UNIVERSITÀ DEGLI STUDI
DI GENOVA

CEDIA
Centro Dati, Informatica e
Telematica di Ateneo

Viale Cembrano, 4
16148 Genova GE Italia
segreteria@cedia.unige.it
csita@pec.unige.it
www.csita.unige.it

Università degli Studi di Genova: Misure Minime di Sicurezza - CeDIA

Genova, 29 dicembre 2017

PREMESSE

Considerata l'eterogeneità degli ambiti operativi in cui è necessario contestualizzare le misure minime di sicurezza (diversa sensibilità, competenza, preparazione degli utenti, tipologia, criticità, sensibilità di servizi erogati e dati trattati), si è ritenuto opportuno suddividere in macro-ambiti differenti lo scenario globale. Per poter attivare le misure minime in modo più puntuale ed adeguato alle esigenze del contesto di riferimento, si sono individuati tre macro-ambiti:

CORE**:** l'insieme delle risorse fisiche e virtuali su cui insistono servizi e dati, personali e sensibili, gestiti da CeDIA per conto dell'ateneo. Dunque rappresenta la parte centrale di massima criticità, per la quale le misure di sicurezza necessarie a impedirne proprio la compromissione.

I sistemi coinvolti sono per la quasi totalità ospitati all'interno dell'infrastruttura virtualizzata di CeDIA. Sono implementati in un sottoinsieme di macchine virtuali, messe in comunicazione per mezzo di reti virtuali logiche (VLAN). Tali sottoreti sono opportunamente e profondamente segmentate e filtrate (microsegmentazione) per mezzo di un firewall su cui sono implementate strettamente le politiche di comunicazione consentite tra l'utenza e i servizi erogati, nonché tra i servizi stessi. Tale infrastruttura è amministrata da un ristretto numero di amministratori tramite criteri di buona pratica (good practices) condivisi e convergenti alle misure minime di sicurezza. La comunicazione via rete verso i sistemi interni all'infrastruttura core è consentita esclusivamente verso i servizi pubblici (ad esempio siti web), per i quali si adottano strategie di protezione più stringenti, o verso le applicazioni erogate all'interno dell'ateneo ad un numero ristretto di reti (reti di CeDIA e amministrazione), in cui le macchine sono sottoposte allo standard di policy delle misure minime di sicurezza.

AMMINISTRAZIONE**:** l'insieme della rete e delle postazioni di lavoro (PDL) assegnate all'amministrazione centrale e che costituisce l'utenza principale dei servizi amministrativi dell'ateneo, avendone titolarità.

CEDIA**:** tutto ciò che riguarda le postazioni di lavoro del personale di CeDIA (Centro Dati, Informatica e telematica di Ateneo) o che comunque accede per finalità di manutenzione, gestione, sviluppo applicativo dei servizi erogati; tali postazioni in quanto "privilegiate" per l'accesso ai sistemi core sono state considerate come ambito operativo a parte.

Occorre infine evidenziare che l'Ateneo a oggi non si è dotato organizzativamente di un'unità di Security Management Officer (SMO), per promuovere azioni preventive attraverso l'emanazione di linee guida e policy, di formazione, di esercitazione, utili alla diffusione di una gestione consapevole della sicurezza dei sistemi ICT di Ateneo. In assenza di tale unità organizzativa CeDIA promuove e pone in essere azioni di vigilanza per i sistemi dallo stesso gestiti e sopradescritti.

