Documento Tecnico

Piattaforma OPENVentiquattro®
per la Pubblica Amministrazione

DOCUMENTO RISERVATO

Il presente documento al quale avete avuto accesso autenticandovi alla Piattaforma Applicativa OpenVentiquattro, è riservato. E' pertanto espressamente vietata la divulgarlo, anche parziale, a terzi.

Indice

1. INTRODUZIONE

Nel Codice dell'Amministrazione Digitale (CAD) il concetto Portale Istituzionale assume un ruolo di particolare rilievo, in quanto, è visto come punto d'incontro privilegiato fra la Pubblica Amministrazione (Ente), che eroga una serie di servizi e i cittadini o le imprese che sono i fruitori di tali servizi.

E' necessario o almeno auspicabile che l'Ente renda fruibile un Portale Istituzionale che risponda punto per punto alle esigenze dei cittadini e delle imprese.

In sintesi, deve:

- semplificare le procedure amministrativa;
- snellire le procedure di accesso e partecipazione dei cittadini
- costruire il dialogo tra strutture pubbliche e cittadino (comunicazione);
- proporre un sistema che permetta di adeguare i servizi alle esigenze dei cittadini (riconoscimento delle status con diritti e doveri);
- offrire uno strumento che consenta al cittadino di accedere in maniera unitaria ai servizi della P.A. in una modalità multicanale, cioè attraverso punti di distribuzione fisici e virtuali (internet);

Oltre alla necessità di utilizzare una soluzione che consenta di gestire nel tempo le informazioni in totale autonomia (Content Management), ha la necessità di informare con un sistema multicanale direttamente la propria utenza utilizzando opportunamente strumenti come ad esempio le e.mail e gli SMS. Ha infine la necessità di aprire un canale comunicativo bidirezionale verso la propria utenza con l'uso di strumenti comunicativi diretti basati su servizi tipo form to e.mail (Citizen Relationship Management).

Con le stesse modalità l'Ente ha la necessità di informare i propri dipendenti su procedure, modelli, attività, ecc.. Da qui l'esigenza di attivare opportunamente i servizi presenti su una soluzione Internet (dotata di CMS e CRM) anche all'interno della propria struttura principale realizzando pertanto una INTRANET e verso le strutture periferiche ampliando i servizi ad una EXTRANET.

L'Intranet/Extranet, si basa sulla stessa tecnica di Internet ed è accessibile unicamente a un gruppo predefinito di collaboratori di un'organizzazione. Utilizzando l'Intranet/Extranet si potrà facilitare ai propri collaboratori l'accesso alle informazioni.

Altro elemento del CAD è la Gestione Documentale nel senso che bisognerà trasformare gestioni che mettono la carta al primo posto a complete gestione Digitali del Documento ovvero, prevede **L'ESCLUSIVO USO DEL DOCUMENTO DIGITALE**

Nello steso modo il CAD propone una serie di regole tecniche in materia di gestione documentale (adottate con DPCM 3 dicembre 2013), provvedendo – tra gli altri adempimenti – ad **aggiornare i propri sistemi di protocollo informatico e a predisporre il manuale** della gestione documentale.

È questo il contesto in cui entra in vigore il **Decreto del 13 novembre 2014 sul documento informatico**: adempimenti stringenti che – se disattesi – non solo esporranno gli enti a sanzioni e responsabilità, ma determineranno addirittura l'illegittimità dell'azione amministrativa.

La soluzione proposta, ATTRAVERSO LA SOLUZIONE OPENVENTIQUATTRO, risiede sui server in uso a TechMA ed installati presso la Server Farm di ARUBA S.p.A. senza gravare sugli oneri economici dell'Ente per la realizzazione di una adeguata struttura Hardware e Software nonché di costi per personale specializzato.

Il software applicativo sarà accessibile in modalità FrontEnd e BackEnd, e sarà possibile interagire con il sistema attraverso la tecnologia WEB Services, in accordo ai dettami della architettura SOA (Serviced Oriented Architecture).

OpenVentiquattro® è una piattaforma di servizi online che consente di attuare il processo di dematerializzazione e gestione dei Documenti Informatici includendo un Sistema Documentale Avanzato, il Protocollo Elettronico e l'Archiviazione Sostitutiva. Consente la gestione del Portale internet Istituzionale. Consente di pubblicare comunicati e circolari.

Nel dettaglio OpenVentiquattro include:

1. registrazione (o trasferimento) e mantenimento del dominio **GOV.it**, realizzazione del sito internet a valore legale strutturato in base alla normativa sull'accessibilità e sull'**Amministrazione Trasparente**,
2. **Albo Pretorio** on Line a norma,
3. moduli relativa all'amministrazione trasparente in riferimento alla **Legge 190 (AVCP)** e DL 33 Art. 26, c. 2 e art. 27,
4. attivazione delle **applicazioni per la dematerializzazione** per come previsto dal Codice dell'Amministrazione Digitale incluso sistema documentale, protocollo informatico e strumenti per l'Archiviazione Sostitutiva e la distribuzione elettronica dei documenti digitali (**WorkFlow delle pratiche amministrative**),

5 attivazione dei **connettori per la posta elettronica** che consente di protocollare ed archiviare direttamente dalla vostra PEO (Posta Elettronica Ordinaria) e PEC (Posta Elettronica Certificata) Istituzionale,

6 attivazione dei **servizi di posta elettronica avanzata** che includono la registrazione di una casella di posta elettronica per ogni operatore e l'inoltro di documenti direttamente dalla soluzione OpenVentiquattro,

7 attivazione del sistema per la gestione delle **comunicazioni/circolari**,

8 per le scuole, attivazione del **Registro Elettronico**. Evidenziamo che la nostra soluzione **cosente ai docenti di apporre una firma elettronica avanzata (in abbinamento con i kit disponibili non inclusi) su tutti i documenti prodotti dal registro elettronico**. E' quindi una soluzione che, soddisfando in pieno la normativa, **è a valore legale**.

2. ARCHITETTURA FUNZIONALE

OpenVentiquattro si può considerare articolata in due grandi aree:

