Documenti di sicurezza

Questo allegato riporta - in conformità con il paragrafo 2.1 delle Linee guida AGID - i documenti INAPP relativi alla protezione dei dati per come relazionabili al SGD (Sistema di gestione documentale). Si è ritenuto opportuno entrare maggiormente nel dettaglio del sistema FOLIUM/CIVILIA in quanto l'uno gestisce il SGD (FOLIUM) l'altro i processi (CIVILIA) da cui si generano documenti; i due sistemi sono integrati ed è per questo motivo che il documento tecnico in calce del fornitore Dedagroup riporta come titolo Scheda tecnica Civilia.

ALLEGATO 7

ALLEGATO 7

INAPP
PUBLIC POLICY INNOVATION

Linee Guida LAVORO AGILE o SMART WORKING in sicurezza

In relazione alla nuova modalità di lavoro, denominata Lavoro Agile o Smart Working, attivata dall'INAPP a seguito dell'emergenza sanitaria determinata dalla diffusione del Covid19, con la presente si intende fornire una linea guida sulla sicurezza informatica dei dispositivi personali utilizzati dal personale (pc, smartphone, tablet).

La Legge n.120 del 11 settembre 2020 ha modificato l'articolo 12 **Norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa** del CAD Codice dell'Amministrazione Digitale, che al comma 3 bis prevede:

3-bis. I soggetti di cui all'articolo 2, comma 2, favoriscono l'uso da parte dei lavoratori di dispositivi elettronici personali o, se di proprietà dei predetti soggetti, personalizzabili, al fine di ottimizzare la prestazione lavorativa, nel rispetto delle condizioni di sicurezza nell'utilizzo.

Queste linee guida recepiscono le raccomandazioni elaborate da AGID in materia di misure minime di sicurezza per le Pubbliche Amministrazioni e intende supportare il personale dell'INAPP nell'utilizzo sicuro e consapevole dei propri dispositivi.

Di seguito le raccomandazioni per il Lavoro Agile/Smart Working sicuro

- Segui prioritariamente le policy e le raccomandazioni dettate dall'ente
- Utilizza i sistemi operativi per i quali attualmente è garantito il supporto
- Effettua costantemente gli aggiornamenti di sicurezza del tuo sistema operativo
- Assicurati che i software di protezione del tuo sistema operativo (Firewall, Antivirus, ecc) siano abilitati e costantemente aggiornati
- Assicurati che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy emanate dall'ente
- Non installare software proveniente da fonti/repository non ufficiali
- Blocca l'accesso al sistema e/o configura la modalità di blocco automatico quando ti allontani dalla postazione di lavoro
- Non cliccare su link o allegati contenuti in email sospette
- Utilizza l'accesso a connessioni Wi-Fi adeguatamente protette
- Collegati a dispositivi mobili (pen-drive, hdd-esterno, etc) di cui conosci la provenienza (nuovi, già utilizzati, forniti dall'ente)
- Effettua sempre il log-out dai servizi/portali utilizzati dopo che hai concluso la tua sessione lavorativa."

INAPP – Istituto Nazionale per l'Analisi delle Politiche Pubbliche
Corso d'Italia, 33 – 00198 Roma (RM) – C.F. 80111170587
tel. +39.06854471 – fax +39.0685447334 - protocolloinapp@pec.it - www.inapp.org

Documenti di sicurezza-Sistemi informativi

In aggiunta alle suddette raccomandazioni fornite dall'AGID, ai fini di un corretto e sicuro utilizzo, evitate di lasciare web-cam e microfoni sempre attivi in quanto potrebbero essere oggetto di attacco informatico a scopo di intercettazione o sorveglianza, ed attivati da remoto (senza alcun segnale visivo o audio).

Di seguito misure minime da seguire per minimizzare i rischi potenziali in caso di attacco

- Assicurarsi che il software di sicurezza sia sempre aggiornato. Questo vale anche per il sistema operativo e per le applicazioni nel dispositivo che hanno accesso alla webcam.
- Tenete sempre attivato il firewall che impedisce accessi non autorizzati al computer e abusi dei dati.
- La spia, che avvisa se la webcam è attiva o meno, può essere aggirata da parte di potenziali aggressori. Quando non si utilizza il portatile, tenerlo sempre chiuso. Se si dispone di una webcam esterna collegata alla porta USB del computer, connetterla solo prima di utilizzarla.
- Utilizzare la rete domestica protetta da password complessa.

ALLEGATO 7

INAPP
PUBLIC POLICY INNOVATION

PASSWORD POLICY

La gestione delle credenziali di accesso

Obiettivi generali

Ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i.,Codice in materia di protezione dei dati personali nonché del Regolamento generale per la protezione dei dati personali n. 2016/679 (General Data Protection Regulation o GDPR) occorre definire misure di protezione adeguate ed idonee per il trattamento e la tutela dei dati personali degli utenti.

La protezione delle credenziali di accesso rappresenta uno dei principi fondamentali della sicurezza delle informazioni, in particolare la creazione e la gestione delle password che costituiscono la principale contromisura agli accessi non autorizzati.

In questo documento viene definita la procedura - password policy- che stabilisce i criteri per la creazione, l'utilizzo, la conservazione e la gestione delle credenziali di autenticazione fornite agli utenti per l'accesso ai servizi informatici erogati.

In generale, i servizi informatici presenti in Istituto individuano, come strumento di accesso per gli utenti, un sistema di autenticazione (e di autorizzazione) basato su credenziali di accesso.

Esso consiste in un codice per l'identificazione dell'utente ("*username*" o "*nome utente*"), associato ad una parola chiave riservata ("*password*") conosciuta esclusivamente dal solo utente. I due elementi, uniti insieme, costituiscono la credenziale di accesso ("*account*" o "*utenza*") così come definito dalla normativa vigente in tema di dati personali.

