Dichiarazione sulle misure di sicurezza applicate

Servizi basati su CMS ISWEB – Linea ePORTAL e servizi al riuso PAT

Ultimo aggiornamento 09/09/2020

www.isweb.it

ISWEB S.p.A.
Via Cadorna 31 - 67051 Avezzano (AQ)
Via Fiume Giallo 3 - 00144 Roma

ISO 9001-2015 - RINA
Sistema di gestione della qualità certificato RINA
Certificato n° 14770/06/S

Numero Verde Gratuito
800 97 34 34

Indice

Premessa

Nell'erogazione dei propri servizi, ISWEB si impegna ad osservare le misure di sicurezza che seguono, anche ai sensi della Circolare AGID 18 aprile 2017, n. 2/2017, in quanto applicabili e indicate nel presente documento.

Sicurezza delle piattaforme software

Sviluppo

Tutti i servizi relativi al presente documento sono basati o richiedono la piattaforma CMS ISWEB per la propria esecuzione.
ISWEB sviluppa le proprie piattaforme con approccio security control.

Patch management

Le patch di sicurezza vengono rilasciate non appena disponibile il bugfix realizzato a seguito dell'eventuale scoperta di una vulnerabilità.
Le patch che non incidono sulla sicurezza vengono rilasciate secondo la calendarizzazione del reparto tecnico.

Sicurezza dell'accesso alle piattaforme software da parte di personale ISWEB

Tracciamento degli accessi utente e utenze

ISWEB individua specificamente i propri utenti e le relative utenze abilitate agli accessi alle piattaforme che trattano dati personali dei clienti in funzione degli specifici privilegi di accesso.
In particolare, sono individuati nominativamente gli amministratori di sistema, ai quali sono impartite specifiche istruzioni sul rispetto delle misure di sicurezza dirette a preservare confidenzialità, integrità e attendibilità dei dati ai quali hanno accesso.
Gli accessi sono configurati a livello applicativo in modo che gli utenti non possano alterare i log.

Formazione degli utenti

Gli utenti ricevono adeguata formazione in materia di sicurezza informatica e rispetto delle prescrizioni di cui alla normativa sulla protezione dei dati personali

Continuità operativa e disaster recovery

Ripristino attività a seguito di criticità della piattaforma

ISWEB utilizza i servizi di facility management di primari data-center italiani che prevedono politiche di backup e continuità operativa in grado di ripristinare la disponibilità dei dati e dei servizi entro 48 ore dalla criticità, salvi eventi di gravità tale da non consentire il rispetto del termine suindicato.

Ripristino attività a seguito di criticità dell'infrastruttura

Benché ISWEB si impegni al rispetto dei termini di cui al precedente paragrafo, in caso di criticità relativa all'infrastruttura di facility management i tempi di ripresa dell'erogazione dei servizi dipenderanno da quelli impiegati dal data-center per ritornare all'operatività.

Si precisa che soluzioni dedicate di DR sono disponibili su progetto.

Misure anti-intrusione

L'infrastruttura di facility management prevede la presenza di firewall e antivirus perimetrali.

Allegato 1 – Misure minime di sicurezza ICT-PA

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Tutte le risorse attive sono censite all'interno dei repository del reparto tecnico ISWEB sia con modalità manuali sia con modalità automatiche garantite dagli apparati di rete
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Tutte le risorse attive sono censite all'interno dei repository del reparto tecnico ISWEB sia con modalità manuali sia con modalità automatiche garantite dagli apparati di rete
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	Il server DHCP effettua il log di ogni operazione all'interno della rete aziendale.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	I repository dei dispositivi sono aggiornati automaticamente ad ogni modifica
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Gli apparati di rete utilizzano modalità automatiche per il censimento dei dispositivi
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Gli apparati di rete che censiscono i dispositivi, memorizzano anche l'indirizzo IP sia nel caso di assegnazione dinamica sia nel caso di assegnazione statica.
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	L'inventario dei dispositivi è sempre formato da queste informazioni

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server,	Il reparto tecnico ISWEB mantiene un elenco dei software utilizzabili da ogni dispositivo

				workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	I sistemi sono monitorati automaticamente dai sistemi protezione software utilizzati e dal sistema operative stesso