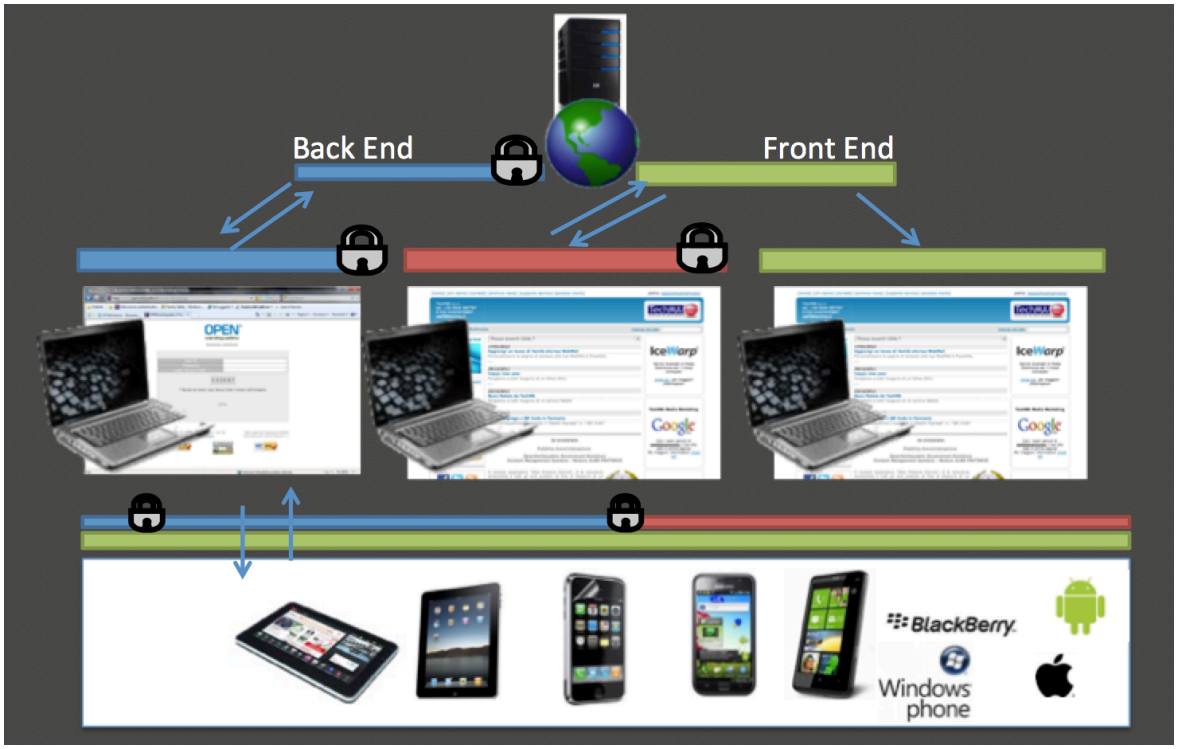
- Area Internet
- Area Intranet / Extranet

Entrambe le aree avranno:

- Area del Front-End alla quale appartengono l'area pubblica e l'area pubblica ad accesso riservato alla quale, ad esempio, i cittadini potranno accedere dopo il rilascio di credenziali di autenticazione;
- Area del Back-End alla quale appartiene l'area di servizio gestionale.

Pertanto l'offerta si compone di:

- Front-End
  - Area pubblica
  - Area ad accesso ristretto (zona autenticata)
- Back End
  - Area Privata (Zona Autenticata)



2.1. Classi di Utenza

OpenVentiquattro è lo strumento operativo attraverso il quale l'Ente può gestire il proprio sistema gestione e conservazione dei documenti e l'erogazione d'informazioni attraverso il proprio sito internet.

L'analisi degli attori di **OpenVentiquattro** consente di individuare due classi di utenti: Gli Utenti Interni e quelli esterni.

Gli utenti interni sono i responsabili dell'operatività e dell'amministrazione di **OpenVentiquattro** come luogo per la produzione e gestione.

Nello specifico è possibile identificare le tipologie e i ruoli previsti:

Classe Utenti Esterni	
Tipologia	**Descrizione**
Utente non registrato (anonimo)	Categoria Chiunque accede al sistema tramite Internet; si tratta di soggetti che richiedo alle sezioni Pubbliche del Portale informazioni generiche (ad esempio sfogliare le sezioni di amministrazione trasparente e accedere alle pubblicazioni dell'Albo). Esigenza primaria Qualità e fruibilità dell'informazione: informazioni corrette, complete e aggiornate rese fruibili attraverso strumenti, di semplice utilizzo, in grado di consentire forme efficaci di accesso all'informazione. Attività (modalità d'interazione) L'Utente è passivo rispetto alle informazioni ricevute; fanno parte di questa categoria tutti i servizi d'informativa, rivolti di volta in volta a tutti indistintamente (**informativa generale**) o a specifici gruppi di interesse (**informativa specialistica**).

	Modello di comunicazione *standard* Ambito operativo Area pubblica (funzioni operative non dedicate).
Utente registrato / riconosciuto (*)	Esigenza primaria Informazioni selezionate, comunicazioni, circolari, ecc. Attività (modalità d'interazione) L'Utente è attivo nel caso in cui esista uno scambio d'informazioni tra l'utente ed il soggetto erogatore di servizi; in questo caso l'utente si configura come una componente attiva del processo di comunicazione (**informativa individuale** e **servizi**). Modello di comunicazione Personalizzato. Ambito operativo Area riservata (funzioni operative dedicate).

(*) L'utente esterno si definisce "riconosciuto" quando il processo di registrazione è integrato da procedure che consentono una forma d'identificazione dell'Utente stesso.

Classe Utenti Interni

Ruolo	**Descrizione**
Amministratore	Categoria Sono gli Amministratori della Piattaforma. Forniscono il supporto delle attività previste dalla gestione dei servizi. Esigenza primaria Garantire il Controllo dei servizi erogati (Erogazione e accesso all'Informazione).

	Attività principale Attività operative connesse alle funzioni di gestione. Gli Amministratori si occupano della creazione e gestione degli utenti; della Definizione e dell'organizzazione (architettura informativa) dei contenuti informativi; gestire il processo di revisione, approvazione e pubblicazione dei contenuti.
	Ambito operativo Area riservata (funzioni operative dedicate).
Utente Interno (Operatore, Redattore, o *content- publisher e Archivisti*)	Categoria Sono operatori, con diritti di gestione dei documenti e pubblicazione sui contenuti informativi che integrano i servizi transazionali; appartengono alla struttura organizzativa dell'Ente. Esigenza primaria Garantire adeguati livelli di qualità (completezza, aggiornamento, coerenza) di contenuti informativi e documenti. Attività principale Gestione del sistema documentale e dei contenuti informativi.
	Ambito operativo Area riservata (funzioni operative dedicate).

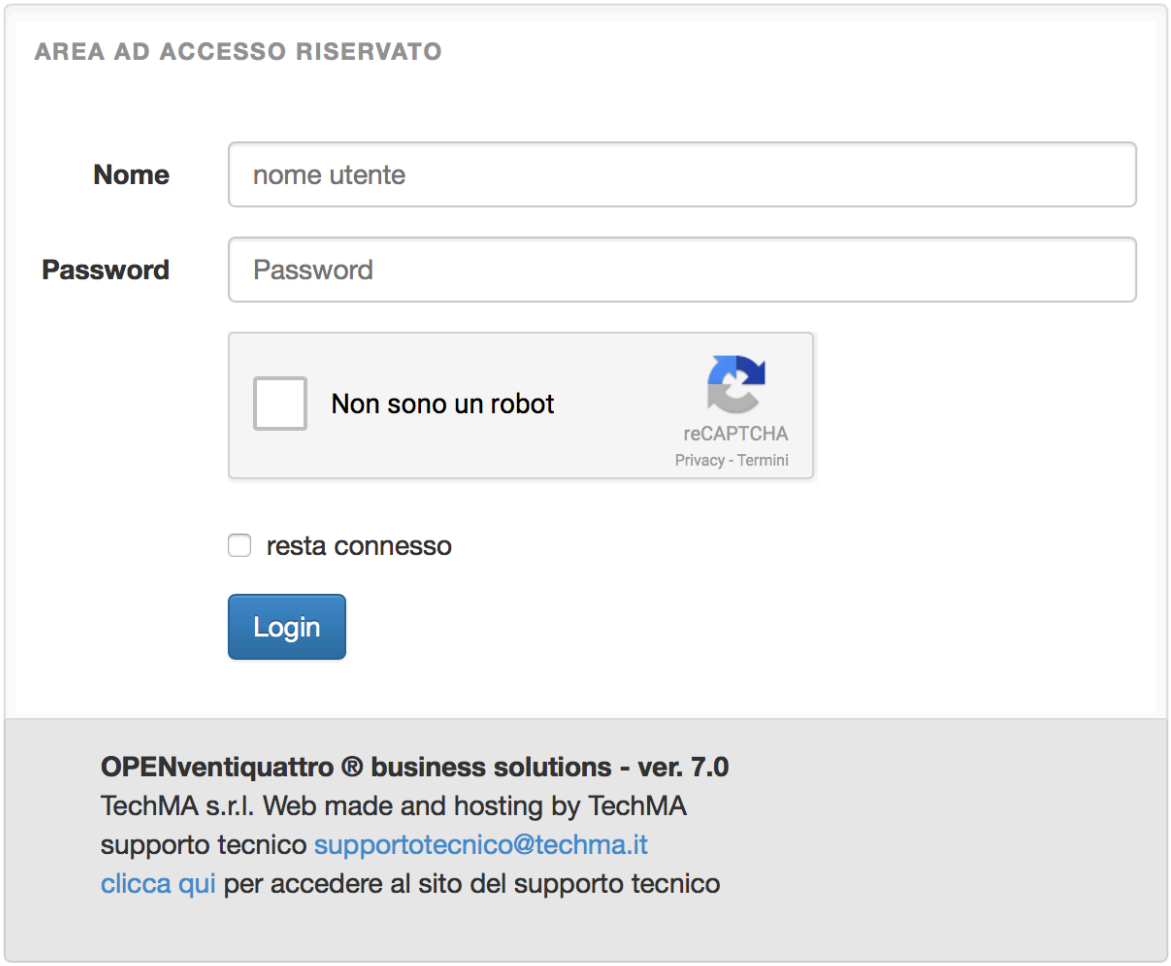
Per soddisfare le esigenze di tutte queste categorie di utenti, la soluzione offre un insieme di caratteristiche che, secondo una strutturazione in livelli, possiamo classificare come:

