ALLEGATO A) alla deliberazione n. del

A.S.L. V.C.O.
Azienda Sanitaria Locale
del Verbano Cusio Ossola

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

1209 31 DICEMBRE 2018

REGIONE PIEMONTE

AZIENDA SANITARIA LOCALE VCO
OMEGNA

IL DIRETTORE GENERALE
(Nominato con DGR n. 37-1365 del 27/04/2015)

DELIBERAZIONE N. 968 del 29 DICEMBRE 2017

OGGETTO	**PRESA D'ATTO ATTUAZIONE ADEMPIMENTI PREVISTI DALLA CIRCOLARE AGENZIA PER L'ITALIA DIGITALE (AgID) N. 2 DEL 18/4/2017 INERENTE LE MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI.**

L'anno duemiladiciassette il giorno VENTINOVE

del mese di DICEMBRE in OMEGNA,

IL DIRETTORE GENERALE

- Dott. Giovanni Caruso

coadiuvato da:

- Dott. Antonino Trimarchi **DIRETTORE SANITARIO**
ASSENTE GIUSTIFICATO

- Dott. Antonio Jannelli **DIRETTORE AMMINISTRATIVO**

REGIONE PIEMONTE

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634680033

L'estensore dell'atto
Collaboratore Amministrativo
Sig.ra Emanuela Motetta
Omegna, lì 22/12/2017

Il responsabile del procedimento
Dr.ssa
Omegna, lì 28/12/2017

Riservato alla S.O.C. Gestione Economico-Finanziaria e Patrimonio per la registrazione della spesa:

data _____

al N. _____ conto _____

al N. _____ conto _____

al N. _____ conto _____

al N. _____ conto _____

Si attesta la regolarità contabile e le imputazioni
a Bilancio derivanti dal provvedimento
Il Direttore SOC GEP
(Dott.ssa Manuela Succi)

_____

Beneficiario _____ €. _____

Beneficiario _____ €. _____

Beneficiario _____ €. _____

Annotazioni eventuali :
EM/EM
Nome file: DELIBERA misure minime di sicurezza ICT 311217

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

IL DIRETTORE GENERALE
Dr. Giovanni Caruso
(Nominato con DGR n. 37-1365 del 27/04/2015)

Nella data sopraindicata, su propria iniziativa, in conformità al Regolamento approvato con delibera n. 290 del 12/05/2017

PREMESSO CHE

- L'art. 14-bis del D.lgs. 7/3/2005 n. 82 (C.A.D. Codice dell'Amministrazione Digitale), al comma 2, lett. a), tra le funzioni attribuite all'AgID (Agenzia per l'Italia Digitale), prevede, tra l'altro, l'emanazione di regole, standard e guide tecniche, nonché di vigilanza e controllo sul rispetto delle norme di cui al medesimo C.A.D., anche attraverso l'adozione di atti amministrativi generali, in materia di sicurezza informatica;

- La Direttiva del 1° agosto 2015 del Presidente del Consiglio dei Ministri impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici e, al fine di agevolare tale processo, individua nell'AgID l'organismo che dovrà rendere prontamente disponibili gli indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partners del nostro paese e delle organizzazioni internazionali di cui l'Italia è parte.

DATO ATTO CHE, in applicazione della normativa sopra richamata, AgID ha emanato la circolare n. 2 del 18/4/2017, nella quale, all'allegato 1, sono indicate le misure minime per la sicurezza ICT che debbono essere adottate dalle Pubbliche Amministrazioni entro il 31/12/2017 al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i sistemi informativi.
La circolare in argomento stabilisce inoltre, all'art. 3, che il Responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art. 17 del C.A.D., ovvero, in sua assenza, il Dirigente allo scopo delegato, ha la responsabilità dell'attuazione delle misure minime citate.

EVIDENZIATO CHE l'art. 4 della circolare di cui trattasi fissa le modalità con cui ciascuna misura debba essere adottata, mediante la compilazione del "Modulo di implementazione delle MMS-PA" (allegato 2 alla circolare), da firmare digitalmente con marcatura temporale dal soggetto di cui all'art. 3 sopra citato e dal Responsabile Legale della struttura. Dopo la sottoscrizione tale modulo deve essere conservato e, in caso di incidente informatico, trasmesso al CERT-PA unitamente alla segnalazione dell'incidente stesso.

PRESO ATTO che con nota prot. 75768 in data 20/12/2017 la Responsabile della SOS I.C.T. (Tecnologia dell'Informazione e della Comunicazione) ha comunicato l'adozione delle misure minime in oggetto, con il completamento del modulo di implementazione previsto da AgID, debitamente sottoscritto digitalmente con marcatura temporale, trasmettendo contestualmente il file in formato cartaceo, così come risulta dal documento allegato alla presente deliberazione quale parte integrante e sostanziale sotto la lettera A) .