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

ABSC_ID			Livello	Descrizione	MODALITA' DI IMPLEMENTAZIONE		
					CORE	AMMINISTRAZIONE	CeDIA
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Ogni sistema che viene attivato deve necessariamente essere configurato da console amministrativa attribuendo le interfacce ad una VLAN specifica. Senza l'installazione di regole specifiche sul FW che lo consentano non è comunque possibile alcuna comunicazione con gli altri sistemi dentro e fuori infrastruttura core.	Per effettuare la verifica delle macchine attive è già consolidato utilizzo di ARPWatch che registra la corrispondenza IP:MAC:nomeDNS delle macchine attive in rete. Come ulteriore inventario delle macchine attive in rete si ipotizza un più ampio utilizzo del sw OCS (Open Computer and Software Inventory) che registra in modalità "asincrona" i sistemi attivi in rete. Anche per le stampanti attive sulla rete, esiste un database delle anagrafiche delle stesse.	Per effettuare la verifica delle macchine attive in "real time" si renderà effettivo **entro 15 febbraio 2018** ARPWatch che registra la corrispondenzaIP:MAC:nomeDNS delle macchine attive in rete. Come ulteriore inventario delle macchine attive in rete si ipotizza un più ampio utilizzo del sw OCS (Open Computer and Software Inventory) che registra in modalità "asincrona" i sistemi attivi in rete.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	La registrazione dei nodi avviene al momento della messa in attività dei nodi.	La registrazione dei nodi avviene al momento della messa in attività dei nodi.	La registrazione dei nodi avviene al momento della messa in attività dei nodi.
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla	Attraverso la registrazione su DNS del nome a dominio e la	Attraverso la registrazione su DNS del nome a dominio e la	Attraverso la registrazione su DNS del nome a dominio e la corrispondente registrazione della risoluzione inversa.

				rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	corrispondente registrazione della risoluzione inversa. Si ricorda che CeDIA non usa il protocollo DHCP per l'assegnazione dinamica degli indirizzi.	corrispondente registrazione della risoluzione inversa. Si ricorda che CeDIA non usa il protocollo DHCP per l'assegnazione dinamica degli indirizzi.	Si ricorda che CeDIA non usa il protocollo DHCP per l'assegnazione dinamica degli indirizzi.

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

ABSC_ID			Livello	Descrizione	MODALITA' DI IMPLEMENTAZIONE		
					CORE	AMMINISTRAZIONE	CeDIA
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.	I sistemi core sono macchine fisiche su cui è installato il software di virtualizzazione. Su ogni nodo viene installato l'hypervisor di una versione recente e ritenuta stabile ed affidabile. Nessun altro software estraneo viene installato a questo livello. A questi nodi si accede soltanto da una rete segregata, protetta da un firewall dedicato e tramite vpn con autenticazione a due fattori, certificati personali e utenti individuali con password. Sui server virtualizzati vengono	Gli utenti non hanno diritti di amministratore sulla macchina in uso quindi, se non per esplicite esigenze di servizio, la possibilità di installare sw non presente nel master della macchina non è disponibile. La modalità di installazione ed aggiornamento dei sistemi prevede l'approntamento di una immagine master con S.O. aggiornato e tutte le applicazioni in uso nell'ateneo preinstallate. Sono preconfigurate le impostazioni di sicurezza ritenute adeguate per il contesto e credenziali amministrative	Il personale del Centro tecnico-informatico ha diritti di amministratore e usa: -software soggetto a licenza, autorizzato dal responsabile di struttura che lo acquisisce e lo manutiene attraverso dei contratti; -software per il quale l'installazione "standard" garantisce requisiti di sicurezza adeguati. Il personale tecnico-informatico può aggiungere software, verificandone i requisiti sotto la propria responsabilità. In tutti i casi non si devono violare le policy definite dal GARR (AUP).

