

DATI GENERALI

| DESCRIZIONE | DATO |
|---------------------------------|----------------------------|
| DATA | 22/12/2017 |
| Denominazione | COMUNE DI POMARETTO |
| Indirizzo | Piazza della Libertà, 1 |
| CAP | 10063 |
| località | POMARETTO |
| Prov. | TO |
| P.I. | 01504050012 |
| C.F. | 85003270015 |
| Tel. | 0121.81241 |
| Fax | 0121.803719 |
| Contatto | Gaydou Ornella |
| E-Mail | pomaretto@ruparpiemonte.it |
| Legale Rappresentante (sindaco) | Breusa Danilo Stefano |
| Resp. Trattamento (sindaco) | Breusa Danilo Stefano |
| | |
| Luogo di custodia dati | MUNICIPIO DI POMARETTO |

INVENTARIO RISORSE ATTIVE

| IP | Tipo | hostname | BRAND | Ubicazione | Operatore | S.O. | D/WG |
|---------------|-------------|---------------|-------|-------------------------------|---------------------|---------------------|------|
| 10.169.58.10 | WORKSTATION | PC-ORNELLA | ACER | UFFICIO SEGRETERIA | Ornella Gaydou | Windows 7 | D |
| 10.169.58.17 | WORKSTATION | PC-LAURA-NEW | DELL | UFFICIO RAGIONERIA | Laura Pasero | Windows 7 | D |
| 10.169.58.19 | NOTEBOOK | NB-ASSESSORI | ACER | SALA RIUNIONE ASSESSORI | Assessori del Comun | Windows 7 | D |
| 10.169.58.20 | WORKSTATION | TECNICO | ASUS | UFFICIO TECNICO | Luigi Casetta | Windows 10 | D |
| 10.169.58.24 | WORKSTATION | PC-SINDACO | ASUS | UFFICIO DEL SINDACO | Danilo Breusa | Windows 10 | D |
| 10.169.58.34 | WORKSTATION | VIDEOSERVER | ACER | UFFICIO DI POLIZIA MUNICIPALE | Ferruccio Pons | Windows 10 | D |
| 10.169.58.18 | WORKSTATION | PC-FERRUCCIO | ACER | UFFICIO DI POLIZIA MUNICIPALE | Ferruccio Pons | Windows 7 | D |
| 10.169.58.180 | WORKSTATION | PC-ANAGRAFE | DELL | UFFICIO ANAGRAFE | Baron Daniele | Windows 7 | D |
| 10.169.58.182 | WORKSTATION | PC-PROTOCOLLO | ACER | UFFICIO ANAGRAFE | Baron Daniele | Windows 10 | D |
| 10.169.58.226 | SERVER | SERVER | ACER | CED | Alpimedia | Windows 2003 server | D |
| 10.169.58.218 | WORKSTATION | FOTOVOLTAICO | ACER | CED | Alpimedia | Windows xp | D |
| 192.168.1.200 | WORKSTATION | PC-INGRESSO | ACER | INGRESSO | Ornella Gaydou | Windows 7 | D |

SOFTWARE

| Software | Brand | Versione |
|--|--------------------------------------|---|
| Office Microsoft | Microsoft | Tutte le versione |
| software di lettura documenti in PDF | Adobe, etc | Tutte le versione |
| AV | Web Root | Ultima versione sempre aggiornata |
| Programmi obbligatori per espletare le mansioni specifiche di ogni singolo ufficio | Ministero, Banca, Agenzia entrate, A | Tutte le ultime versioni disponibili sui rispettivi s |
| Geo tech SUE | SISCOM | Tutte le ultime versioni |
| Gestionale | SISCOM | Ultima versione rilasciata dal produttore |
| java e motori di programmazione | | Versioni richieste dai produttori dei sistemi in us |
| Software di accesso remoto con protezione cifrata (Teamviewer) | | Versione richiesta dai servizi di assistenza |

| apparati | chi autorizzo |
|----------|---|
| w | tutti gli operatori |
| w | tutti gli operatori |
| w+s | tutti gli operatori |
| w+s | tutti gli operatori |
| w | Ufficio tecnico |
| w+s | tutti gli operatori |
| w+s | tutti gli operatori |
| w+s | tutti gli operatori e aziende di assistenza informatica h&s |