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

RITENUTO di dover pertanto prendere atto dell'avvenuta attuazione degli adempimenti previsti dalla Circolare AgID n. 2 del 18/4/2017 entro i termini prescritti,

ACQUISITO il parere espresso ai sensi del combinato disposto dell'art. 3 c. 7 e 4 c. 1 del D.Lgs. 502/1992 e s.m.i., dal solo Direttore Amministrativo in quanto il Direttore Sanitario risulta assente giustificato

DELIBERA

1°) Di dare atto che, in adempimento a quanto stabilito dalla Circolare AgID n. 2 del 18/4/2017, relativa alle misure minime di sicurezza ICT da adottare dalle Pubbliche Amministrazioni, la Responsabile della SOS ICT ha provveduto alla compilazione dell'apposito "Modulo di implementazione" previsto dall'art. 4 della circolare citata, ed alla sua sottoscrizione digitale, congiuntamente al Direttore Generale, con l'apposizione di marcatura temporale per la successiva conservazione a norma di legge.

2°) Di allegare alla presente deliberazione quale parte integrante e sostanziale sotto la lettera A), il Modulo di implementazione di cui al punto 1° in formato cartaceo.

3°) Di precisare che dall'assunzione del presente atto non derivano oneri di spesa per l'Azienda.

4°) Di dichiarare la presente deliberazione immediatamente eseguibile ai sensi di legge.

Omegna, li 29 DIC. 2017

IL DIRETTORE GENERALE
Dr. Giovanni Caruso

IL DIRETTORE AMMINISTRATIVO

Dr. Antonio Jannelli

FAVOREVOLE

FIRMA

DATA 29 DIC. 2017

IL DIRETTORE SANITARIO

ASSENTE GIUSTIFICATO

Dr. Antonino Trimarchi

REGIONE PIEMONTE

ALLEGATO A) ALLA DELIBERAZIONE N. 908 DEL 29 DICEMBRE 2017
COMPOSTO DA N.12 FACCIATE

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	Esistono due tipi di Inventario: • Inventario fisico dei cespiti aziendali – Procedura centralizzata Amministrativo Contabile e Patrimoniale (OLIAMM). Assegnazione numero inventario. • Inventario delle risorse collegate alla rete aziendale (Fusion Inventory e Sophos). Assegnazione indirizzo IP.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Le risorse vengono preventivamente autorizzate al collegamento in rete e successivamente rilevate in tempo reale.
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	I dispositivi non autorizzati non possono collegarsi alle risorse di rete aziendali (server, applicativi, risorse condivise, ecc.)
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	Gli accessi alla rete sono discriminati tramite strumenti che separano il traffico istituzionale (utenti autorizzati tramite active directory) da quelli che possono utilizzare semplicemente internet Free.
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	Da attivare
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Non necessario in quanto le risorse vengono preventivamente autorizzate al collegamento in rete e successivamente rilevate in tempo reale.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	La procedura di acquisizione delle apparecchiature prevede un iter di processo che consente l'aggiornamento dell'inventario.
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	La procedura di acquisizione delle apparecchiature prevede un iter di processo che consente l'aggiornamento dell'inventario.
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	La procedura di acquisizione delle apparecchiature prevede un iter di processo che consente l'aggiornamento dell'inventario. Viene sempre registrato l'indirizzo IP e nel caso di pc e server anche il nome della risorsa .
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.	Questi dati sono rilevabili tramite l'incrocio tra le informazioni degli inventari indicati in ABSC_ID 1.1.1

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.	Alla rete dati possono accedere solo dispositivi mobili o fissi autorizzati.
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.	Alla rete dati possono accedere solo dispositivi mobili o fissi autorizzati e quindi presenti in inventario.
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	Lato client: l'autenticazione alla connessione alla rete locale è preventivamente assegnata da ICT (Non vengono utilizzati certificati lato client)

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.	L'elenco dei software è gestito dagli inventari sopra indicati per l'hardware. Le procedure autorizzate sono quelle di utilizzo istituzionale e aziendale. Solo l'amministratore del sistema può installare software, previa verifica di compatibilità con le politiche di sicurezza aziendali. In ogni caso non può essere installato alcun software senza l'autorizzazione del Dirigente responsabile del servizio.
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.	Non esiste una "whitelist". In ambito aziendale è autorizzato l'accesso ai soli software istituzionali e aziendali verificati.
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).	Allo stato attuale non c'è la necessità.
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state	Non esiste una "whitelist".

				modificate.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	La presenza di software non autorizzato è inibita in quanto ne viene bloccata l'installazione.
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.	L'inventario viene mantenuto e aggiornato in tempo reale mediante l'utilizzo dei software che monitorano le apparecchiature collegate alla rete aziendale.
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.	L'inventario viene mantenuto e aggiornato in tempo reale mediante l'utilizzo dei software che monitorano le apparecchiature collegate alla rete aziendale.
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.	Allo stato attuale non c'è la necessità.