- **funzionali**, ossia di servizi e funzionalità disponibili per le diverse categorie di utenti, secondo il ruolo di ciascuno nel sistema;
- **applicative**, ossia di componenti e moduli software che implementano i servizi e le funzionalità citati in termini di gestione dell'interfaccia utente, dei contenuti, della sicurezza, ecc.;
- **tecnologiche**, ossia di componenti hardware e software di base e d'ambiente che ospitano e supportano i moduli applicativi citati.

Tale piattaforma consente l'erogazione dei servizi sia attraverso il "Portale Internet" che attraverso il "Portale Intranet/extranet".

2.2. Servizi di Accesso

L'accesso alle aeree riservata (Front e Back End) avviene attraverso protocollo SSL con crittografia a 128 bit e certificato rilasciato da autorità di certificazione e l'utilizzo di Nome Utente e Password in abbinamento alla tecnologia "Captha"



Per proteggere l'accesso, quindi, i propri dati, così come per evitare che qualcuno possa leggere la posta personale, accedere a Computer e a Servizi On Line la soluzione opportuna è l'adozione di password valide.

Le password consentono effettivamente di salvaguardare i dati riservati dagli sguardi indiscreti solo se complesse e aggiornate regolarmente.

Una password complessa ha le seguenti caratteristiche:

1. Ha una lunghezza di almeno otto caratteri (e comunque, più lunga è meglio è)

2. Include lettere maiuscole e minuscole, numeri e simboli
3. Viene cambiata di frequente
4. Ogni nuova password è sensibilmente diversa dalla precedente

Una volta create password complesse o in forma di frase, ci sono 3 modi per garantirne l'efficacia:

- Sconnettersi sempre dal sistema quando si deve lasciare il PC incustodito
- Cambiare le password almeno ogni 90 giorni
- Non condividere le password con nessuno

Sfruttando l'efficacia delle password complesse, si potrà garantire alle informazioni riservate la segretezza che meritano.

2.3. L'architettura funzionale

In riferimento all'erogazione dei Servizi l'Applicazione può essere suddivisa il 6 Aree Applicative:

1) Document Management Systems (Gestione documentale)
    a) Conservazione Sostitutiva
2) Content management Systems (Gestione Contenuti)
    a) portale Pubblico
    b) portale Pubblico ad accesso riservato agli utenti (cittadini e imprese)
    c) portale Intranet/Extranet riservato ai dipendenti
3) Citizien Relationschip Management (Gestione e cura dei Cittadini)
4) Mail Server per i servizi di messaggistica
5) Web Server per i Servizi Applicativi
6) Storage Server e Servizi di BackUp

Ognuna delle 6 Aree viene integrata in un'unica soluzione gestionale e coopera per svolgere

3. Il Document Management Systems (DMS)

Document Management Systems (**DMS**)**,** letteralmente **Sistema di Gestione dei Documenti**, è la risposta immediata alle esigenze di gestione dei documenti scolastici per come previsto **dall'art. 42 del CAD D.Lgs 7/3/2005 n° 82 e note applicative con la deliberazione CNIPA n° 11/2004**.

Consente l'acquisizione di documenti informatici, la creazione dei documenti, la loro gestione, l'assegnazione del Numero di Protocollo Informatico e il flusso operativo.

Con il modulo **WorkFlow** sarà possibile inviare i documenti agli uffici di competenza (o ai responsabili) e seguirne i flussi e le responsabilità di "avanzamento". Tali flussi saranno gestiti tramite avvisi di posta elettronica e sulla scrivania di lavoro di **OpenVentiquattro.**

Con il modulo **Protocollo Informatico** risponde anche alle normative e alle disposizioni emanate dal CNIPA per la gestione documentale nella Pubblica Amministrazione.

Document Management Systems integra strumenti per l'**ARCHIVIAZIONE SOSTITUTIVA**.

L'archiviazione sostitutiva è la procedura legale/informatica regolamentata dalla legge italiana, in grado di garantire nel tempo la validità legale di un documento informatico.

Con il **Modulo** Pubblicazione **integra strumenti per la pubblicazione dei documenti sul proprio sito web scolastico e con accessi Pubblici e/o Riservati.**

Il Modulo **Albo On Line** consente le pubblicazioni degli atti con valore legale.

I Moduli sull' Amministrazione Trasparente consentono le Pubblicazione per come stabilito dall'Art. 26, c. 2 e a art. 27 del **d.lgs. 33/2013** e Art.1 Comma 32 **Legge 190/12 AVCP**.

Il sistema di Document Management, integrato con le soluzioni della piattaforma applicativa OpenVentiquattro fornisce:

a) Garanzie per la sicurezza e l'integrità del sistema;
b) Garanzie per la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita;
c) informazioni sul collegamento esistente tra ciascun documento ricevuto e/o generato;

d) il reperimento delle informazioni riguardanti i documenti registrati;
e) l'accesso alle informazioni in condizioni di sicurezza del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;
f) garanzia per la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

Inoltre, OpenVentiquattro risponde ai seguenti punti:

1) dislocamento: l'architettura software permette la gestione dei documenti a partire dalle varie sedi geograficamente distribuite. Il sistema inoltre gestirà politiche di permessi tra i vari operatori residenti in differenti sedi territoriali. Sarà possibile stabilire per ogni utente una "vista" sul database in modo da limitare, per ogni utente, gli accessi solamente ad una parte del database. Inoltre, a ogni utente potrà essere assegnato un ruolo per stabilire modalità di accesso differenziati.
2) interoperabilità: il sistema di Document Management consentirà l'interrogazione da entità software di terze parti grazie all'utilizzo di WebService e lo standard XML.
3) integrabilità: il DMS sarà completamente indipendente dalla logica applicativa e quindi integrabile con i reali flussi di lavoro dell'Ente.