Campo di Applicazione

La password policy si applica a tutti i servizi informatici centrali, gestionali ed applicativi, compresi quelli web, alle postazioni di lavoro, al servizio di posta elettronica e a tutte le applicazioni e risorse informatiche presenti in Istituto che prevedono un sistema di autenticazione per l'accesso.

Responsabilità degli amministratori di sistema

Gli amministratori di sistema devono proteggere la riservatezza e l'integrità delle password sui sistemi da loro gestiti e configurare i servizi informatici per soddisfare i requisiti della presente password policy.
Lo username viene assegnato, salvo diverso avviso, esclusivamente dall'amministratore del servizio (o amministratore del sistema) o da un suo delegato. La password viene gestita, dopo la sua prima assegnazione da parte dell'amministratore, esclusivamente dall'utente, con l'eccezione dei casi in cui particolari eventi richiedano il reset della password e la sua riattribuzione.

Il codice identificativo è univoco e non potrà più essere riassegnato ad altri soggetti, nemmeno in tempi successivi, al fine di garantire un'archiviazione e storicizzazione delle utenze (come riportato dalla normativa vigente in tema di dati personali).
Le credenziali di accesso non utilizzate da almeno 6 (sei) mesi verranno disattivate (salvo diversa preventiva autorizzazione legata a motivazioni tecniche oggettive)
Le credenziali devono essere disattivate anche quando l'utente perde il ruolo, la mansione e le qualità che gli consentono di utilizzarle per accedere ai vari servizi d'Istituto (es. cessazione del rapporto di lavoro, trasferimento, etc etc.).

Le credenziali sono personali e non vanno comunicate ad altri

Le password di default - come quelle che vengono inizialmente comunicate ai nuovi utenti o in caso di reset password - devono essere cambiate dall'utente al primo accesso. Tale cambio password viene imposto all'utente dal sistema.

Si evidenzia che l'invio / comunicazione delle credenziali (username e password) avverrà con canali di trasmissione diversi e in momenti non temporalmente contigui

ALLEGATO 7

Responsabilità degli utenti

Gli utenti si impegnano a rispettare i criteri di creazione, conservazione e gestione delle credenziali di accesso di seguito indicati.

Gli utenti, una volta in possesso delle credenziali, devono cambiare la password al primo accesso rispettando i criteri di seguito descritti, evitando combinazioni facili da identificare. Devono scegliere password univoche, che abbiano un senso solo per l'utente che le sceglie, evitando di usare la stessa password per altre utenze.

La password è strettamente personale e non deve essere comunicata e/o condivisa con nessun'altra persona all'interno dell'Istituto.

Gli utenti devono prestare attenzione a fornire le proprie credenziali di accesso, a rispondere ad e-mail sospette e/o a cliccare sui link durante la navigazione web (o nella mail) al fine di contrastare possibili frodi informatiche (come il phishing, lo spear phishing, il furto d'identità, ecc.).

Ogni utente è responsabile di tutte le azioni e le funzioni svolte dal suo account.

Qualora vi sia il sospetto che le credenziali assegnate possano essere conosciute da terzi, l'utente dovrà cambiare immediatamente la password.

La memorizzazione della password non deve essere effettuata su supporti custoditi nel medesimo ambiente che ospita la postazione di lavoro.

Qualora l'utenza venga bloccata a seguito della scadenza della password oppure sia necessario modificare la password perché dimenticata ovvero a fronte di qualsiasi altra motivazione, l'utente deve contattare il servizio di assistenza tecnica o l'amministratore di sistema.

Requisiti tecnici per la creazione e gestione delle password

Come regola generale, la password deve essere ragionevolmente complessa e difficile da individuare e/o ricavare.

Documenti di sicurezza-Sistemi informativi

Nei limiti tecnici consentiti dai sistemi, la password:

- ✓ deve essere di lunghezza non inferiore ad 8 caratteri oppure, nel caso in cui il sistema non lo dovesse prevedere, di lunghezza pari al massimo consentito;
- ✓ deve essere obbligatoriamente cambiata al primo utilizzo e successivamente almeno ogni 6 (sei) mesi;
- ✓ deve contenere, ove possibile, almeno 3 caratteri tra numeri, caratteri alfabetici in maiuscolo e minuscolo, e caratteri speciali;
- ✓ deve essere sempre diversa dalle ultime 5 precedentementeutilizzate;
- ✓ non deve presentare una sequenza di caratteri identici o gruppi di caratteri ripetuti;
- ✓ deve essere nota esclusivamente all'utilizzatore e non può essere assegnata e/o comunicata ad altri;
- ✓ non deve contenere riferimenti agevolmente riconducibili all'utente o ad ambiti noti;
- ✓ non deve essere basata su nomi di persone, date di nascita, animali, oggetti o parole ricavabili dal dizionario (anche straniere) o che si riferiscano ad informazioni personali;
- ✓ non deve essere memorizzata in funzioni di log-in automatico, in un tasto funzionale o nel browser utilizzato per la navigazione internet.

Ove tecnicamente possibile, i requisiti di cui ai punti precedenti vengono imposti da meccanismi automatici del sistema.