					installati S.O. in base alle applicazioni che devono essere ospitate e a partire da template validati che vengono generati nel seguente modo: nel caso di sistemi operativi linux si eseguono installazioni di due distinte distribuzioni: a) per usi generici con software open source Ubuntu di tipo LTS (supporto garantito tre anni) in corso di validità ; b) per software che pone vincoli commerciali al fine di garantire manutenzione e supporto si installa l'ultima versione di RedHat Enterprise Linux. In entrambi i casi vengono applicati gli aggiornamenti di sicurezza solo in caso si sia valutato che correggano vulnerabilità con un possibile impatto per le modalità di utilizzo specifiche del server. Nel caso di sistemi Windows, vengono mantenuti aggiornati i template delle versioni supportate dal produttore e,	personali per il personale dedicato alla manutenzione. Dunque i software contenuti nell'immagine "certificata" dal centro di competenza di CeDIA sono già di fatto autorizzati. Rappresentano deroghe quei dispositivi portatili di proprietà dell'ente, ma affidati anche nella gestione ordinaria e straordinari a dipendenti che li utilizzano prevalentemente fuori dalla rete di Ateneo. Per questo l'affidatario del bene è anche amministratore del dispositivo. Occorre una informativa almeno annuale sulle procedure organizzative, tecniche e di gestione per la protezione dei sistemi di cui ognuno è responsabile quando ha i diritti di amministratore.	Inoltre attraverso una procedura organizzativa interna al Centro, si verificheranno a campione i software installati sulle postazioni di lavoro. Infine per diminuire comunque il rischio, quale evoluzione dei datacenter di CeDIA, **nel primo semestre 2018** è intendimento avviare e concludere un'analisi di fattibilità della separazione degli ambienti di test, e delle procedure di deployment delle applicazioni sia quelle sviluppate in house sia quelle acquisite da terze parti. Occorre una informativa almeno annuale sulle procedure organizzative, tecniche e di gestione per la protezione dei sistemi di cui ognuno è responsabile quando ha i diritti di amministratore.

					all'atto dell'instanziazione, si predilige l'utilizzo del sistema piu' recente supportato dal software che si andra' ad installare. Per quanto riguarda i sistemi windows, questi vengono aggiornati in base alle notifiche da parte del produttore o in basea vulnerabilita' rese note e che richiedano l'applicazione di aggiornamenti urgenti al fine di ridurre al minimo eventuale impatto di vulnerabilita' presenti in funzione dell'utilizzo a cui sara' soggetto il sistema. Sui sistemi vengono installati i software aggiuntivi richiesti, indicati dal fornitore, per consentire il funzionamento dei prodotti per i quali vengono predisposti i sistemi.		

2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Il Centro si dota di un software che permette di verificare le vulnerabilità, Nessus. Da un punto di vista procedurale l'infrastruttura dei datacenter è protetta verso l'esterno e accessibile soltanto a 4 persone, che tracciano quanto viene fatto in termini di utilizzo di nuovo software.	Tramite OCS è possibile verificare l'elenco dei sw installati su una PDL e quindi verificare la presenza di sw non autorizzato, ad eccezione delle versioni *portable*. Il task periodico che possa individuare anomalie nel SW installato verrà messo in produzione **entro il 31 dicembre 2018,** se i prodotti di mercato sono compatibili con le tecnologie oggi in uso dal centro.	Anche sulle postazioni in uso a CeDIA è installato OCS ed è quindi possibile verificare lo stato di installazione dei sw. Il task periodico che possa individuare anomalie nel SW installato verrà messo in produzione entro il 31 dicembre 2018, se i prodotti di mercato sono compatibili con le tecnologie oggi in uso dal centro.

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione		
					CORE	AMMINISTRAZIONE	CeDIA
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	La configurazione iniziale dei S.O. avviene da template e quindi corrisponde a criteri standard di implementazione. Le ulteriori misure impiegate sono approntate sulla base di considerazioni specifiche in base al software	La standardizzazione delle configurazioni è garantita dal corretto impiego dei master approntati per l'installazione e conservati nell'infrastruttura di gestione off line.	Occorre una informativa almeno annuale sulle procedure organizzative, tecniche e di gestione per la protezione dei sistemi di cui ognuno è responsabile quando ha i diritti di amministratore.