DMS permetterà all'Ente di ridurre i tempi ed i costi della gestione documentale incrementando nel contempo la produttività e fornendo una soluzione completa per la produzione e gestione dell'archivio elettronico.

Consente agli utenti di creare, archiviare e gestire documenti.

Il DMS, con il Modulo Protocollo Informatico e WorkFlow fornisce, quindi, la memorizzazione di tutte le informazioni necessarie ad adempiere alle indicazioni del CNIPA

3.1. PROTOCOLLO INFORMATICO

Nella Pubblica Amministrazione, secondo la normativa vigente, tutti i documenti dai quali possano nascere diritti, doveri o legittime aspettative di terzi devono essere protocollati.

Il registro di protocollo, da un punto di vista giuridico, è un atto pubblico che fa fede della data di ricevimento effettivo e dell'effettiva spedizione di un documento trattato da una

pubblica amministrazione ed è idoneo a produrre effetti giuridici a favore o a danno delle parti.

Ciascun documento, prodotto o ricevuto da un'amministrazione e da questa protocollato, può essere univocamente identificato attraverso quattro elementi essenziali:

- il numero di protocollo (che deve essere unico per ciascun documento),
- la data di arrivo o di partenza,
- il mittente o destinatario
- l'oggetto

Per il documento informatico l'elemento essenziale è "l'impronta". Affinché possa esistere certezza sulla veridicità delle registrazioni, è necessario garantire che l'interrelazione tra questi elementi essenziali sia costante ed immodificabile. OpenVentiquattro utilizza un sofisticato algoritmo (HASH) che ne rende immodificabile la registrazione.

3.2. Timbratura di protocollo

La timbratura di protocollo è l'apposizione o l'associazione all'originale (informatico) del documento, in forma permanente e non modificabile, delle informazioni riguardanti la registrazione di protocollo del documento stesso: il numero e la data di protocollo, il titolario.

Come per il documento cartaceo in arrivo la timbratura viene posta di norma sul frontespizio del documento tramite un timbro ad inchiostro indelebile recante la dicitura "Prot. N°…. ", data, Titolario, nel documento informatico

l'indicazione del numero di protocollo è immediatamente successiva all'attribuzione alla registrazione del numero di protocollo da parte della procedura informatica.

Per i documenti in partenza, la segnatura può essere apposta tramite timbro, o indicata nel testo del documento.

3.1. WORKFLOW

E' possibile associare ai documenti generati e/o acquisiti un flusso operativo rendendo in qualche modo le informazioni "attive".

E' possibile quindi definire le azioni, i tempi, le persone che devono/possono vedere un documento, da chi deve essere "firmato", quindi revisionato e a chi deve essere distribuito.

Tutto il flusso viene tenuto sotto controllo attraverso lo "stato del documento" ed è possibile attivare automaticamente delle azioni (invio e-mail di notifica, segnalazioni) al verificarsi di determinate condizioni.

3.2. Conservazione Sostitutiva

L'applicativo consente di aggiungere ai dati trattati dal DMS le informazioni previste dalla normativa vigente. La metodologia di attribuzione garantisce l'apposizione della segnatura e l'Impronta obbligatoria nell'archiviazione di documenti ricevuti in maniera elettronica. .

In base a quanto previsto dagli art. 43 e 44 del Codice dell'Amministrazione digitale e dalle regole tecniche in materia di sistema di conservazione, di cui al DPCM 3 dicembre 2013, le P.A. possono ***realizzare al proprio interno un sistema di conservazione****, secondo le suddette regole tecniche o possono* ***richiedere il servizio di conservazione a soggetti, pubblici o privati, accreditati dall'Agenzia per l'Italia Digitale.***

OpenVentiquattro integra strumenti per la "Archiviazione Sostitutiva" attraverso i quali viene prodotto il "Pacchetto di Versamento" e la gestione del suo trasferimento verso il Sistema di Conservazione scelto.

Due le possibilità: Archiviare in "casa" predisponendo un sistema NAS locale o archiviare presso una struttura terza.

Nel primo caso, TechMA può fornire una propria soluzione NAS da installare presso la sede del cliente. Nel secondo caso, OpenVentiquattro è integrato con le procedure per la Conservazione sostitutiva di ARUBA, della quale TechMA è Partner.

Per approfondire l'argomento conservazione sostitutiva si può fare riferimento al "Manuale della Conservazione sostitutiva" disponibile in OpenVentiquattro [Strumenti] > [Download] > [Manualistica]

3.3. LA MESSAGGISTICA

Lo scambio d'informazioni avviene principalmente mediante l'uso di moduli applicativi presenti nel Sistema e l'utilizzo della posta elettronica.

E' possibile utilizzare il sistema di Posta Elettronica Certificata – PEC.

4. Il Content Management System (CMS), Strumento di gestione dei contenuti

Viene sviluppato un sistema di Content Management che risponderà ai seguenti punti:

a) **contenuti del portale** attraverso l'utilizzo di una applicazione Web Based con interfaccia grafica semplice ed intuitiva. Tale interfaccia permetterà di consultare on-line i contenuti del portale ed aggiornare tali dati in maniera sincrona.
b) **indipendenza dal portale:** ciò permetterà al sistema di poter modificare i contenuti senza intervenire sulla struttura e sulle pagine del portale web.
c) **gestione dei contenuti come dati:** i contenuti del sito verranno gestiti come se fossero dati, e non semplicemente testo, in modo da poter indicizzare le informazioni del sito e di utilizzare i dati inseriti anche attraverso software di terze parti.
d) **dislocamento:** l'architettura software proposta permetterà la gestione dei contenuti a partire dalle varie sedi geograficamente distribuite. Il sistema inoltre gestirà politiche di permessi tra i vari operatori residenti in differenti sedi territoriali. Sarà possibile stabilire per ogni utente una "vista" sul database in modo da limitare, per ogni utente, gli accessi solamente ad una parte del database. Inoltre, ad ogni utente sarà assegnato un ruolo per stabilire modalità di accesso differenziati.
e) **interoperabilità:** il sistema di Content Management consentirà l'interrogazione da entità software di terze parti grazie all'utilizzo di WebService e lo standard XML.
f) **integrabilità:** il CMS sarà completamente indipendente dalla logica applicativa del portale.

Il Content Management System permetterà all'Ente di ridurre i tempi ed i costi della comunicazione online incrementando nel contempo la produttività e fornendo una soluzione completa per la gestione dei contenuti Web.

Consente agli utenti di creare, pubblicare e gestire i contenuti. I semplici strumenti disponibili nel Content Management Systems permettono ai collaboratori di pianificare l'aggiornamento dei contenuti, gestire i flussi di lavoro e indicizzare i contenuti direttamente da un browser Internet (modalità sincrona).

Il CMS offre gli strumenti necessari per creare e rilasciare rapidamente l'infrastruttura del Portale Internet, inclusa la struttura del sito, i template per la presentazione dei dati, il layout del sito, l'integrazione delle applicazioni e le funzioni di sicurezza.

CMS memorizza tutti in contenuti in oggetti HTML al fine di assicurare la massima flessibilità.