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Tutti I dispositivi utilizzati applicano le configurazioni di sicurezza standard
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Tutti I dispositivi utilizzati applicano le configurazioni di sicurezza standard
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Nel caso di verifica di compromissione di un sistema o di un dispositivo, si procede con un completo ripristino e con l'applicazione delle configurazioni standard
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Tutte le immagini di installazione utilizzate sono disponibili anche offline in repository locali o su supporti fisici
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	Tutte le operazioni che richiedono una gestione remota, sono sempre eseguite tramite canali sicuri come SSH, SFTP e HTTPS
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	Sono attivi servizi di monitoraggio continuo
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	I servizi di monitoraggio producono alert e log
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del	Tutti I dispositivi utilizzano la verifica della firma digitale dei software

				sistema, delle variazioni dei permessi di file e cartelle.	tramite le funzionalità garantite dai produttori dei sistemi operativi utilizzati. Anche I software antivirus e firewall utilizzati nelle configurazioni standard effettuano un monitoraggio di questo tipo.

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	Le verifiche vengono svolte attraverso strumenti automatici di verifica ad ogni nuova release
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	Tutte le attività di verifica vengono svolte dal solo personale autorizzato e con strumenti validati ed autorizzati.
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	I software utilizzati per le verifiche vengono continuamente aggiornati con modalità sia automatiche che manuali quando necessario.
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per	I software utilizzati per le verifiche vengono continuamente aggiornati con modalità sia automatiche che manuali quando necessario.

				aggiornare le attività di scansione	
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Tutte le postazioni utilizzano le procedure di aggiornamento automatiche previste dal sistema operativo utilizzato. Per le componenti applicative del servizio, le modalità di aggiornamento possono variare in funzione dell'applicazione stessa.
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Non sono utilizzati sistemi separate dalla rete.
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	Tutte le eventuali vulnerabilità software vengono verificate all'interno dei cicli di sviluppo del software e nelle attività di verifica interne
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	La documentazione è consultabile dietro richiesta
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	Tutte le operazioni di patching e di upgrade dei software sono sempre associate alle eventuali vulnerabilità rilevate o alla segnalazione di bug.
4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono	Nel caso di vulnerabilità non risolvibili in tempi brevi, vengono sempre applicate misure temporanee per la mitigazione della stessa fino alla risoluzione effettiva

				immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	Tutti I cicli di sviluppo software e le relative verifiche vengono effettuate in ambienti di collaudo

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	Le utenze di amministrazione del servizio sono in disponibilità esclusiva al reparto tecnico ISWEB ed ai referenti individuati dal committente
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Tutti gli accessi utente, sia quelli tentati che quelli riusciti, vengono registrati nel log delle attività dell'applicazione e nei log di servizio
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	L'ambiente applicativo utilizza un Sistema ACL modulare per l'assegnazione dei permessi all'utente. I profili di permessi vengono identificati sulla base delle necessità operative indicate dal committente.
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Tutte le operazioni amministrative effettuate vengono registrate nel log delle attività dell'applicazione
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	L'ambiente applicativo dispone di una comoda funzionalità dedicate alla gestione delle utenze amministrative, disponibile per gli operatori individuati dal committente.
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	Tutti i dispositivi vengono configurati in fase iniziale secondo gli utilizzi
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Tutte le operazioni amministrative effettuate vengono registrate nel log delle attività dell'applicazione

5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Tutti gli accessi utente, sia quelli tentati che quelli riusciti, vengono registrati nel log delle attività dell'applicazione
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	L'autenticazione a due fattori è attualmente in fase finale di sviluppo su tutti i servizi basati su CMS ISWEB.
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	L'autenticazione a due fattori è attualmente in fase di sviluppo su tutti i servizi basati su CMS ISWEB, fino al rilascio la password policy prevede almeno 14 caratteri di lunghezza
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	La password policy prevede un minimo di 14 caratteri, con la conformità ad almeno 4 delle seguenti regole: almeno una lettera maiuscola; almeno una lettera minuscola; almeno un numero; almeno 1 carattere speciale tra i seguenti: @_|#!?; non più di 2 caratteri uguali consecutivi
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	La piattaforma richiede alle utenze un cambio password periodico (configurabile su richiesta)
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	L'ambiente applicativo controlla che ogni nuova password impostata non sia uguale alle ultime utilizzate dall'utente
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	L'ambiente applicativo utilizza un Sistema ACL estremamente modulare per l'assegnazione dei permessi all'utente. Gli account sono sempre indipendenti sulla base dei relativi ACL. Tutti gli aspetti relativi a questo ambito sono quindi gestibili direttamente dal committente.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Questo aspetto è gestito direttamente dal committente.
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative	Gli accessi amministrativi a livello servizio vengono utilizzati esclusivamente quando strettamente necessario al tipo di operazioni e sono

				credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	disponibili esclusivamente per gli operatori ISWEB abilitati.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Gli algoritmi utilizzati per la crittografia della password sono rispettivamente: - Bcrypt per la generazione della password concatenata con altri dati; - Openssl con metodo AES-256-CBC ed hash sha256 per la chiavi univoca del singolo utente. Funzionamento: L'algoritmo di generazione della password crittografata avviene nel seguente modo: Passo 1: generazione di una chiave univoca per ogni singolo utente; Passo 2: concatenamento della password utente più la chiave interna "ISWEB_KEY"; Passo 3: creazione e criptazione delle chiavi univoca per ogni utente, casella e-mail e password; Passo 4: generazione dell'Hash della password con il concatenamento descritto nel passo 3.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non vengono utilizzati certificati digitali

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	Tutte le postazioni utilizzate dispongono di software antivirus aggiornati automaticamente.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Tutte le postazioni utilizzate dispongono di software Firewall ed IPS aggiornati automaticamente con il sistema operativo. Sono anche presenti sistemi firewall hardware nella rete.

8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Gli operatori ISWEB utilizzano esclusivamente dispositivi autorizzati.
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	Tutte le postazioni ed i dispositivi consentiti sono configurati con funzionalità DEP e di controllo dell'account.
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	Le funzionalità sono incluse negli strumenti software antivirus e firewall utilizzati. In termini infrastrutturali, sono garantite dagli apparati e le policy infrastrutturali.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Le funzioni sono disabilitate di default nei software utilizzati
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Le funzioni sono disabilitate di default nei software utilizzati
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Le funzioni sono disabilitate nei servizi utilizzati
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Le funzioni sono disabilitate di default nei software utilizzati
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Le funzionalità sono incluse negli strumenti software antivirus e firewall utilizzati da ogni postazione.
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	Le funzioni sono incluse nei servizi utilizzati
8	9	2	M	Filtrare il contenuto del traffico web.	Le funzionalità sono incluse negli strumenti software antivirus e firewall utilizzati
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	Le funzioni sono incluse nei servizi utilizzati e negli strumenti software antivirus e firewall utilizzati da ogni postazione
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Le funzionalità sono incluse negli strumenti software antivirus e firewall utilizzati

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID	Livello	Descrizione	Modalità di implementazione

10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Le funzionalità sono incluse nelle policy di business continuity. Inoltre le funzionalità di DR sono attivabili in modalità dedicata sul singolo progetto
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	Le funzionalità sono incluse nelle policy di business continuity e delle piattaforme di backup in utilizzo (TSM).
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	I dati relative ai backup non sono mai disponibili su servizi normalmente esposti

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	In generale, lo scopo principali dei servizi in questo ambito è la pubblicazione per obblighi normativi (es: 33/2013) di informazioni di stampo pubblico. Nel caso di servizi o basi di dati con particolari necessità di riservatezza, sono disponibili su progetto funzionalità aggiuntive di protezione (es: crittografia, pseudonimizzazione).
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Le funzionalità sono garantite dagli apparati firewall e dai software antivirus in utilizzo

Contatti

ISWEB S.p.A.

Azienda certificata UNI EN ISO 9001:2015 - RINA
"Progettazione e sviluppo applicativi software per ambienti di rete"

Sede legale e factory:
Via Cadorna, n.31 - 67051 - Avezzano (AQ)
Unità locale (commerciale):
via Fiume Giallo, 3 - 00144 - Roma

NUMERO VERDE
800.97.34.34

Tel. +39.0863.441163
Fax. +39.0863.444757

e-mail: info@isweb.it
pec: pec@pec.isweb.it
Sito web: http://www.isweb.it

Registro delle Imprese del Gran Sasso d'Italia
P.IVA, C.F. e numero d'iscrizione: 01722270665

Elenco firmatari

ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI

Questo documento è stato firmato da:

NOME: VISINTIN ROBERTO
CODICE FISCALE: VSNRRT69E24Z133P
DATA FIRMA: 13/06/2022 12:27:15
IMPRONTA: 11C6154EC9B4B6C7FA5DC90481293AD47ADE758D00DD08D999A0E40DFF13A3E1
7ADE758D00DD08D999A0E40DFF13A3E11CAAE4250CFC3AEF34540356A2C19B25
1CAAE4250CFC3AEF34540356A2C19B25DA1662E0C2A8C1FF148656292B63968A
DA1662E0C2A8C1FF148656292B63968AB092F8BD6D20DE844BB7B2765749AA97