Per motivate necessità di urgente accesso alle informazioni, in caso di impedimento del titolare delle credenziali, la password può essere annullata e sostituita dagli amministratori di sistema con una nuova password.
In questo caso la nuova password dovrà essere consegnata dall'amministratore di sistema all'utente, il quale dovrà modificarla al primo accesso

ALLEGATO 7

INAPP

Dedagroup Public Services
Scheda tecnica Civilia

Appendice A all'Atto di Nomina a Responsabile Trattamento
Caratteristiche del software applicativo ed elenco delle misure tecnico-organizzative
in carico al Responsabile del trattamento
(In Applicazione del Regolamento Europeo in materia di protezione dei dati personali)

DEDAGROUP PUBLIC SERVICES

Novembre 2021

Il file è incorporato pertanto è visibile solo on line non stampare

Dedagroup Public Services
Scheda tecnica Civilia

Appendice A all'Atto di Nomina a Responsabile Trattamento
Caratteristiche del software applicativo ed elenco delle misure tecnico-organizzative in carico al Responsabile del trattamento
(In Applicazione del Regolamento Europeo in materia di protezione dei dati personali)

Novembre 2021

Sommario

Civilia

Con il termine Civilia raggruppiamo 3 suite applicative che Dedagroup Public Services ha prodotto e che sono in esercizio presso la propria clientela in un percorso evolutivo che ha visto, nel tempo, affermarsi le architetture client/server, web e cloud.
Alle tre suite applicative che permettono la gestione di svariate Aree delle Pubbliche Amministrazioni Locali è associata di norma una quarta suite, denominata Open web, che si può interfacciare a ciascuna delle 3 suite di base per fornire servizi on line: albo pretorio, trasparenza amministrativa e, più in generale quelle che si definiscono "pratiche on line"
La presente scheda sintetizza le caratteristiche tecniche di ciascuna delle nostre soluzioni viste nell'ottica del General Data Protection Regulation. Per ciascuna architettura è stato predisposto un documento di maggior dettaglio che mettiamo a disposizione on line per la clientela.

Civilia Next

GDPR ED IL CLOUD MICROSOFT AZURE

La suite Civilia Next si appoggia su Microsoft Azure, piattaforma di cloud computing conforme alle leggi sulla privacy tra Unione Europea e Stati Uniti e alle clausole del modello UE con criteri di privacy e misure di sicurezza leader di settore per proteggere i dati nel cloud, incluse le categorie di dati personali specificate dal GDPR.

- Gestione delle identità e controllo dell'accesso: Azure AD (Active Directory). gli utenti autorizzati possono accedere ad ambienti, ai dati e alle applicazioni; le operazioni effettuate dal singolo utente applicativo sono tracciate in tempo reale;
- I servizi e gli strumenti di Azure indicati di seguito sono di supporto a soddisfare gli obblighi del GDPR:
    - monitoraggio continuo delle risorse, raccomandazioni sulla sicurezza; prevenzione delle minacce; analisi avanzate integrate (Centro sicurezza di Azure Microsoft);
    - crittografia automatica dei dati by design (storage Microsoft) secondo lo standard AES 256.
    - anonimizzazione dei dati sensibili
    - controllo e registrazione (configurabili) degli eventi, identifica e corregge problemi di sicurezza, in modo da impedire le violazioni. (Log Analytics di Azure)
- SQL Server e il database SQL di Azure sono servizi Microsoft integrati che offrono standard di sicurezza avanzati, con criteri che rispettano le politiche di *privacy by design e by default* tipiche del GDPR.

Le funzionalità di sicurezza predefinite consentono la riduzione dei rischi e l'adeguamento ai principi del Regolamento europeo in materia di protezione dei dati personali:

- Il firewall del database SQL di Azure limita l'accesso ai singoli database all'interno del server; l'accesso è quindi consentito esclusivamente alle connessioni autorizzate.
- L'autenticazione di SQL Server garantisce l'accesso al server di database ai soli utenti autorizzati con credenziali valide. Le autorizzazione di SQL Server permettono di gestire gli accessi ai dati in base al principio dei privilegi minimi.
- La mascheratura dei dati dinamica è una funzionalità predefinita usata per limitare l'esposizione dei dati sensibili.

Protezione dei dati personali dalle minacce alla sicurezza. Le funzionalità predefinite di SQL Server e del database SQL di Azure assicurano la protezione dei dati e l'identificazione delle violazioni:

- Transport Layer Security (TLS) è utilizzato per la protezione dei dati in transito nelle connessioni al database SQL.

- Audit Log con cui è possibile produrre un log di controllo in grado di identificare le possibili minacce o i casi sospetti di abuso o violazione della sicurezza.
- Sistema di rilevamento delle minacce integrato, rileva attività insolite e sospette. Con questo strumento è possibile soddisfare il requisito relativo alla notifica delle violazioni dei dati imposto dal GDPR.

CERTIFICAZIONI DEL CLOUD MICROSOFT AZURE

Azure soddisfa un'ampia gamma di standard di conformità internazionali (vedi dettagli)

POLITICHE DI BACKUP

È garantita l'esecuzione periodica e programmata di procedure di backup; ciò consente di far fronte alle situazioni in cui sussiste una esigenza di immediato recupero dei dati a prescindere dalla causa.

PAIRED REGION

Ai fini di business continuity e disaster recovery le regioni sono abbinate in "Regional Pair", in caso di disastro i servizi sono ripristinati nella regione "associata".

BACKUP DI TIPO POINT-IN-TIME

Azure mette a disposizione un restore automatico (point-in-time) di SQL Azure che assicura il ripristino su un periodo fino a 35 gg precedenti dalla data attuale.
La periodicità con cui i backup vengono effettuati automaticamente da Microsoft è di 5 minuti.

BACKUP DI TIPO LONG-TERM

Dedagroup ha utilizzato lo strumento di Azure "*Recovery Service Vault*" che permette di avere un backup settimanale del database per 10 anni dalla data di esecuzione.

BACKUP DI TIPO GEO-REPLICATION

Dedagroup ha attivato la feature di SQL Azure di replica geografica (geo-replication): l'opzione consente di replicare l'istanza principale del servizio (Amsterdam, Olanda) con l'istanza secondaria (Dublino, Irlanda).