Il CMS permetterà di inserire oltre a testi anche immagini, file audio, file video, documenti in allegato nei formati più utilizzati (.PDF, .DOC, .XLS, .XML, .P7M, ecc.),

4.1. Interfaccia Grafica e proposizione delle informazioni

Il Portale/Sito web garantisce agli utenti accessi semplici ed immediati.

Ha le seguenti caratteristiche minime:

1. Grafica accattivante, intuitiva, facilità di navigazione
2. Contenuti organizzati in aree tematiche
3. News,
4. Stumenti di ricerca e di orientamento

Contienei seguenti servizi minimi:

di base: tutti i servizi di carattere generale, indipendenti dalle caratteristiche di specificità del dominio applicativo a cui il portale è rivolto: Ricerca testuale sui contenuti del sito, Ricerca semplice, Ricerca avanzata, Mappa del sito, Caselle di posta elettronica.

orientati: tutti i servizi specifici alla natura stessa del portale, e riferibili al proprio dominio di appartenenza distinti in:

- **informazione** (accesso aperto):

○ Generici, per fornire informazioni generali, sulle sedi, etc., con indirizzi, orari, contatti;

○ Tematici, dati e notizie generali;

○ Percorsi orientati, basati su, ad esempio, guide agli studi di settore, segnalazioni in corso, ecc.;

○ interazione:

○ servizi in cui l'accesso è riservato solo agli utenti registrati, con la possibilità di accedere o scaricare: schede sintetiche, convenzioni, iter burocratici, ecc..

4.2. Interfaccia Web e Usabilità

L'interfaccia Web sarà realizzata nel rispetto delle linee guida per l'accessibilità denominate WCAG 1.0 (Web Content Accessibility Guidelines), definite dal consorzio W3C (World Wide Web Consortium) e richiamate dall'Art.2 del Regolamento di attuazione della cosiddetta 'Legge Stanca' (L. 9/Gennaio 2004), e delle tecniche di implementazione proposte nel documento di definizione delle WCAG 1.0.

Inoltre, al fine di 'progettare' sin dai contenuti l'accessibilità di un sito Web, tali linee guida contempleranno sia accorgimenti tecnici, volti a superare gli eventuali limiti tecnologici o a proporre alternative valide, sia accorgimenti volti alla fase di redazione dei contenuti (uso di un linguaggio semplice, spiegazione dei termini stranieri e degli acronimi, etc.).

In particolare, tra i livelli previsti, per il progetto sarà adottato il livello 'A', che definisce gli accorgimenti tecnici principali per la realizzazione di un sito accessibile.

4.3. Accessibilità

L'interfaccia utente deve soddisfare un vasto numero di requisiti di *usabilità*, che consentono agli utenti l'utilizzo semplice e completo del sistema informativo, e di *accessibilità*, che consentono l'accesso ai contenuti ed ai servizi indipendentemente dalla tecnologia utilizzata per accedervi.

Usabilità ed Accessibilità sono quindi due caratteristiche che concorrono ortogonalmente alla produzione di interfacce di qualità.

4.4. IL PORTALE INTRANET/EXTRANET

Come detto, la gestione dei contenuti (inserimento, variazione, e cancellazione di informazioni testuali e multimediali) del portale pubblico e pubblico ad accesso riservato avviene utilizzando la piattaforma su area di Back-End.

Data la sua natura e l'inevitabile contenuto di dati riservati, l'intranet è visibile solo a coloro che avranno avuto autorizzazione. Le autorizzazioni e gli accessi ai contenuti dell'intranet/extranet verranno concessi in base al ruolo, alla carica ricoperta, al settore amministrativo di appartenenza.

L'Intranet offrire i seguenti servizi minimi:

- Un servizio di **messaggeria** che consentirà all'utente dell'Intranet/extranet, una volta "loggato", di visualizzare direttamente sul Portale, senza l'ausilio di software aggiuntivo, i messaggi che ha ricevuto, di compiere delle operazioni di selezione ed archiviazione degli stessi, ed inviare messaggi e comunicazioni ad altri utenti del portale o ad utenti esterni ad esso.
- Una sezione dell'Intranet conterrà **link** verso servizi e sezioni del portale che hanno maggiore importanza per il singolo utente e divisi per argomento. I link saranno dettagliati nella descrizione breve e nelle informazioni sulle funzionalità disponibili nei siti ai quali essi fanno riferimento.
- Nella Intranet/Extranet sarà resa disponibile agli utenti la **modulistica.** Ogni utente avrà a disposizione strumenti di gestione, di creazione, di condivisione della modulistica in base ai suoi privilegi di accesso.

Il Sistema consente all'ente di sviluppare un portale intelligente che connette perfettamente utenti, team e dati, in modo da permettere l'utilizzo vantaggioso di informazioni pertinenti in più processi aziendali e favorire così lo sviluppo di un ambiente di lavoro più efficiente.

E' possibile accedere a tutte le informazioni, i documenti e le applicazioni utilizzati quotidianamente. Sarà possibile trovare e riutilizzare informazioni pertinenti e tempestive di sistemi e report nonché individuare e accedere rapidamente a documenti, progetti e procedure consigliate mediante ricerche nel portale intranet/extranet

4.5. LA MESSAGGISTICA

Lo scambio d'informazioni avviene principalmente mediante l'uso di moduli applicativi presenti nel Sistema e l'utilizzo della posta elettronica.

E' possibile utilizzare il sistema di Posta Elettronica Certificata – PEC.

4.6. Albo On Line

Modulo applicativo integrato al sistema di CMS per la gestione del sito web e DMS per la gestione del documento informatico e protocollo che consente la pubblicazione di delibere, ordinanze, bandi, ecc. come stabilito dalla legge 69/2009.

4.7. Comunicazioni e Circolari

E’ il modulo applicativo integrato al sistema di CMS per la gestione del sito web e DMS per la gestione del documento informatico e protocollo che consente di pubblicare su area riservata comunicazioni e circolari verso gli “Utenti Registrati”.

5. Citizen Relationship Management, mettere il Cittadino al centro

Il Citizen Relationship Management (CRM), ovvero la valutazione, la cura e la gestione delle necessità espresse dalla cittadinanza e il monitoraggio della soddisfazione raggiunta con i servizi offerti, è una delle finalità principali di ogni servizio pubblico e motivo che dovrebbe guidare l'azione di governo locale e centrale nel suo insieme.

La cura delle relazioni con i Cittadini ma anche le Imprese, come previsto dalla Legge 150/2000, è demandata nello specifico all'URP – Ufficio Relazioni con il Pubblico. Più in generale, comunque, si può dire che il Citizen Relationship Management sia una funzione trasversale, che coinvolge tutte le attività amministrative e sta alla base di ogni Patto di Servizio stipulato dagli enti con la cittadinanza.

Il Codice dell'Amministrazione Digitale spinge questo concetto ancora più in là, proponendo agli enti locali e centrali l'uso di strumenti informatici per realizzare questo obiettivo: "Le pubbliche amministrazioni – recita il Codice, all'Articolo 7 – provvedono alla riorganizzazione e aggiornamento dei servizi resi; a tal fine sviluppano l'uso delle tecnologie dell'informazione e della comunicazione, sulla base di una preventiva analisi delle reali esigenze dei Cittadini e delle Imprese, anche utilizzando strumenti per la valutazione del grado di soddisfazione degli utenti".