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
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	E' in corso la sostituzione delle apparecchiature "non a norma". Le nuove apparecchiature vengono installate utilizzando una configurazione master appositamente configurata.
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.	E' in corso la sostituzione delle apparecchiature "non a norma". Le nuove apparecchiature vengono installate utilizzando una configurazione master appositamente configurata.
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.	E' in corso la sostituzione delle apparecchiature "non a norma". Le nuove apparecchiature vengono installate utilizzando una configurazione master appositamente configurata. Le immagini utilizzate vengono riviste in funzione degli aggiornamenti critici.
3	2	1	M	Definire ed impiegare una configurazione standard per	Modalità operativa in essere nella nostra organizzazione.

				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.	Modalità operativa in essere nella nostra organizzazione.
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	Modalità operativa in essere nella nostra organizzazione.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Modalità operativa in essere nella nostra organizzazione.
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Modalità operativa in essere nella nostra organizzazione.
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).	Modalità operativa in essere nella nostra organizzazione.
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.	Da attivare
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.	Da attivare
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.	Modalità operativa in essere nella nostra organizzazione.
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	Modalità operativa in essere nella nostra organizzazione.
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	Modalità operativa in essere nella nostra organizzazione.
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	Modalità operativa in essere nella nostra organizzazione.

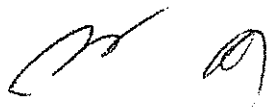
ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

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.	Tutte le modifiche vengono testate prima di essere messe in produzione.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Vengono eseguite ricerche periodiche utilizzando gli strumenti.
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).	Non disponibile
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Non disponibile
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Non disponibile
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	Attivo tramite il sistema di antivirus (Sophos)
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.	Modalità operativa in essere nella nostra organizzazione.
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.	Modalità operativa in essere nella nostra organizzazione.
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Modalità operativa in essere nella nostra organizzazione.
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole	Modalità operativa in essere nella nostra organizzazione.

				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.	Sono state implementate policies aziendali che automaticamente installano gli aggiornamenti dei sistemi operativi in modo compatibile con gli applicativi aziendali.
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 esistono sistemi separati dalla rete.
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.	Modalità operativa in essere nella nostra organizzazione.
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.	Modalità operativa in essere nella nostra organizzazione.
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.	Modalità operativa in essere nella nostra organizzazione.
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.).	Anche se tutte le vulnerabilità vengono costantemente analizzate e, per quanto possibile compatibilmente con la compatibilità con gli applicativi aziendali, risolte, non esiste un piano dei rischi formalizzato.
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.	Modalità operativa in essere nella nostra organizzazione.
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.	Modalità operativa in essere nella nostra 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.	Modalità operativa in essere nella nostra organizzazione.

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.	Modalità operativa in essere nella nostra organizzazione.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Modalità operativa in essere nella nostra organizzazione.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Modalità operativa in essere nella nostra organizzazione (CREDNET)
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Modalità operativa in essere nella nostra organizzazione. (CREDNET)
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Modalità operativa in essere nella nostra organizzazione. (CREDNET)
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Le utenze con privilegi di amministratore di sistema sono assegnate solamente alla Struttura organizzativa ICT e alle professionalità individuate formalmente dai fornitori dei sistemi centrali. (CREDNET)
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.	Modalità operativa in essere nella nostra organizzazione.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Modalità operativa in essere nella nostra organizzazione.
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Le utenze con privilegi di amministratore di sistema sono assegnate solamente alla Struttura organizzativa ICT e alle professionalità individuate formalmente dai fornitori dei sistemi centrali
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Non vengono assegnate utenze amministrative a personale diverso da quello assegnato alla struttura organizzativa ICT. I privilegi di tali utenze sono differenziate in funzione dei compiti da svolgere e sono preventivamente autorizzate a livello di Dirigente.
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Non supportato



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.	Non supportata
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).	E' in fase di attivazione la regola di complessità delle password non solo degli amministratori di sistema ma anche di tutti gli utenti di dominio.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	E' in fase di attivazione la regola di complessità delle password non solo degli amministratori di sistema.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	E' attiva la regola di scadenza delle password di amministratore ogni 90 giorni.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	E' attiva la regola che impedisce l'utilizzo delle ultime quattro password utilizzate.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Questa regola non è attiva in quanto è consentito il cambio della password nel caso in cui si abbia il dubbio che qualcun altro ne sia venuto a conoscenza.
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Vedi ABSC_ID 5.7.3 e ABSC_ID 5.7.4
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.	Gli amministratori aziendali posseggono due credenziali distinte a secondo che operino come amministratore o come utente.
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.	Non implementato
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Gli amministratori aziendali posseggono due credenziali distinte a secondo che operino come amministratore o come utente.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Modalità operativa in essere nella nostra organizzazione.
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	Modalità operativa in essere nella nostra organizzazione.