BACKUP DI TIPO SCRIPT POWERSHELL

Dedagroup ha sviluppato degli script di backup che giornalmente eseguono una copia di un database SQL AZURE copiando i files prodotti dal backup in due diverse storage crittografati su due diversi siti geografici.

STORAGE DI ARCHIVIAZIONE

Dedagroup adotta l'opzione GRS (Geo Redundant Storage) che garantisce, ai fini di disaster recovery e business continuity, una copia dei dati nella regione "pair" Azure.

BUSINESS CONTINUITY E DISASTER RECOVERY

Particolare attenzione è stata posta nell'attuazione di un piano di continuità operativa: i dati e l'intera infrastruttura di Civilia Next è replicata in una seconda region di Microsoft Azure.

ACCESSO AI DATI E ALL'APPLICATIVO

L'accesso alla suite CiviliaNext e quindi ai dati avviene tramite browser su protocollo https, i dati scambiati vengono protetti dal protocollo TLS (Transport Layer Security) che garantisce tre livelli di protezione fondamentali: **Crittografia, Integrità dei dati, Autenticazione.** Si evitano così attacchi di tipo man-in-the-middle.

INTEROPERABILITÀ E SICUREZZA

La suite CiviliaNext espone servizi REST che consentono l'integrazione con moduli software di terze parti, l'accesso è consentito soltanto previa autenticazione di tipo oauth2 su protocollo https.
Non è consentito in nessun caso l'accesso diretto ai dati.

POLICY PASSWORD DI ACCESSO

Il sistema di autenticazione impone un cambio password ogni 60 gg e una complessità minima.
Le policy sono descritte compiutamente nel documento di riferimento "Scheda tecnica Civilia Next"
È gestita la politica "Strong password".

TRATTAMENTO NELL'AMBITO DELL'ACCESSO ALLA SUITE

Dedagroup non detiene le password degli utenti nei propri archivi avvalendosi di Azure AD come sistema di autenticazione. È cura del cliente il rispetto delle norme sulla conservazione e gestione delle password.

TRASFERIMENTO DEI DATI ALL'ESTERO

Dedagroup si avvale dei datacenter europei di Microsoft, in particolare quelli presenti in Olanda e come secondario in Irlanda, i dati non sono trasferiti al di fuori del territorio europeo.

UTILIZZO SPAZI DI ARCHIVIAZIONE

Lo storage di archiviazione per i file prodotti nell'uso dell'applicativo Civilia Next utilizza un sistema di crittografia/decrittografia trasparente con algoritmo AES a 256 bit conforme a FIPS 140-2 con chiavi univoche gestite da Microsoft, questo assicura che in nessun caso lo spazio utilizzato e successivamente eliminato possa essere riutilizzato.

TRACCIAMENTO (LOG)

Nel documento di riferimento "Scheda tecnica Civilia Next" sono definiti gli ambiti del servizio di tracciamento, le informazioni tracciate e gli attributi W3C. Vengono anche descritte le finalità del tracciamento e, in un apposito paragrafo, la valutazione di impatto e i rischi del trattamento.

ENTRY POINTS ED EXIT POINTS DEL SISTEMA CIVILIANEXT

PUNTI DI INGRESSO AI SISTEMI

I punti di ingresso alle componenti infrastrutturali sono di esclusiva competenza del fornitore: Portale di amministrazione Azure; Componenti infrastrutturali: *Database*, *Cache*, *Storage*, *Sistema di logging*, *Componenti PaaS*, *Console di monitoraggio*, *Macchine virtuali.*
L'accesso è ristretto agli amministratori di sistema autorizzati e censiti che accedono con protocollo *https* e sistema di autenticazione certificato (Azure AD). Le attività svolte sono tracciate in appositi log.

PUNTI DI USCITA DAI SISTEMI

Il sistema "CiviliaNext" non dipende da componenti infrastrutturali esterni all'ambiente Azure.
Non si presentano quindi elementi di rischio collegati ad un possibile data leak nella comunicazione tra sistemi.

PUNTI DI INGRESSO DEL SOFTWARE

Possiamo considerare i punti di ingresso al software CiviliaNext

- L'accesso all'applicazione WEB
- L'accesso mediante Web API

Ai fini della valutazione del rischio per attacchi informatici e quindi *data breach* si può dire che l'utilizzo del protocollo *https* e di un sistema di autenticazione certificato (Azure AD) porta ad una valutazione bassa del rischio per i primi due punti.

PUNTI DI USCITA DEL SOFTWARE

I punti di uscita possono essere considerati gli elementi sistemistici infrastrutturali come Database, Storage, Cache. La comunicazione tra l'applicativo e questi elementi avviene su canale cifrato e attraverso chiavi di accesso.
Il database è protetto da firewall che consente l'accesso solo ad ip autorizzati.
È possibile considerare basso quindi il rischio caratterizzante queste componenti.

Civilia Web

CiviliaWeb - Atti Formali e Procedimenti Amministrativi è un modulo software dedicato alla gestione dei procedimenti amministrativi, utilizzato principalmente nell'ambito degli atti formali, delle pratiche edilizie e delle pratiche SUAP ma che viene spesso utilizzato come "generatore di applicazioni" per problematiche inerenti il workflow strutturato.
Civilia Web – Protocollo Informatico (Folium) è un modulo software dedicato alla gestione a norma del protocollo informatico.
Nel prosieguo ci riferiremo a Civilia Web per descrivere le caratteristiche comuni ai due sistemi.
La suite prevede un'architettura composta da più livelli (compliant J2EE) tipicamente rappresentata da un RDBMS (Oracle o Postgres), un servizio documentale (Alfresco con relativo repository) oppure direttamente su filesystem (fileserver) o all'interno del DBMS (IFS), un server applicativo (JBoss) o un servletcontainer (Tomcat) ed un web server.
L'applicativo è multi piattaforma (linux, windows, altro...) scritto in java.