L'ascolto dei Cittadini/Imprese e la comunicazione interna, i processi di verifica della qualità dei servizi e di gradimento degli stessi da parte degli utenti è fondamentale per programmare interventi e spendere correttamente le risorse pubbliche. In questa logica, il servizio pubblico deve iniziare a considerare il Cittadino e le Imprese come "clienti" da soddisfare, referenti da ascoltare e aiutare nelle loro richieste di assistenza.

La tecnologia può aiutare gli Enti in questo compito, permettendo di comprendere, prevedere e rispondere alle richieste degli interlocutori di un'organizzazione. Grazie al monitoraggio delle istanze dei Cittadini, all'analisi e allo studio di risposte efficaci, ogni Ente potrebbe anticipare e risolvere problematiche di pubblica utilità, favorendo le relazioni Government to Citizen (G2C) e massimizzando il livello di fiducia, nella prospettiva di governare meglio.

Il Progetto può essere integrato delle soluzioni di CRM. OpenVentiquattro Government Solutions – CRM è semplice da usare e da personalizzare offrendo Tecnologie e soluzioni innovative per la Pubblica Amministrazione Digitale una manutenzione efficiente e grande flessibilità nella progettazione di azioni. Utile per il Citizen Relationship Management favorisce la cooperazione, l'analisi e la condivisione, fornendo alla P.A. uno strumento inedito e potente

per la gestione dei contatti. Inoltre, OpenVentiquattro Government Solutions – CRM è facilmente integrabile con la suite OpenVentiquattro ed in particolare con OpenVentiquattro Government Solutions – CMS. Ciò garantisce un'estrema facilità d'utilizzo e una significativa riduzione dei costi e dei tempi necessari per la formazione degli utenti.

OpenVentiquattro è integrato di strumenti quali la gestione dei Ticket (Richieste) attraverso l'attivazione di un servizio di URP On Line.

6. HOSTING E SERVIZI SISTEMISTICI

6.1. Caratteristiche

La piattaforma hardware prevede l'utilizzo di server in uso a TechMA S.r.l. collocati presso la Server Farm di Auba S.p.A. con la seguente configurazione:

- Sistema Operativo: Windows Server 2008 o successive versioni
- HTTPS / SSL Support
- Hosting con Web Server, Applications Server, Data Base Server e BackUp Server su Hardware ad elevate capacità e prestazioni
- Implementazione regole di firewalling su firewall condiviso: HTTP, HTTPS, ILS, POP3, SMTP.
- Manutenzione hardware
- Monitoraggio del server H24x7, con tracing di utilizzo di CPU e RAM, occupazione di spazio disco e corretto funzionamento delle componenti di rete
- Gestione centralizzata del DNS
- Servizi di Posta elettronica con servizio web mail, antivirus ed antispam
- Servizi di Posta elettronica Certificata.

6.2. BackUp Conservazione dei Dati

Sono previsti BackUp della base dati e dei File gestiti sui servizio Hosting di TechMA e BackUp del file di conservazione sostitutiva.

Per la gestione OpenVentiquattro, "**Data Base e Documenti Informatici dell'archivio Corrente**", il servizio di BackUp ha le seguenti policy:

1. BackUp Dati di tipo incrementale con frequenza settimanale
2. BackUp Dati di tipo Completo con frequenza mensile

Per la gestione OpenVentiquattro "Conservazione Sostitutiva" relativamente al **Pacchetto di Versamento generato da OpenVentiquattro**, il servizio di BackUp ha le seguenti policy:

1. BackUp Dati di tipo incrementale con frequenza settimanale
2. BackUp Dati Applicativi di tipo Completo con frequenza mensile

Per la Conservazione Sostitutiva il servizio di backup acquisisce la Policy del "Conservatore" se terzo, oppure, in caso di archiviazione presso l'utilizzatore, il servizio di BackUp ha la seguente Policy:

1. BackUp Dati di tipo conpleto con frequenza settimanale

Infine la piattaforma applicativa è integrata di strumenti di BackUp attivabile direttamente dall'utilizzatore.

7. Gestione della Posta Elettronica

Tramite i **connettori per la posta elettronica** è possibile protocollare ed archiviare direttamente dalla PEO (Posta Elettronica Ordinaria) e PEC (Posta Elettronica Certificata) Istituzionale.

Al fine di una completa interazione dei servizi di posta elettronica con il sistema di gestione documentale è previsto:

- Attivazione di Caselle posta elettronica ordinaria con servizio web mail, antivirus ed antispam sul dominio @nomeente.gov.it
- Certificazione dominio @pec.nomeente.gov.it
- Attivazione di Caselle di Posta Elettronica Certificata sul dominio suddetto

8. Conformità Privacy

TechMA S.r.l., nell'espletamento del servizio di Hosting, Posta Elettronica e Cloud, per l'erogazione dei servizi attraverso piattaforma applicativa OpenVentiquattro Businness e Government Solutions e di tutti i Servizi base ad essi connessi, Utilizza più Server di proprietà Aruba S.p.A. acquisiti attraverso il servizio "Server Dedicato".

Aruba S.p.A. è un Provider autorizzato con concessione n° 473 del Ministero delle Comunicazioni.

Aruba S.p.A., per come previsto sul propria dichiarazione di Conformità Privacy, adotta tutte le misure minime di sicurezza obbligatorie previste dal Disciplinare Tecnico allegato al D.Lgs. n. 196 del 30.06.2003, e più in generale, si è dotata di adeguate misure di sicurezza informatiche ed organizzative atte a garantire la sicurezza, integrità e riservatezza dei dati personali trattati per conto del cliente.

Le misure adottate da Aruba S.p.A. che riguardano la sicurezza fisica dei server e consistono:

- Misure di sicurezza logica a garanzia della riservatezza, integrità e disponibilità dei dati

- Manutenzione periodica delle risorse hardware e software di proprietà di Aruba s.p.a.
- Istallazione e aggiornamento quotidiano sui server di produzione e sulle
- postazioni di lavoro dei dipendenti
- Firewall
- Antivirus
- Antispam
- Back up

Le misure relative ai dipendenti di Aruba s.p.a.:

- Il personale potrà accedere ai dati attraverso un sistema di autenticazione e/o autorizzazione, inoltre è prevista l'adozione di un programma di formazione oltre che un obbligo di riservatezza per i dipendenti di Aruba s.p.a.

Misure di sicurezza degli ambienti fisici:

- Aruba S.p.A garantisce idonee misure di sicurezza tramite la predisposizione ed il mantenimento di un ambiente fisico che impedisca la perdita, la sottrazione, la falsificazione o l' alterazione dei dati consultabili alla pagina http://webfarm.aruba.it/caratteristiche.asp):
  - ◦ Alimentazione:
    - Cabina elettrica dedicata, collegata alla rete elettrica di ENEL, che assicura scalabità ed espandibilità degli oltre 5 MVA attualmente installati.
    - Generatore di elettricità di pari capacità, con motori diesel in grado di sopperire in qualsiasi momento e per qualsiasi periodo di tempo ad eventuali mancanze nelle erogazioni di energia elettrica da parte di ENEL
    - 4 gruppi di UPS da 600Kva ciascuno espandibili n + 2, in parallelo ridondato con durata 2 ore garantiscono una totale sicurezza ed un'ulteriore garanzia di continuità oltre alla protezione da sbalzi, micro - interruzioni e variazioni di tensione.
  - Climatizzazione:
    - Sistema d'aria condizionata flessibile ed espandibile, garantisce una temperatura ed umidità costanti.
    - Nelle sale dati la temperatura è mantenuta costantemente sui 23 gradi.
    - Impianto per il ricambio d'aria attraverso l'espulsione forzata verso l'esterno.
    - Ricambio completo nelle sale dati in meno di 2 ore.
  - Sicurezza:

        - Accesso controllato ai locali con utilizzo di badge
        - Telecamere a circuito chiuso
        - Sistema antincendio ad argonite rilevamento elettronico,
        - sistema antifumo
    - Infrastruttura di sicurezza della web farm. I principali elementi relativi alla sicurezza delle struttura sono i seguenti:
        - Accesso controllato ai locali con utilizzo di badge
        - Presidio fisico 24 ore su 24 sette giorni su sette
        - Telecamere a circuito chiuso
        - Sistema antincendio
        - Sistema antifumo
        - Sistema d'aria condizionata flessibile ed espandibile
        - Controllo temperatura sale dati. La temperatura è mantenuta costantemente sui 23 Gradi
        - Impianto per il ricambio d'aria. Ricambio completo nelle sale dati in menodi 2 ore.