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 | In allegato |
| 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. | Aggiornato al 2 dicembre 2017 |
| 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 dispositivi di rete stessi, registrando almeno l'indirizzo IP. | Aggiornato al 2 dicembre 2017 |
| 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. | In allegato elenco di software autorizzati. L'installazione del software non in elenco deve essere autorizzata dal responsabile della transizione digitale. |
| 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. | |
| 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. | Verifica periodica (almeno annuale) a cura dell'azienda incaricata per la manutenzione software e hardware |
| 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 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. | Ogni postazione è configurata con antivirus e personal firewall e aggiornamento s.o. automatico attivo. L'installazione di nuovi programmi è eseguita sempre in collaborazione con l'azienda informatica specializzata. |
| 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. | La configurazione standard dei client prevede l'installazione del S.O., del software office, software AV, software Gestionale, l'attivazione degli aggiornamenti automatici e la configurazione della rete e delle stampanti. La configurazione standard dei server prevede l'installazione del S.O., software AV, software Gestionale, l'attivazione degli aggiornamenti automatici, la configurazione della rete e dei sistemi di backup. |
| 3 | 2 | 2 | M | Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard. | In caso di compromissione sarà ripristinato il sistema seguendo le indicazioni del punto precedente. |
| 3 | 2 | 3 | S | Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti. | |
| 3 | 3 | 1 | M | Le immagini d'installazione devono essere memorizzate offline. | Le immagini d'installazione sono su cd forniti dal produttore. |

| | | | | | |
|---|---|---|---|---|---|
| 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). | E' richiesto a tutte le aziende di consulenza/assistenza informatica hardware e software di utilizzare connessioni remote sicure durante le varie sessioni di assistenza (es. Teamviewer) |
| 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. | Ad ogni modifica significativa sarà incaricata un'azienda informatica specializzata che fornirà un report con le indicazioni necessarie. |

| | | | | | |
|---|---|---|---|--|--|
| 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. | I software a disposizione dell'ente (es. antivirus) sono impostati per l'aggiornamento automatico e in occasione di ogni passaggio dei tecnici dell'assistenza viene chiesto loro di fare una verifica del funzionamento. In caso incarichi periodici legati alla ricerca di vulnerabilità, le aziende, dovranno garantire di usare software adeguato allo scopo e correttamente aggiornato. |
| 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. | I sistemi operativi e le applicazioni di base (es. pdf, java, etc) sono impostati per l'aggiornamento automatico. Gli aggiornamenti relativi al gestionale sono normalmente comunicati dal produttore |

| | | | | | |
|---|----|---|---|---|--|
| | | | | | ed installati con procedura manuale da parte di ogni operatore con l'eventuale assistenza remota del produttore stesso. |
| 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 sono presenti 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. | |
| 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. | Qualora se ne verificasse la necessità si eseguirà la procedura come indicato. |
| 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.). | Come piano gestione rischi, livelli di gravità rilevato e impatto sugli apparati, si considera ancora valido quanto documentato nel dps 2011. Si evidenzia - la sostituzione dei computer re-inventariata ed aggiornata in allegato alla presente - cambio del personale dipendente e in convenzione e amministratori comunali edotti ai rischi della gestione dati. |
| 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. | I sistemi sono configurati per applicare automaticamente le patch segnalate dai produttori del software come 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. | La limitazione dei privilegi amministrativi viene attuata grazie all'inserimento a Dominio degli utenti i quali a sua volta, se necessario, verranno inseriti nel gruppo Administrator del server. Tali privilegi assegnati solamente all'azienda informatica che si occupa dell'assistenza |
| 5 | 1 | 2 | M | Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato. | Qualora se ne verificasse la necessità si eseguirà la procedura come indicato. L'accesso al sistema è registrato in automatico nei registri eventi di Windows. |
| 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. | Ogni utenza amministrativa è autorizzata tramite lettera di incarico che dovrà essere debitamente firmata. |
| 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. | Prima del collegamento alla rete di un nuovo dispositivo il tecnico preposto all'installazione provvederà a modificare le credenziali con valori coerenti con quelle 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). | Sono impostate password amministrative con lunghezza di almeno 14 caratteri. Per il momento NON sarà introdotto nessun sistema con autenticazioni a due fattori. |
| 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). | E' implementato la sostituzione obbligatoria della password ogni 90 giorni. |
| 5 | 7 | 4 | M | Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history). | E' implementato il controllo sulla possibilità di riutilizzo di una password già utilizzata. |
| 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. | Sono riviste tutte le configurazioni degli utenti e migliorata la gestione dei privilegi per gli amministratori |
| 5 | 10 | 2 | M | Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona. | Ad ogni incaricato con accesso al sistema è stata assegnata una coppia di credenziali specifica. |
| 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. | In caso di situazioni di emergenza che richiedano l'utilizzo delle utenze amministrative anonime (es. root, Administrator, etc) sarà utilizzato un sistema cartaceo per registrare i dati della persona autorizzata ad eseguire l'attività. |