Il sistema Civilia Web può essere erogato come Saas oppure può essere governato integralmente presso i server del cliente finale.
Nel prosieguo vengono descritte le caratteristiche by design del software. Ai fini della tutela della privacy devono essere considerate separatamente le architetture Saas e Web.

GESTIONE IDENTITA' - PRESENZA DI UN IDENTITY MANAGER ALL'INTERNO DELL'ENTE

Il sistema è predisposto per attivare IM centralizzati in grado di strutture IM esterni (es. LDAP, Active directory) integrandosi nativamente con l'IM già in dotazione del cliente.
Gli IM, sistemi integrati di tecnologie, criteri e procedure, consentono alle organizzazioni di controllare gli accessi degli utenti ad applicazioni e dati critici, proteggono contestualmente i dati personali da accessi non autorizzati.

BLINDATURA DEI SISTEMI SERVER

Nel caso di installazione presso il cliente, l'utente finale (titolare dei dati) avrà il compito di collocare i server in luoghi il più possibile sicuri, dotati di sorveglianza e/o di controllo degli accessi. Potranno essere usati firewall ed altri meccanismi per permettere l'accesso alle sole risorse necessarie e dai componenti conosciuti della architettura. Lato integrità dei dati ci si affida per la coerenza al database di riferimento (Oracle, Postgres) ed al documentale in uso (Alfresco, IFS).

ACCESSO ALL'APPLICATIVO

Agli applicativi CiviliaWeb si accede tramite portale o webservice solo previa autenticazione.
Il protocollo utilizzato per i portali che espongono il servizio in internet è *https* (anche noto come HTTP over TLS, HTTP over SSL e HTTP Secure) mentre in ambito LAN il cliente a volte ha la facoltà di utilizzare protocollo *http*, visto l'isolamento dei luoghi fisici.

CONDIVISIONE DI RISORSE

CiviliaWeb non condivide risorse se non tramite i webservice opportunamente configurati ed abilitati, sottoposti a proprie rigorose regole di visibilità.

ISOLAMENTO DELLE PERIFERICHE E CONTROLLO DEVICE

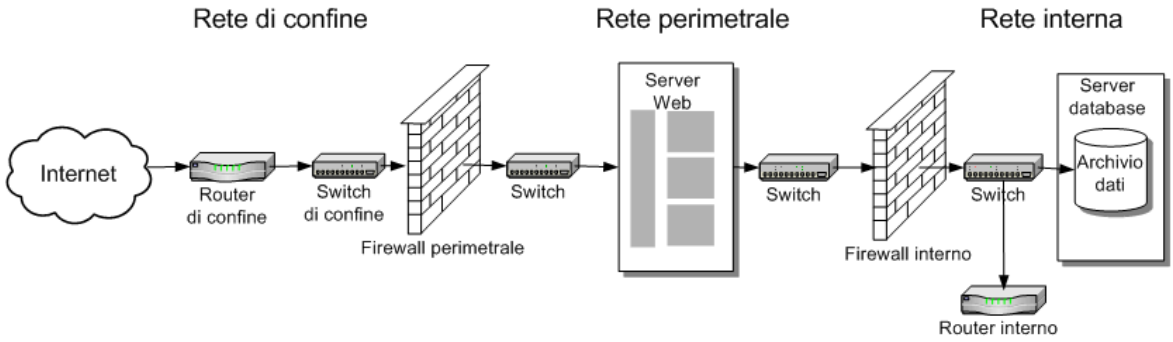
L'utilizzo di strumentazione esterna (ad esempio scanner o stampanti di etichette) non viene direttamente controllata da CIVILIAWEB. Viene eventualmente delegato il controllo alla singola postazione e/o alle policy di dominio.

SISTEMA ANTIVIRUS (ANTI MALWARE)

L'adozione di strumentazioni di sicurezza atte a limitare i rischi e gli accessi o attacchi dall'esterno deve essere tenuta in debita considerazione.
È consigliata una strategia di limitazione degli eventi, attuando specifiche azioni come l'adozione di sicurezza attiva/passiva (antivirus, anti malware).

FIREWALL DI FRONTIERA

L'isolamento del back-end (database, storage) è passo fondamentale per preservare l'informazione come bene aziendale. Deve essere garantita la sicurezza da attacchi esterni e/o dolosi.
La presenza di apparecchiature di frontiera (firewall), garantisce l'integrità e la coesistenza di necessità applicative con la navigazione extranet/internet.



BACKUP E D&R

Nel caso di installazioni in ASP presso il datacenter Dedagroup Spa, il servizio SaaS soggiace a regole di Business Continuity e D&R espressione del singolo datacenter. Presso il datacenter di Dedagroup Spa le Virtual machine (VM) sono sottoposte a snapshot giornalieri (ovvero istantanee dello stato del sistema in un particolare momento) con retention di 10 gg.
Ulteriormente vengono mantenuti da Dedagroup Spa backup settimanali su librerie con retention 3 mesi. Alcune VM (servizi) sono costantemente allineate con un sito di D&R (Roma) che può in ogni momento eseguire il recovery secondo politiche di consistenza e coerenza. Nel caso di *failure* il sistema ripristinato sul sito D&R può essere raggiungibile riconfigurando le VM secondo nuove regole dettate dai DNS.
Nel caso di installazioni non in ASP, cioè presso i server del cliente, consigliamo fortemente di adottare analoghe politiche di backup e disaster recovery, adeguate a garantire l'integrità e la salvaguardia dei dati.

ACCESSO AL DATABASE

La suite CiviliaWeb non dispone di un accesso diretto sui DBMS e non mette a disposizione alcun metodo o tool per interrogare lo schema. Nel DBMS ogni schema ha una profilatura minima che consente di operare solo sui dati relativi all'applicazione.