Le misure adottate da TechMA S.r.l. riguardano la sicurezza di accesso fisica ai client utilizzati per l'accesso ai server di Aruba S.p.A. e consistono:

- Misure di sicurezza logica a garanzia della riservatezza, integrità e disponibilità dei dati
- Manutenzione periodica delle risorse hardware e software di proprietà di TechMA S.r.l.
- Istallazione e aggiornamento quotidiano sui server di produzione e sulle postazioni di lavoro dei dipendenti
- Firewall
- Antivirus
- Antispam
- Back up

Misure relative ai dipendenti di TechMA S.r.l.:

- Il personale potrà accedere ai dati attraverso un sistema di autenticazione e/o autorizzazione, inoltre è prevista l'adozione di un programma di formazione oltre che un obbligo di riservatezza per i dipendenti di TechMA S.r.l.

Misure di sicurezza degli ambienti fisici:

- TechMA S.r.l. garantisce idonee misure di sicurezza tramite la predisposizione ed il mantenimento di un ambiente fisico che impedisca la perdita, la sottrazione, la

falsificazione o l'alterazione dei dati tramite Accesso controllato ai locali con utilizzo di Sistema di Allarme.

Ricordiamo, comunque, che i sistemi operativi non vengono creati ne da Aruba S.p.A. ne da TechMA S.rl., pertanto le stesse non possono essere responsabile per eventuali bug di sicurezza dei sistemi operativi stessi e che relativamente virus ed altro software malevoli che possano inficiarne il corretto funzionamento esiste un lasso di tempo imprevedibile fra il momento in cui il virus nasce e si diffonde a quando vengono effettivamente creati i sistemi per la sua eliminazione.

Vi comunichiamo che per inevitabili esigenze di segretezza in merito alle caratteristiche tecniche dei dispositivi di sicurezza che noi adottiamo ai fini della protezione dei dati immessi, non possiamo fornire ulteriori dettagli, proprio per non inficiare i sistemi stessi.

In base al contratto Stipulato fra TechMA e il cliente, quest'ultiomo è titolare dei dati immessi nel proprio servizio web.

In base alla nostra privacy policy, il Cliente non può inserire dei dati sensibili o giudiziari nello spazio condiviso per ragioni di sicurezza ed è tenuto ad un utilizzo conforme alla legislazione sulla Privacy per quanto riguarda il trattamento di dati personali direttamente riconducibile a terzi.

- informazione ex art. 13 D.Lgv 196/2003 nei confronti dei terzi interessati.
- Acquisizione del consenso di terzi alla pubblicazione/diffusione dei dati che li riguardano.
- Adempimento degli ulteriori obblighi di informativa, consenso, autorizzazione, notificazione ove necessari e redazione di proprio DPS facendo riferimento, soltanto dal lato fisico del server su cui è ospitato il dominio, alle misure sopra descritte.
- Prestare particolare attenzione sulle applicazioni e sui software inseriti nel proprio spazio web (Servizio Hosting) al fine di evitare eventuali bugs di sicurezza e/o errate configurazioni.
- Il cliente resta responsabile per qualsiasi conseguenza pregiudizievole che dovesse derivare a causa del mancato rispetto da parte sua della normativa in materia di trattamento dei dati personali.

A carico del Cliente non sussiste nessun limite per quanto riguarda il tipo di dati inseriti attraverso il servizio che ha sottoscritto anche se è consigliabile per il Cliente leggere attentamente la normativa in tema di trattamento dei dati sensibili e giudiziari attraverso strumenti informatici, che implica notevoli adempimenti sia per quanto riguarda aspetti burocratici che di sicurezza (ad

es. consenso scritto, notifiche e autorizzazioni da parte del Garante, obbligo di prendere misure idonee e non solo minime, ecc...). La normativa di riferimento è il D.lgs 196/2003, attuazione della direttiva CE 58/2002, a cui la rinvio. Altre indicazioni utili potranno essere reperite sul sito del garante: www.garanteprivacy.it.

9. IMPLEMENTAZIONE DELLE MISURE MINIME DI SICUREZZA

Sono stati determinati i livelli di copertura prodotti dalle misure poste in essere da TechMA S.r.l. in relazione allegato 2 della circolare Agid 18 aprile 2017, n. 2/2017 relativa alle misure minime di sicurezza informatica per realizzare lo ABSC (Agid Basic Security Control) secondo le seguenti linee:

- ABSC 3 (CSC 3): proteggere le configurazioni di hardware e software sui server
- ABSC 4 (CSC 4): valutazione e correzione continua della vulnerabilità
- ABSC 5 (CSC 5): uso appropriato dei privilegi di amministratore
- ABSC 8 (CSC 8): difese contro i malware
- ABSC 10 (CSC 10): copie di sicurezza
- ABSC 13 (CSC 13): protezione dei dati

Le misure minime di sicurezza sono distinte in tre livelli:

Minimo: È quello al quale ogni pubblica amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme.

Standard: Può essere assunto come base di riferimento nella maggior parte dei casi.

Avanzato: Deve essere adottato dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come obiettivo di miglioramento da parte di tutte le altre organizzazioni.

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

Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza dei server utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv.
3	1	1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Misura implementata. Tutti i server utilizzano una configurazione standard che prevede antivirus e malware, firewall, utente con privilegi di amministrazione, disattivazione di tutte le altre utenze. I server non sono utilizzati per attività di lavoro ordinario. La connessione remota per attività di amministrazione avviene tramite protocolli protetti.	M
		2	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.	Misura implementata: ABSC 3.1.1	S
		3	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	Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del nostro sistema informatico.	A

	2	1	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Misura implementata: ABSC 3.1.1	M
		2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Misura implementata: ABSC 3.1.1	M
		3	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	Misura implementata: ABSC 3.1.1.	S
	3	1	Le immagini d'installazione devono essere memorizzate offline	Misura implementata attraverso la presenza di un server di backup dove trovano installati tutti software necessari. In caso di necessità il sistema viene aggiornato con il backup degli archivi e viene effettuato lo switch dal sistema compromesso a quello di backup	M
		2	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Misura implementata: ABSC 3.3.1.	S
	4	1	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).	Misura implementata: I server non sono utilizzati per attività di lavoro ordinario. La connessione remota per attività di amministrazione avviene tramite protocolli protetti.	M
	5	1	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.	Misura implementata. I server non sono utilizzati per attività di lavoro ordinario.	S
		2	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento	Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del nostro sistema informatico.	A

			automatico, per qualunque alterazione di tali file deve essere generato un alert.		
		3	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.	Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del nostro sistema informatico.	A
		4	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del nostro sistema informatico.	A
	6	1	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	Misura implementata: ABSC 3.1.1	A
	7	1	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	Misura Implementata: ABSC 3.3.1	A