					applicativo installato e da considerazioni di contesto operativo in cui il sistema è messo ad operare.		
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	I template delle macchine virtuali sono differenziati per tipologia di S.O. e implementano le configurazioni standard specifiche adottate.	La configurazione del master per le PDL dell'amministrazione centrale costituisce ad oggi la configurazione standard. Non sono stati realizzati master differenziati in base alla profilazione delle tipologie di software necessarie in base al ruolo dell'utente.	Occorre una informativa almeno annuale sulle procedure organizzative, tecniche e di gestione per la protezione dei sistemi di cui ognuno è responsabile quando ha i diritti di amministratore, differenziandola per tipologia di dispositivo.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	In caso di corruzione di una macchina virtuale si valuta l'integrità delle immagini salvate della stessa. In caso si rilevassero segni di corruzione anche in tutte le immagini di salvataggio si procede alla riconfigurazione a partire da un template valido.	È pratica consolidata il ripristino dei sistemi compromessi reinstallando il master.	Si procede ad una verifica periodica delle policy adottate dal personale tecnico-informatico per le proprie postazioni di lavoro.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	I template sono custoditi in un volume non accessibile direttamente dalla rete. Le operazioni su di essi vengono	Esiste una infrastruttura di gestione off line per il "repository" dei master da impiegare per	Si procede ad una verifica periodica delle policy adottate dal personale tecnico-informatico per le proprie postazioni di lavoro.

					effettuate dalla rete segregata precedentemente descritta e non accessibile da persone che non si autentichino con doppio fattore.	l'installazione delle pdl, crittografati.	
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).	La rete di gestione dell'infrastruttura è segregata (doppia interfaccia di rete fisica separata dalla rete dati di accesso), protetta da un firewall dedicato e tramite vpn con doppia autenticazione, certificati personali e utenti individuali con password. L'accesso amministrativo ai sistemi avviene esclusivamente attraverso protocolli sicuri e solo da reti specifiche assegnate a CeDIA o tramite VPN crittografata.	Si stanno adottando due strumenti che utilizzano canali sicuri: -il remote desktop del S.O., integrato nello stesso; -mesh central che aggiunge altre informazioni quali elenco delle postazioni attive.	Si procede ad una verifica periodica delle policy adottate dal personale tecnico-informatico per le proprie postazioni di lavoro.

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione		
					CORE	AMMINISTRAZIONE	CeDIA
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire	L'infrastruttura virtualizzata contiene un tale numero di macchine e servizi da essere in evoluzione pressoché	Si usa OPEN VAS per effettuare scansioni a intervalli regolari	Si usa OPEN VAS per effettuare scansioni a intervalli regolari

				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.	continua. L'uso di un vulnerability scanner con frequenza molto ravvicinata potrebbe costituire una criticità per le performance dei sistemi coinvolti. Si sta valutando l'opportunità di effettuare scansioni programmate a intervalli di tempo più ampi ancora da quantificare, **per esempio 6 mesi.**		
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Si adotterà un sw che garantisca l'aggiornamento dello stesso, a fronte delle vulnerabilità più rilevanti. A tal fine si farà un check periodico della presenza di aggiornamenti per il sw di scansione delle vulnerabilità.	Si adotterà un sw che garantisca l'aggiornamento dello stesso, a fronte delle vulnerabilità più rilevanti. A tal fine si farà un check periodico della presenza di aggiornamenti per il sw di scansione delle vulnerabilità.	Si adotterà un sw che garantisca l'aggiornamento dello stesso, a fronte delle vulnerabilità più rilevanti. A tal fine si farà un check periodico della presenza di aggiornamenti per il sw di scansione delle vulnerabilità
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Non si ritiene sufficientemente affidabile e sicura l'attivazione di un sistema di aggiornamento dei sistemi in modalità non presidiata. I rilasci devono essere testati in opportuni ambienti di prova e le eccezioni documentate.	Non si ritiene sufficientemente affidabile e sicura l'attivazione di un sistema di aggiornamento dei sistemi in modalità non presidiata, nel caso di applicazioni che non siano della suite Windows. Nel caso della suite Windows, si usano i sistemi automatici di	Non si ritiene sufficientemente affidabile e sicura l'attivazione di un sistema di aggiornamento dei sistemi in modalità non presidiata, nel caso di applicazioni che non siano della suite Windows. Nel caso della suite Windows, si usano i sistemi automatici di aggiornamento e patching dei