ACCESSI TRAMITE VPN

Se l'Ente prevede o ha delle connessioni esterne VPN (si pensi a servizi dislocati sul territorio), la suite si presta a questo tipo di collegamento, criptato per definizione.

POLICY PASSWORD DI ACCESSO

Indipendentemente dal tipo di installazione (in ASP o presso i server del cliente) e dall'identity manager (IM) in uso, consigliamo fortemente l'adozione di policy per la gestione delle password applicative opportune a garantire un adeguato controllo degli accessi.
Con l'IM interno, il sistema Civilia WEB mette a disposizione la possibilità di attivare e configurare dei meccanismi per la gestione delle password (con scadenza automatica a 3 o 6 mesi). L'amministratore di sistema può resettare la password ma non può mai conoscerne il valore attuale.

Civilia Open

La suite Civilia Open è distribuita all'interno di una rete locale, con un'architettura a due livelli, DBMS, file server nel back end e una serie di librerie - Runtime – presente su ogni singola postazione dotata di un sistema operativo Microsoft.

DOMINIO ALL'INTERNO DELL'ENTE

Data la semplicità e la tipologia dell'architettura presente, il sistema consente un Identity Manager in gestione all'utente finale (tipicamente un Dominio Active Directory). L'ente può utilizzare le funzioni base di accesso con user-id e password definiti all'interno del database locale e gestiti in autonomia dall'ente stesso.

BLINDATURA DEI SISTEMI SERVER

La blindatura dei sistemi server è nella responsabilità del cliente (collocazione dei server in luoghi il più possibile sicuri, dotati di sorveglianza e/o di controllo degli accessi). L'accesso ai server ed ai servizi vitali (p.e. Identity Management) è permesso solo ad utenti con profilo *Administrator*.

CRITTOGRAFAZIONE DEI DISCHI

Non si tratta di una caratteristica intrinseca alla Suite Civilia Open. È possibile attivare e configurare tecnologie di crittografazione automatica (SED).

ACCESSO ALLE INFORMAZIONI

Le possibili tecniche di attacco possono essere molteplici. È necessario usare contemporaneamente diverse tecniche difensive per proteggere un sistema informatico/informativo (sicurezza attiva). Non si tratta di una caratteristica intrinseca alla Suite Civilia Open.

CONDIVISIONE DI RISORSE

L'autenticazione al dominio permette di controllare costantemente gli accessi. La mappatura delle risorse permette un profilo di rischio compatibile all'utilizzazione ed alla produzione del materiale (tipicamente documenti di stampa, report, merge) strettamente connesso e necessario allo svolgimento delle attività previste, seguendo il principio di privacy dettato dal GDPR. Viene garantita l'integrità e la confidenzialità dell'informazione.

AUDITING UTENTI CONNESSI AL DOMINIO

Con l'autenticazione di dominio si possono sfruttare tutte le potenzialità offerte dall'AUDITING di Active Directory (log di ogni evento in merito al collegamento su una postazione, sulle operazioni effettuate, sugli accessi alle cartelle fino alla granularità che si rendesse necessaria).
Ogni accesso al file system di rete viene controllato dalle policy di account e viene delegato/negato dall'amministratore di Dominio (o utente appartenente al gruppo Domain Admins)

ISOLAMENTO DELLE PERIFERICHE E CONTROLLO DEVICE

Come servizio eventualmente da attivare tramite policy di Active Directory viene reso disponibile il controllo e l'identificazione di strumentazione ritenuta non idonea alle necessità del singolo operatore, ovvero possono essere escluse strumentazioni di dubbia provenienza (USB generiche, HD esterni, Cd-Rom, etc) che potrebbero compromettere l'integrità del sistema informativo.

SISTEMA ANTIVIRUS (ANTI MALWARE)

L'adozione di strumentazioni di sicurezza atte a limitare i rischi e gli accessi o attacchi dall'esterno deve essere tenuta in debita considerazione. Gestione in carico al titolare del trattamento ove non diversamente indicato contrattualmente.

FIREWALL DI FRONTIERA

L'isolamento del back-end (database, storage) è passo fondamentale per preservare l'informazione come bene aziendale. Deve essere garantita la sicurezza da attacchi esterni e/o dolosi (extranet/internet) con adeguati sistemi di difesa perimetrali (firewall) senza precludere la fruizione di servizi/applicativi indispensabili all'operatività degli utenti. Gestione in carico al titolare del trattamento ove non diversamente indicato contrattualmente.

BACKUP E D&R

È possibile, con adeguati accorgimenti, effettuare un completo e consistente salvataggio del patrimonio informativo, attuando politiche di backup in grado di abbassare/ridurre notevolmente il rischio di perdita dei dati.
Gestione in carico al titolare del trattamento ove non diversamente indicato contrattualmente.

ACCESSO AL DATABASE

Nessun utente applicativo è a conoscenza delle credenziali dell'OWNER dello schema DBMS a meno degli amministratori dell'ente o loro subalterni e nessuno strumento viene fornito per un accesso alternativo.

ACCESSO AI DATI DALLE SINGOLE POSTAZIONI

Le informazioni prelevate utilizzando l'applicazione non possono essere trasportate in blocco sul Pc dell'utente (sub-set complessivo) ma con delle sub-query successive e poco strutturate attraverso l'utilizzo di "bind variables" non contestualizzabili puntualmente e quindi non associabili ad alcun soggetto.