M = Minimo, S = Standard, A = Alto

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

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv.
4	1	1	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.	Misura implementata: L'utilizzo di un sistema di protezione installato su ogni singolo server. Il Sistema protegge i server, per la privacy, password, file, ecc, con gestione tramite l'utenza di Amministrazione.	M
		2	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Misura implementata: ABSC 4.1.1	S
		3	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).	Misura implementata: ABSC 4.1.1	A
	2	1	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Misura Implementare. Analisi periodica attraverso l'utenza di amministrazione dei log generati dal server. Monitoraggio continuo delle attività di tutti i software di sicurezza.	S
		2	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Misura implementata: ABSC 4.2.1	S
		3	Verificare nei Log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabilità	Misura implementata: ABSC 4.2.1	S
	3	1	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto,	Misura implementata: ABSC 4.2.1	S

			utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.		
		2	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.	Misura implementata: ABSC 4.2.1	S
	4	1	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Misura implementata: ABSC 4.1.1	M
		2	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	Misura implementata: ABSC 4.1.1	S
	5	1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Misura implementata: la configurazione dei sistemi prevede la verifica e l'aggiornamento automatico delle patch di sicurezza.	M
		2	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Misura non implementata. Tale dispositivi sono da intendersi non autorizzati e pertanto non possono essere connessi alla rete	M
	6	1	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	Misura non implementata: Privilegi di amministrazione sono solo attribuiti all'Amministratore dei Sistemi.	S
	7	1	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.	Misura implementata: ABSC 4.1.1	M
		2	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.	Misura implementata: ABSC 4.5.1	S
	8	1	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.).	Misura implementata: il piano viene gestito dall'Amministratore dei Sistemi manualmente. Con cadenza mensile l'amministratore dei Sistemi verifica tutti i server abbiano o non abbiano verificato vulnerabilità e che abbiano eseguiti gli aggiornamenti automatici.	M

		2	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabiltà a partire da quelle più critiche	Misura implementata: ABSC 4.8.1	M
	9	1	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.	Misura implementata: ABSC 4.8.1	S
	10	1	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.	Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del nostro sistema informatico.	S

M = Minimo, S = Standard, A = Alto

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

Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv.
5	1	1	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	Misura implementata: Solo l'utenza amministratore ha i privilegi di amministrazione su tutti i server	M
		2	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Misura Implementata: ABSC 5.1.1	M
		3	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Misura Implementata: ABSC 5.1.1	S
		4	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Misura Implementata: ABSC 5.1.1	A
	2	1	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Misura non implementata. Esiste solo l'utenza di Amministratore	M
		2	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Misura non implementata. Esiste solo l'utenza di Amministratore	A
	3	1	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	Misura non implementata: non è previsto nessun collegamento di nuovi dispositivi	M
	4	1	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Misura implementata: vedi ABSC 4.2.1.	S
		2	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Misura implementata vedi ABSC 4.2.1.	S
		3	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Misura implementata vedi ABSC 4.2.1	S
	5	1	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Misura implementata vedi ABSC 4.2.1.	S
	6	1	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio.	Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del nostro sistema informatico.	A

			L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.		
	7	1	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Misura Implementata.	M
		2	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Misura Implementata	S
		3	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Misura implementata: Policy del cambio password come relazionato sul piano per la sicurezza.	M
		4	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Misura implementata: Policy del cambio password come relazionato sul piano per la sicurezza	M
		5	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del nostro sistema informatico.	S
		6	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del nostro sistema informatico.	S
	8	1	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.	Misura non implementata: non applicabile	S
	9	1	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.	Misura non implementata: non applicabile.	S
	10	1	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Misura non implementata: non applicabile.	M
		2	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Misura Implementata	M
		3	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di	Misura implementata: tutte le utenze, ad esclusione di quella di amministrazione non anonima, sono disabilitate	M

			emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.		
		4	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	Misura non implementata: non applicabile.	S
	11	1	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Misura Implementata	M
		2	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Misura Implementata	M

M = Minimo, S = Standard, A = Alto

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv.
8	1	1	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.	Misura Implementata. Software di prevenzione installato e attivo su ogni server	M
		2	Installare su tutti i dispositivi firewall ed IPS personali.	Misura Implementata.	M
		3	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Misura non implementata in quanto i server gestititi dalla nostra società non sono in rete fra di loro.	S
	2	1	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	Misura Implementata	S
		2	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.	Misura non implementata in quanto i server gestititi dalla nostra società non sono in rete fra di loro	S
		3	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	Misura non implementata in quanto i server gestititi dalla nostra società non sono in rete fra di loro	A
	3	1	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Misura Implementata: nessun dispositivo non autorizzato può essere collegato alla rete	M
		2	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Misura non implementata: non applicabile	A
	4	1	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data	Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del nostro sistema informatico.	S

			Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.		
		2	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del nostro sistema informatico.	A
	5	1	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del nostro sistema informatico.	S
		2	Installare sistemi di analisi avanzata del software sospetto.	Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del nostro sistema informatico.	A
	6	1	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Misura implementata relativamente ai server di posta elettronica	S
	7	1	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Misura non implementata: non applicabile	M
		2	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Misura non implementata: non applicabile	M
		3	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Misura non implementata: non applicabile	M
		4	Disattivare l'anteprima automatica deicontenuti dei file.	Misura non implementata: non applicabile	M
	8	1	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Misura non implementata: non applicabile	M
	9	1	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	Misura implementata relativamente ai server di posta elettronica	M
		2	Filtrare il contenuto del traffico web.	Misura implementata: sistema firewall attivo sui software	M
		3	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).	Misura implementata: relativamente ai server di posta elettronica	M

	10	1	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del nostro sistema informatico.	S
	11	1	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.	Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del nostro sistema informatico.	S

M = Minimo, S = Standard, A = Alto

ABSC 10 (CSC 10): COPIE DI SICUREZZA

Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv.
10	1	1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema	Misura Implementata.	M
		2	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software	Misura implementata: vedi ABSC 3.3.1	A
		3	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamento nella fase di restore	Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del nostro sistema informatico.	A
	2	1	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova	Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del nostro sistema informatico.	S
	3	1	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 in cloud	Misura Implementata	M
	4	1	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	Misura Implementata	M

M = Minimo, S = Standard, A = Alto

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv.
13	1	1	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	Misura Implementata: tali misure sono proprie del sistema Documentale e dei nostri Software Gestionali.	M
	2	1	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Misura non implementata: non applicabile	S
	3	1	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.	Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del nostro sistema informatico.	A
	4	1	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.	Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del nostro sistema informatico.	A
	5	1	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.	Misura non implementata: non applicabile	A
		2	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)	Misura non implementata: non applicabile	A

			cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.		
	6	1	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.	Misura non implementata: non applicabile	A
		2	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	Misura non implementata: non applicabile .	A
	7	1	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Misura non implementata: non applicabile	A
	8	1	Bloccare il traffico da e verso url present in una blacklist.	Misura non implementata: non applicabile	M
	9	1	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..	Misura non implementata: non applicabile	A

M = Minimo, S = Standard, A = Alto