						aggiornamento e patching dei sistemi forniti dalla casa produttrice del S.O. e delle applicazioni in uso sulle PDL. Esistono altri sw: Firefox, Thunderbird, Adobe vengono aggiornati in automatico per far incrementare i livelli di sicurezza. Sono stati disabilitati al momento della configurazione altri sw: Java, applicazioni dell'INPS.	sistemi forniti dalla casa produttrice del S.O. e delle applicazioni in uso sulle PDL. Esistono altri sw: Firefox, Thunderbird, Adobe vengono aggiornati in automatico per far incrementare i livelli di sicurezza.
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.	Non ne esistono.	Non esistono dispositivi separati dalla rete e gestiti dal Centro.	Non esistono dispositivi separati dalla rete e gestiti dal Centro.
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o	Si ritiene di poter accettare un rischio ragionevole, in quanto il core è presidiato da un team che ha le competenze per adottare	Scansioni periodiche tramite OPEN VAS.	Scansioni periodiche tramite OPEN VAS.

				implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	contromisure, documentandone l'intervento.		
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.).	Tale analisi viene effettuata dagli amministratori della infrastruttura virtuale sia in fase di implementazione architetturale dei servizi che nella gestione ordinaria degli stessi. Non è definito un processo formale di definizione di un piano, per il quale è opportuno che la stesura sia fatta con Security Management Officer. Il piano deve tener conto anche dei servizi erogati direttamente o indirettamente tramite fornitori. Questo deve essere regolamentato anche nella nuova contrattualistica, adattandola e differenziandola nel caso di servizi in hosting o in cloud.	Occorre definire un piano dei rischi con un Security Management Officer, estendibile a tutto l'Ateneo. Il piano deve tener conto anche dei servizi erogati direttamente o indirettamente tramite fornitori. Questo deve essere regolamentato anche nella nuova contrattualistica, adattandola e differenziandola nel caso di servizi in hosting o in cloud.	Occorre definire un piano dei rischi con un Security Management Officer, estendibile a tutto l'Ateneo. Il piano deve tener conto anche dei servizi erogati direttamente o indirettamente tramite fornitori. Questo deve essere regolamentato anche nella nuova contrattualistica, adattandola e differenziandola nel caso di servizi in hosting o in cloud.
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare	Rientra nella procedura interna adottata, in maniera selettiva.	Rientra nella procedura interna adottata, in maniera selettiva.	Rientra nella procedura interna adottata, in maniera selettiva.

				applicare le patch per le vulnerabilità a partire da quelle più critiche.			

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione		
					CORE	AMMINISTRAZIONE	CeDIA
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.	Accesso agli host limitato ai soli utenti autorizzati e competenti. Privilegi amministrativi associati esclusivamente agli operatori autorizzati, non presenti altre utenze con privilegi diversi da quelli amministrativi.	Privilegi di amministrazione associati ai soli utenti autorizzati alle operazioni di manutenzione e configurazione dei sistemi. Si mantiene l'elenco degli ADS aggiornato, con un controllo semestrale da parte del centro di competenza.	Annualmente la Direzione Generale richiede l'elenco degli Amministratori di Sistema ad ogni responsabile di struttura, che sotto la propria responsabilità attesta le competenze per poter operare sui sistemi di cui viene dotato il personale del Centro. Si mantiene l'elenco degli ADS aggiornato, con un controllo semestrale da parte del responsabile dell'unità organizzativa, indicata nell'informativa al personale tecnico del Centro.
5	1	2	M	Utilizzare le utenze amministrative solo per	Verrà gradualmente implementato l'utilizzo del comando di sistema	E' già attivo nel sistema operativo Windows, quindi se	E' già attivo nel sistema operativo Windows, quindi se l'utente accede

				effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	"sudo" sui sistemi linux , eliminando l'utilizzo del comando "*su*". L'account di root verrà disabilitato da rete e potrà essere usato esclusivamente da console e in casi di emergenza. Si sta valutando l'impiego di un Siem per poter collettare le registrazioni degli eventi amministrativi. La valutazione deve tener conto della disponibilità economica,	l'utente accede si registrano data di accesso, data di disconnessione e nome utente. La registrazione dei log avviene localmente. Estensione dell'utilizzo di un Siem per monitorare eventi relativi alle pdl	si registrano data di accesso, data di disconnessione e nome utente. La registrazione dei log avviene localmente. Estensione dell'utilizzo di un Siem per monitorare eventi relativi alle pdl in dotazione al personale CeDIA.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Ad oggi le utenze amministrative sull'infrastruttura virtualizzata sono limitate. Deve essere formalizzato un processo di individuazione degli effettivi utenti amministrativi di tutte le macchine virtuali e della revoca degli stessi	Le utenze amministrative locali alle pdl sono nominative e personali e sono già preconfigurate nei master di installazione. Le credenziali amministrative di dominio sono limitate.	Le utenze amministrative locali alle pdl possono essere nominative e personali . Poiché l'affidatario della postazione di lavoro è anche amministratore, in questo ruolo può configurare utenze amministrative anche diverse per permettere test dei servizi rilasciati dal centro ad altri. Si sta cercando un prodotto che automatizzi la gestione dell'inventario di tutte le utenze amministrative. Entro il mese di marzo 2018 si formalizzerà il processo autorizzativo interno al centro.

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.	L'approntamento dei sistemi a partire da template preconfezionati risponde a questa esigenza	Questo viene garantito dalla procedura di installazione a partire dal master.	Si formalizzerà entro marzo 2018 il processo autorizzativo e delle prese in carico delle sottoprocedure previste nelle Misure Minime di Sicurezza, a valle di un'informativa che verrà fatta tra il 15 gennaio e il 15 febbraio 2018.
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).	Non è attualmente operante un enforcement di policy sulle credenziali, ne è tuttavia allo studio l'attivazione.	I futuri master prevederanno l'applicazione di policy congruenti sulle credenziali.	La stessa policy dovrà essere adottata presso il personale CeDIA, a valle dell'informativa sopracitata.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Non è attualmente operante un enforcement di policy sulle credenziali, ne è tuttavia allo studio l'attivazione.	I futuri master prevederanno l'applicazione di policy congruenti sulle credenziali.	La stessa policy dovrà essere adottata presso il personale CeDIA, a valle dell'informativa sopracitata.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a	Non è attualmente operante un enforcement di policy sulle credenziali, ne è tuttavia allo studio l'attivazione.	I futuri master prevederanno l'applicazione di policy congruenti sulle credenziali.	La stessa policy dovrà essere adottata presso il personale CeDIA, a valle dell'informativa sopracitata.

				breve distanza di tempo (password history).			
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Sui sistemi linux ciò è garantito dalla corretta configurazione di “sudo”, che consente di non usare credenziali amministrative, ma di elevare i propri privilegi solo per compiti specifici e delegati ai singoli utenti. I sistemi verranno progressivamente riconfigurati in tal senso.	Le utenze nei master sono già preconfigurate in tal senso.	La stessa policy dovrà essere adottata presso il personale CeDIA, a valle dell’informativa sopracitata.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Con la configurazione sopra descritta di sudo si ottiene tale risultato.	Le utenze nei master sono già preconfigurate in tal senso.	E’ già possibile, questo requisito sarà indicato quale obbligatorio nell’informativa sopracitata.
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	Tali utenze amministrative all’interno dell’infrastruttura virtualizzata sono relegate all’uso da console a cui si ha accesso tramite “vpn” con autenticazione a doppio fattore e quindi facilmente imputabile. Ad oggi le unità di personale del centro che possono accedere alle console sono 4.	Le utenze nei master sono già preconfigurate in tal senso, dove il ruolo “administrator” è disabilitato.	La stessa policy dell’Amministrazione dovrà essere adottata presso il personale CeDIA, a valle dell’informativa sopracitata.

				credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.			
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	L'utente amministrativo deve conservarle in maniera riservata, ricordandoglielo attraverso una informativa adeguata. In questo caso, tenuto conto della delicatezza, verranno tenute in copia nella cassaforte del centro.	L'utente amministrativo deve conservarle in maniera riservata, ricordandoglielo attraverso una informativa adeguata.	L'utente amministrativo deve conservarle in maniera riservata, ricordandoglielo attraverso una informativa adeguata.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Sono adeguatamente protette mediante utilizzo di "passphrase".	Sono adeguatamente protette mediante utilizzo di pin personali o "passphrase".	Sono adeguatamente protette mediante utilizzo di pin personali o "passphrase".

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione		
					CORE	AMMINISTRAZIONE	CeDIA
8	1	1	M	Installare su tutti i sistemi connessi alla	I server in infrastruttura virtuale non sono connessi alla rete locale ma a	Nel master è già preconfigurato l'antivirus e attivati gli	E' già preconfigurato l'antivirus e attivati gli aggiornamenti automatici

				rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	VLAN specifiche, microsegmentate, filtrate da un FW che non consente accessi fra le macchine che non siano congruenti con i flussi applicativi leciti. Si ritiene residuale il rischio di esecuzione di malware, mentre si valuta negativamente l'impatto sulle performance dell'attivazione di un software antivirus.	aggiornamenti automatici delle firme.	delle firme. Rientra, comunque, nelle disponibilità dell'amministratore del dispositivo di poterla eventualmente disabilitare
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Con riferimento alla topologia di rete implementata e all'adozione di regole di filtraggio finemente specificate sul firewall si ritiene poco rilevante l'utilizzo di tali soluzioni per le macchine in infrastruttura virtuale.	Sulle PDL amministrative attivo Windows FW per default.	Sulle PDL amministrative attivo Windows FW per default. Rientra, comunque, nelle disponibilità dell'amministratore del dispositivo di poterla eventualmente disabilitare,
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Non è previsto il collegamento di dispositivi esterni.	Non esiste policy di sicurezza specifica sull'utilizzo di dispositivi esterni e/o personali sulle postazioni dell'amministrazione centrale. Si sta valutando la possibilità di adottare un software di protezione degli endpoint.	Non esiste policy di sicurezza specifica sull'utilizzo di dispositivi esterni e/o personali sulle postazioni dell'amministrazione centrale. Si sta valutando la possibilità di adottare un software di protezione degli endpoint.
8	7	1	M	Disattivare l'esecuzione automatica dei	Non è previsto il collegamento di dispositivi rimuovibili.	Tale policy è implementata nel master di installazione.	Rientra nelle disponibilità dell'amministratore del dispositivo di

				contenuti al momento della connessione dei dispositivi removibili.			poterla eventualmente disabilitare, seppur disabilitato l'"autorun" per default.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Là dove previsto l'elaborazione di file con contenuti dinamici, l'esecuzione degli stessi è disattivata.	Tale policy è implementata nel master di installazione.	Rientra nelle disponibilità dell'amministratore del dispositivo di poterla eventualmente disabilitare, seppur presente nel pacchetto Office come disabilitata.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Non è previsto l'utilizzo di un client di posta.	Tale policy è implementata nel master di installazione.	Rientra nelle disponibilità dell'amministratore del dispositivo di poterla eventualmente disabilitare.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	L'anteprima automatica è disabilitata sui sistemi che la prevedono.	Tale policy è implementata nel master di installazione.	Rientra nelle disponibilità dell'amministratore del dispositivo di poterla eventualmente disabilitare.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Non è previsto il collegamento di dispositivi rimuovibili.	E' già attivata sul master.	Rientra nelle disponibilità dell'amministratore del dispositivo di poterla eventualmente disabilitare.
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario,	Attivato a livello di servizio di posta elettronica servizio antispam e antivirus tramite utilizzo delle SVEA (Sophos virtual Email Appliance)		