				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).	Modalità operativa in essere nella nostra organizzazione.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Modalità operativa in essere nella nostra organizzazione.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non implementato

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.	Modalità operativa in essere nella nostra organizzazione (Sophos).
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Modalità operativa in essere nella nostra organizzazione.
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Modalità operativa in essere nella nostra organizzazione.
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.	Modalità operativa in essere nella nostra organizzazione.
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.	Modalità operativa in essere nella nostra organizzazione.
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	Modalità operativa in essere nella nostra organizzazione.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Modalità operativa in essere nella nostra organizzazione.
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Modalità operativa in essere nella nostra organizzazione.
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address	Modalità operativa in essere nella nostra organizzazione.

				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.	Modalità operativa in essere nella nostra organizzazione.
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.	Modalità operativa in essere nella nostra organizzazione.
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	Modalità operativa in essere nella nostra organizzazione.
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Modalità operativa in essere nella nostra organizzazione.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Modalità operativa in essere nella nostra organizzazione.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Modalità operativa in essere nella nostra organizzazione.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	E' possibile attivare questa modalità
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	E' possibile attivare questa modalità
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Modalità operativa in essere nella nostra organizzazione.
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.	Modalità operativa in essere nella nostra organizzazione.
8	9	2	M	Filtrare il contenuto del traffico web.	Modalità operativa in essere nella nostra organizzazione.
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).	Modalità operativa in essere nella nostra organizzazione.
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Modalità operativa in essere nella nostra organizzazione.
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.	Modalità operativa in essere nella nostra organizzazione.

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.	Modalità operativa in essere nella nostra organizzazione.
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.	Modalità operativa in essere nella nostra organizzazione.
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Modalità operativa in essere in parte nella nostra organizzazione.
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Modalità operativa in essere nella nostra organizzazione.
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.	Abilitata in modo parziale
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.	Modalità operativa in essere nella nostra organizzazione.

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	In fase di analisi, al momento non abilitata
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	In fase di analisi, al momento non abilitata
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul	In fase di analisi, al momento non abilitata

				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.	
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.	In fase di analisi, al momento non abilitata
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.	In fase di analisi, al momento non abilitata
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.	In fase di analisi, al momento non abilitata
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.	In fase di analisi, al momento non abilitata
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	In fase di analisi, al momento non abilitata
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	No Modalità operativa in essere nella nostra organizzazione.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Modalità operativa in essere nella nostra organizzazione.
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.	Modalità operativa in essere nella nostra organizzazione.

Firmato digitalmente da:

Dott. Giovanni Caruso

Direttore Generale ASL VCO

Dott.ssa Anna Gagliardi

ICT ASL VCO

A.S.L. V.C.O.
Azienda Sanitaria Locale
del Verbano Cusio Ossola

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

RELAZIONE DI PUBBLICAZIONE

Si attesta che copia del presente atto è stata posta in pubblicazione all'Albo Ufficiale dell'A.S.L. VCO il giorno 29 DIC. 2017 per 15 giorni continuativi.

IL FUNZIONARIO INCARICATO

IMMEDIATAMENTE ESECUTIVA

~~ESECUTIVITA'~~ IN DATA 29 DIC. 2017

IL FUNZIONARIO INCARICATO
IL RESPONSABILE SOS
Organi Organismi Collegiali
Protocollo URP Ufficio Stampa
(Dott.ssa Giuseppina Primatesta)

Trasmissione a:

- Collegio Sindacale	Nota prot. n. _____	del _____
- Conferenza dei Sindaci	Nota prot. n. _____	del _____
- Giunta Regionale	Nota prot. n. _____	del _____

Copia per strutture:

	DIREZIONE SANITARIA PRESIDI VB-D		DIPSA
	DIP. PREVENZIONE	X	AFFARI GENERALI LEGALI E IST.
	DISTRETTO VCO		LOGISTICA E SERV. TECNICI E INFORM.
	GEST. ATTIVITA' TERRITORIALE		GEST. ECON. FIN. E PATRIMONIO
	FARMACIA		GEST. PERSONALE E FORMAZIONE
	SALUTE MENTALE TERRITORIALE		
	SER.D		