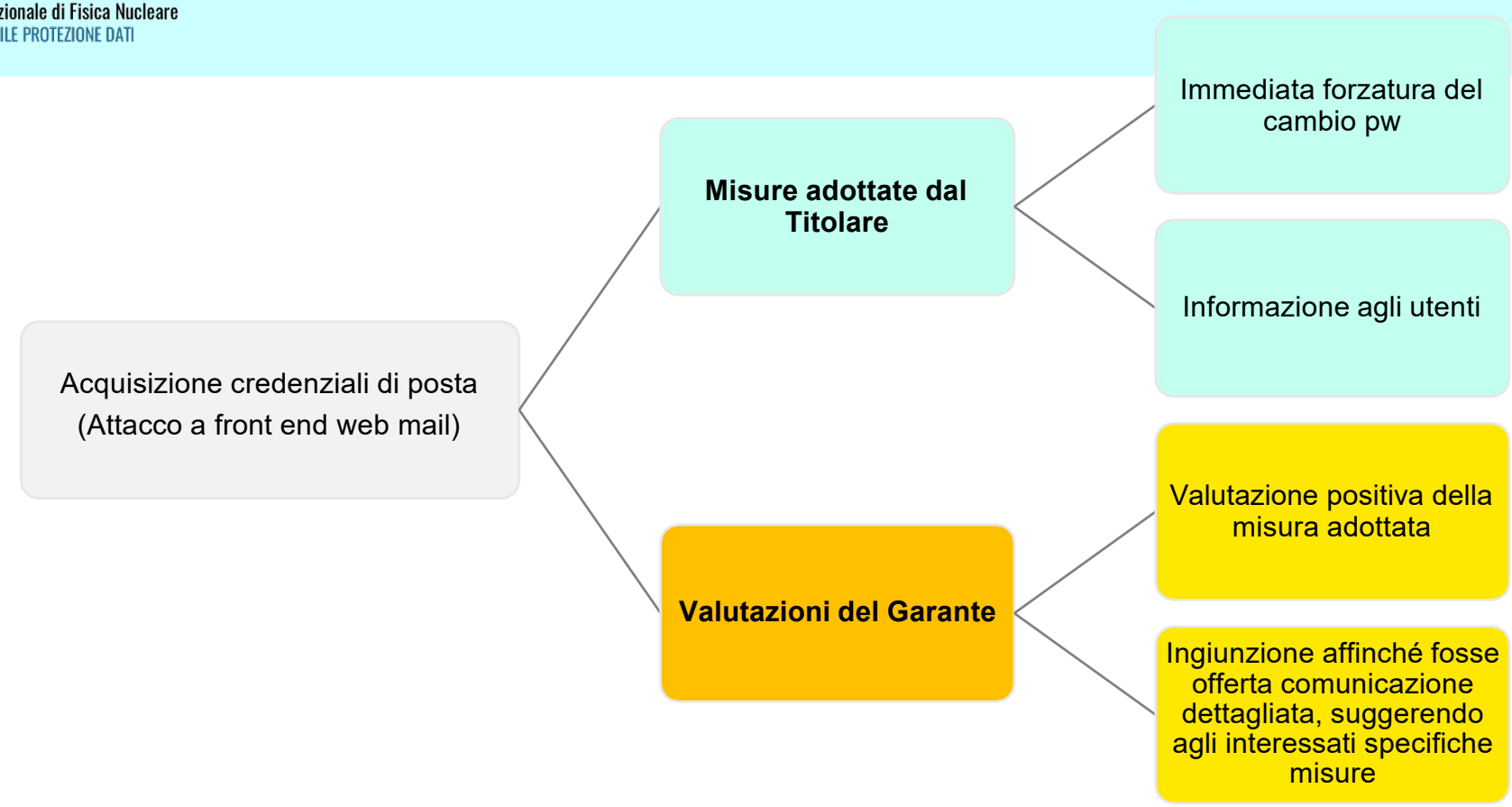
Visualizzazione indebita di dati (Interferenza tra Piattaforma e Applicativo)

- **Misure adottate dal Titolare**
  - Comunicazione della violazione agli utenti
  - Sospensione dell'applicativo e oscuramento della pagina
  - Analisi dei risultati indicizzati da Google e richiesta rimozione dei contenuti
- **Valutazioni del Garante**
  - Il Titolare è tenuto ad adottare procedure per *"testare, verificare e valutare regolarmente l'efficacia delle misure per garantire la sicurezza".*
  - Sanzione: 30.000,00 €

Autore E.Bovo

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Conseguenze delle violazioni



Autore E.Bovo

Privacy… & Security (a)

i due ambiti della privacy per il sistemista

1. **Manipolare i dati personali (log, file con username, database di utenti e asset ecc)**
2. **La security…**

Il titolare del trattamento e quindi l' INFN è chiamato dal GDPR (art.24) a mettere in atto misure tecniche ed organizzative adeguate a garantire, e se richiesto a dimostrare, che i dati personali vengono protetti a norma di regolamento.

Privacy… & Security (b)

Al sistemista, di fatto è richiesto di fare in modo che i dati personali che ci vengono affidati, siano ben protetti, siano essi i log, o la posta elettronica o i file per uso amministrativo. E' qui che si realizza il binomio indissolubile sicurezza-privacy. Per cui il primo problema che il sistemista si deve porre è quello di studiare e attuare misure di sicurezza opportune.

E successivamente valutare se quelle misure sono sufficienti a garantire anche la protezione dei dati personali, nel caso in cui siano presenti sui sistemi di cui si occupa.

E protezione non significa solo misure di difesa, ma anche e soprattutto azioni proattive che riducano i rischi all'origine, secondo i principi di privacy by default e by design indicati nel GDPR.

In caso di dubbi...

DPO@infn.it