| | | | | | |
|---|----|---|---|--|--|
| 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. | Le credenziali amministrative sono conservate in cassaforte. |
| 5 | 11 | 2 | M | Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette. | Non si utilizzano certificati digitali per l'autenticazione delle utenze locali. |

ABSC 8 (CSC 8): DIFESA 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. | E' presente su tutti i sistemi un antivirus commerciale atto a svolgere l'attività richiesta. |
| 8 | 1 | 2 | M | Installare su tutti i dispositivi firewall ed IPS personali. | Il personal firewall è installato e attivato su tutti gli computer. |
| 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. | Non è ammesso l'utilizzo di ulteriori dispositivi oltre a quelli indicati nell'inventario allegato. |
| 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. | Al momento dell'installazione di nuove apparecchiature la funzionalità è disattivata di default. E' necessario prevedere controlli periodici. |
| 8 | 7 | 2 | M | Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file. | Al momento dell'installazione di nuove apparecchiature la funzionalità è disattivata di default. E' necessario prevedere controlli periodici. |
| 8 | 7 | 3 | M | Disattivare l'apertura automatica dei messaggi di posta elettronica. | Al momento dell'installazione di nuove apparecchiature la funzionalità è disattivata di default. E' necessario prevedere controlli periodici. |
| 8 | 7 | 4 | M | Disattivare l'anteprima automatica dei contenuti dei file. | Al momento dell'installazione di nuove apparecchiature la funzionalità è disattivata di default. E' necessario prevedere controlli periodici. |
| 8 | 8 | 1 | M | Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione. | L'antivirus richiede sempre all'operatore l'esecuzione della scansione ad ogni collegamento di supporto rimovibile. E' necessario prevedere controlli periodici. |
| 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. | Si prevede l'utilizzo di un antivirus o firewall con funzione antispam. |
| 8 | 9 | 2 | M | Filtrare il contenuto del traffico web. | E' prevista l'introduzione entro febbraio 2018 di un firewall in grado di eseguire la mansione richiesta. |
| 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). | E' prevista l'introduzione entro febbraio 2018 di un firewall in grado di eseguire la mansione richiesta. |
| 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. | E' presente un sistema di backup giornaliero e un sistema di disaster recovery per il gestionale. |
| 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. | Le copie di sicurezza sono conservate in armadio protetto da chiave. Le copie per il disaster recovery in cloud avvengono in modalità cifrata. |
| 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. | E' attiva una rotazione con due hard-disk rimovibili collegati al server a rotazione settimanale. Il disco non collegato è conservato in cassaforte. |

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 | Per semplicità di gestione si esegue la copia cifrata di tutti i dati. |

| | | | | | |
|----|---|---|---|---|---|
| 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. | |
| 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. | E' prevista l'introduzione entro febbraio 2018 di un firewall in grado di eseguire la mansione richiesta. |
| 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. | |