ISOLAMENTO E CONTROLLO ACCESSI AL RDBM

Si possono considerare contributi all'abbassamento del rischio di intrusione, l'adozione di politiche di tracking degli accessi al Database Server, ovvero abilitare/disabilitare l'accesso solo alle postazioni di una particolare rete o sottorete attivando funzionalità di filtro messe a disposizione dal LISTENER (Oracle) o servizi simili. Questo vale per sistemi strutturati e complessi con una sottodivisione delle reti (tramite subnetting) spesso utilizzate in architetture dipartimentali. Per un utilizzo locale, la configurazione e l'utilizzo del filtro IP può essere un valido strumento di monitoraggio degli utenti NON abilitati all'operatività ed al censimento di postazioni utilizzate al di fuori delle concessioni previste dalle policy dell'ente.

AUDITING ACCESSO AI DATI (AUDITING DB)

È possibile attivare l'AUDITING per censire gli accessi generici (a livello di s.o.) e capillarmente memorizzare ogni accesso ai dati e la loro manipolazione (confidenzialità).
Gestione in carico al titolare del trattamento ove non diversamente indicato contrattualmente.

DBMS: MASKING DEI DATI

La funzionalità può essere attivata con package appositamente studiati per soddisfare particolari situazioni o richieste.

ACCESSO APPLICATIVO CIVILIA_OPEN

Ogni utente viene censito in base all'organigramma dell'Ente e viene associato a dei profili (dipartimenti/uffici/funzioni) che possono essere creati/mantenuti solo da un delegato amministratore (superuser) con un'interfaccia semplice e funzionale. L'utente applicativo può inoltre essere associato strettamente all'utente di Active Directory (o altro identity manager). È configurabile altresì la modalità single-sign-on (SSO) e bloccare la singola postazione dopo n. minuti di inattività.

CONTROLLO E LOG DEGLI ACCESSI

Ogni accesso alla suite CIVILIA_OPEN viene censito e memorizzato su database (tabelle dedicate).

Tutte le operazioni più delicate o importanti vengono sottoposte a LOGGING.

ACCESSI TRAMITE VPN

Se l'ente prevede o ha delle connessioni esterne VPN (si pensi a servizi dislocati sul territorio), la suite si presta a questo tipo di collegamento - criptato per definizione – Possono essere attivati meccanismo di "intrusion detection".

Front End Civilia (Servizi on line OpenWeb)

Un sistema Web dedicato ai servizi OnLine che normalmente viene erogato As A Service
ma che può essere installato ed erogato direttamente dall'Ente sui propri server.

Nel caso di fruizione *as a service* il fornitore garantisce il corretto funzionamento del servizio e gestisce tutto l'impianto di sicurezza.

FRONT END CIVILIA (Servizi on line OpenWeb) - EROGATO AS A SERVICE (SAAS)

COMPONENTI DEL SERVIZIO (database, application server, storage, servizi di infrastruttura)

- **perimetrico**: grazie a firewall di tipo datacenter che si preoccupano anche di monitorare ed analizzare il traffico per identificare e scongiurare minacce (IDS Intrusione detection System e IPS Intrusion Prevention System)
- **a livello di singole componenti**: grazie all'attivazione dei firewall interni
- **a livello di disegno complessivo**: tutte le componenti dialogano fra loro utilizzando una rete privata
- **a livello di disegno del singolo servizio**: viene esposto solo quanto necessario per l'erogazione del servizio

Tutti i servizi prevedono l'accesso con **protocollo HTTPS** (salvo diversa indicazione stabilita con l'ente per la navigazione anonima) per consentire la navigazione http in modalità crittografata. **Tutti i siti (principale e di disastro) sono su datacenter classificati Tier III, posizionati**, in ottemperanza a quanto stabilito dalla norma, **nel territorio europeo**.
Attualmente il sito principale per l'erogazione dei servizi online è all'interno del campus di Milano Caldera, il fiber hub più importante d'Italia.

GESTIONE DEI DATI

Tutti gli accessi ai sistemi ed agli applicativi sono protetti da password complesse e/o chiavi di criptazione.

Ogni Ente ha una porzione dedicata ad accesso esclusivo. **I dischi delle varie componenti del modulo Front End Civilia (Servizi on line OpenWeb) sono criptati** secondo lo standard AES-256 gestita, a basso livello, dal sistema di virtualizzazione.

BACKUP E DISASTER RECOVERY

I backup vengono eseguiti su diversi livelli:

- singole componenti (database server, application server, storage, servizi di infrastruttura)
- database

In entrambi i casi i backup vengono criptati secondo lo standard AES-256.
Il servizio di *disaster recovery* è assicurato mediante una replica su altro datacenter.

POLITICHE DI BACKUP

- Componenti (Macchine virtuali): backup incrementale
- Database: full backup cold
- RTO (recovery time objective): 8 h
- RPO (recovery point objective): 24 h
- Retention: 15 gg per i componenti; database 15 gg + 1 backup per ciascuna settimana

dell'ultimo mese, 1 copia mensile per 6 mesi.

DISASTER RECOVERY

In caso di Disastro vengono ripristinati i backup ed attivato il sito di DR (disaster recovery) come segue:

- RTO (recovery time objective): 24 h
- RPO (recovery point objective): 24 h
- Retention: 48 h

SERVIZI DI INFRASTRUTTURA

Trattandosi di servizi online, a volte è necessario consentire all'Ente un accesso alla propria sezione per consentire determinate operazioni quali ad esempio personalizzazioni o customizzazioni.
Anche in questo caso l'accesso non avviene in nessun modo alle componenti di produzione, ma in un ambiente protetto:

- su macchine dedicate e con servizi preservati
- creando un ecosistema virtuale per ciascun accesso in modo da impedire il libero accesso alla macchina
- creando un accesso alla singola parte necessaria dell'installazione dell'ente.

FRONT END CIVILIA (Servizi on line OpenWeb) – EROGATO DIRETTAMENTE DALL'ENTE

Il sistema è scalabile, può essere configurato in modi diversi e si adatta alle varie tipologie di infrastruttura presenti presso l'Ente.
Si tratta di servizi esposti alla cittadinanza su Internet ed è pertanto necessario utilizzare tutti i possibili accorgimenti di sicurezza previsti dalla normativa vigente.