				prevedendo anche l'impiego di strumenti antispam.	
8	9	2	M	Filtrare il contenuto del traffico web.	Le possibilità di filtrare il traffico web sono limitate, non è possibile filtrare in base al contenuto delle comunicazioni.
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).	Il blocco nella posta elettronica può essere a carico di SVEA. Il blocco nel traffico web dei file in oggetto non è applicabile all'HTTPS, nel traffico in chiaro nel dominio di Balbi esistono già filtri sul proxy, in generale esiste un problema prestazionale da analizzarne i costi e benefici.

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione		
					CORE	AMMINISTRAZIONE	CeDIA
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il	I servizi ospitati in infrastruttura sono configurati in BC Non è ancora definito un piano eventuale di DR Per proteggere i servizi erogati sono implementate varie	Bkp dei dati degli utenti su file server di dominio e locali viene effettuato tramite Shadow copy, inserito nel master.	Si può estendere la policy applicata all'Amministrazione anche a CeDIA, a seguito dell'informativa agli amministratori di sistema.

				completo ripristino del sistema.	strategie per effettuare bkp schedulati		
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.	Le copie di sicurezza non vengono più memorizzate su unità di backup con supporti asportabili (nastri magnetici o dischi magneto/ottici).Le copie di sicurezza sono contenute nei nostri sistemi in SAN, ridondati sul singolo storage e replicati su due sedi e ulteriormente salvati su tape library virtuali del deduplicatore. L'accesso fisico ai supporti che contengono tali copie non consentono facilmente l'accesso ai dati contenuti. E' in corso di valutazione l'applicabilità di cifratura del filesystem che contiene tali copie o alternativamente la cifratura delle copie stesse.	Non si hanno policy di backup delle postazioni in locale, fatta ad eccezione di 30 utenze di posta elettronica, su una terza macchina in modalità cifrata.	Non si hanno policy di backup delle postazioni in locale, ad eccezione dei contenuti creati e gestiti dall'amministrazione del centro.

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.	I backup effettuati con VDP non sono accessibili dal sistema che viene sottoposto a backup.	-	-

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione		
					CORE	AMMINISTRAZIONE	CeDIA
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente	Il CeDIA intende avviare questa analisi a partire dai dati personali, già in corso di censimento nel progetto “attuazione GDPR” , che verrà completata entro il 27 febbraio 2018. A partire dal mese di giugno 2018 verrà estesa questa analisi eventualmente ad altri dati e completata entro il 30 settembre 2018.		

				quelli ai quali va applicata la protezione crittografica	
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Il FW di frontiera ha la possibilità di implementare il filtraggio verso Url specifici tramite blacklisting

ARPWATCH: cosa può monitorare:

- IPMAC
- IPNever Seen By Arp Watch
- Events
- Filtered Events
- Flip Flop Events
- Changedethernetaddress Events
- Reused Old Ethernet Address
- Ethernet Broadcast Events
- Ethernet Mismatch Events
- New Station Events
- New Activity Events
- Network Scaning
- ARP

- All Possible IP

Ing. Patrizia Cepollina

Dirigente-Direttore Tecnico CeDIA

Università degli Studi di Genova

(firmato digitalmente)

Prof. Paolo Comanducci

Rettore

Università degli Studi di Genova

(firmato digitalmente)