CARATTERISTICHE DEL GDPR CHE IL SISTEMA FRONT END CIVILIA (SERVIZI ON LINE OPENWEB) SODDISFA *BY DESIGN*

- connessioni sicure al server ovvero adozione ed attivazione di certificati SSL
- facilità di una blindatura dell'hardware (in carico al conduttore)
- crittografie dei dischi
- uso corretto delle password e degli screen locker
- isolamento delle periferiche di interfaccia (usb, cdrom, ecc)
- blindatura dei sistemi server
- eliminazione di qualunque strumento di accesso diretto ai dati consentendo solo l'accesso tramite applicazione conosciuta
- politica di backup accurata e conservazione protetta delle copie
- posizionamento del server in DMZ
- sistema antivirus accurato
- server isolati con apposito sistema di firewall
- esecuzione di test periodici di intrusion detection avvalendosi di servizi offerti da ditte specializzate
- verifica dell'aggiornamento del sistema operativo soprattutto per le patch di sicurezza

FRONT END CIVILIA (Servizi on line OpenWeb) – SICUREZZA APPLICATIVA

Distinguiamo di seguito 3 tipologie di accesso:

- Accesso dedicato agli operatori dell'ente
- Accesso in cooperazione applicativa
- Accesso dedicato ai cittadini ed alle imprese

Tutte le tipologie di accesso avvengono su protocollo HTTPS.

ACCESSO DEDICATO AGLI OPERATORI DELL'ENTE

Tutti gli accessi vengono rilevati e dettagliati in un apposito file log, dove viene tracciato oltre al giorno e l'ora dell'accesso anche l'IP dal quale viene eseguito l'accesso stesso.
Esistono poi ulteriori e diversi profili di accesso al sistema:

- utente amministratore: è l'unico accesso che può visualizzare in chiaro le informazioni relative ai cittadini, inclusi i dati personali forniti dall'utente stesso in fase di primo accesso al sistema (registrazione e/o accesso mediante SPID o sistema terzo).
- amministratori di servizio / operatori: hanno accesso solo ed esclusivamente alle proprie funzioni senza poter accedere alla consultazione dei dati personali dei cittadini censiti nel sistema

La profilazione di questo tipo di utenti (amministratori e amministratori di servizio) è minima, non èprevista una raccolta di informazioni personali degli operatori, e sono impostate le regole di cambiamento della password come previsto dalle normative in essere.

ACCESSO IN COOPERAZIONE APPLICATIVA

I servizi erogati nel portale spesso devono interagire con i sistemi dell'ente in modalità appunto di cooperazione applicativa. Tutti i webservice esposti dal sistema gestiscono il livello di autenticazioneche tuttavia può variare a seconda del servizio e dalla relativa tecnologia.

ACCESSO DEDICATO AI CITTADINI ED ALLE IMPRESE

L'accesso all'area riservata avviene mediante protocollo HTTPS.
Il sistema ha un suo repository utenti, ma può interagire con sistemi terzi certificati come ad esempio SPID (Sistema Pubblico Identità Digitale).

GESTIONE INFORMATIVE E CONSENSI

Tutti i servizi esposti al cittadino consentono all'Ente di erogare in modalità web – online i propri servizi istituzionali.
Vengono richieste al cittadino anche ulteriori informazioni quali email e/o SMS che vengono poi utilizzati per facilitare l'erogazione dei servizi mediante invio di apposite comunicazioni o notifiche automatiche.

INFORMATIVA

Come stabilito dal Regolamento sono previste apposite informative nella sezione denominata "Portale del Cittadino" (personalizzabili da ciascun Ente).

CONSENSO

Per tutti gli utenti di portale (cittadini, imprese, etc.), all'atto del primo accesso, qualunque sia il sistema di autenticazione adottato, viene richiesto di autorizzare il trattamento dei dati descrivendone gli aspetti tecnici ed operativi legati alla soluzione.

RICHIESTA CANCELLAZIONE DATI

È prevista apposita funzione attraverso la quale il cittadino potrà richiedere la cancellazione dei propri dati. La richiesta viene tracciata nel sistema ed inviata al Responsabile del Trattamento dei dati dell'Ente. Sempre attraverso apposita funzione è possibile procedere con la cancellazione come richiesto. Le informazioni che verranno cancellate sono il profilo dell'utente con tutte le informazioni di contatto.

RETTIFICA DATI

Per quanto concerne la rettifica dei propri dati personali, il cittadino può procedere in autonomia modificando quanto precedentemente dichiarato.

PSEUDONIMIZZAZIONE DEI DATI

Il sistema, nativamente, prevede la separazione fra le informazioni necessarie all'accesso, i dati anagrafici e personali degli individui e le informazioni poi generate nei singoli ambiti applicativi.
L'accesso alla sezione dove sono visibili le informazioni degli individui è consentito solo all'amministratore.
Nelle altre sezioni sono presenti solo le informazioni specifiche ed un riferimento al solo nome e cognome senza ulteriori informazioni e quindi di fatto senza poter risalire con certezza alla persona.

ACCERTAMENTO DI EVENTUALI VIOLAZIONI

Svariati livelli di log consentono di rilevare eventuali violazioni di una delle componenti del sistema.In caso di questo tipo di incidente sarà nostra cura:

- determinare il punto di ingresso
- determinare le informazioni a cui può essere stato effettuato l'accesso

Verranno poi immediatamente adottate le misure del caso:

- attuando tutte le azioni necessarie per rimuovere l'eventuale problema di sicurezza

segnalando al Titolare nei termini e nei modi previsti dal GDPR l'illecito (art. 33 comma 2 del GDPR)