

Dichiarazione sulle misure di sicurezza applicate Servizi ambito Whistleblowing

Ultimo aggiornamento 27/10/2023



Indice

Premessa	3
Sicurezza delle piattaforme software	4
Sviluppo.....	4
Verifiche periodiche di vulnerabilità.....	4
Patch management	4
Sicurezza dell'accesso alle piattaforme software da parte di personale ISWEB	5
Tracciamento degli accessi utente e utenze.....	5
Formazione degli utenti.....	5
Continuità operativa e disaster recovery	5
Ripristino attività a seguito di criticità della piattaforma	5
Ripristino attività a seguito di criticità dell'infrastruttura	5
Misure anti-intrusione.....	5
Altre Misure di sicurezza	6
Allegato 1 – Misure minime di sicurezza ICT-PA	7
ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI.....	7
ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI	7
ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	8
ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ.....	9
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE.....	11
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE.....	13
ABSC 10 (CSC 10): COPIE DI SICUREZZA	14
ABSC 13 (CSC 13): PROTEZIONE DEI DATI	15
Contatti.....	16

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. Si precisa inoltre che nell'ambito del servizio Whistleblowing, le misure di sicurezza organizzative e tecniche applicate sono conformi all'attuale D. Lgs. n. 24/2023 e relative linee guida.

Sicurezza delle piattaforme software

Sviluppo

Il servizio Whistleblowing, è basato sul software opensource Globaleaks (<https://github.com/globaleaks/GlobaLeaks>), sviluppato secondo le linee guida OWASP per lo sviluppo di applicazioni sicure.

Per ogni approfondimento tecnico, è disponibile un'ampia documentazione sui principi di architettura e di security applicativa utilizzati per lo sviluppo del software, all'interno della documentazione di piattaforma disponibile all'indirizzo <https://docs.globaleaks.org/en/main/>

Verifiche periodiche di vulnerabilità

Il codice della piattaforma Globaleaks è periodicamente verificato dalla stessa community nel corso del ciclo di sviluppo, e dal reparto tecnico ISWEB all'interno delle procedure di upgrade dei servizi offerti.

Il repository della piattaforma rende disponibili anche la documentazione relativa a test di vulnerabilità svolti periodicamente e realizzati da organismi indipendenti.

Patch management

Le patch di sicurezza vengono applicate con tempestività sulla base dei rilasci ufficiali nel repository di piattaforma.

Le patch che non incidono sulla sicurezza vengono rilasciate secondo la calendarizzazione del reparto tecnico, con cadenza comunque mai superiore ad un semestre.

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.

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 24 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.

Altre Misure di sicurezza

- ✓ Infrastruttura tecnologica di tipo VPC - Virtual Private Cloud;
- ✓ Alta capacità di elaborazione garantita da processori fisici Intel Xeon Silver;
- ✓ Storage Area Network (SAN) in fiber channel completamente ridondata;
- ✓ Sistemi avanzati di monitoraggio proattivo per le metriche di servizio;
- ✓ Firewall perimetrale con possibilità di gestione geografica dei pacchetti;
- ✓ Supporto per l'esposizione del servizio tramite rete TOR oppure tramite normale TLS;
- ✓ Autenticazione 2FA nativa basata su RFC 6238 con chiave segreta a 160 bits;
- ✓ Sistemi di Proof of Work per login e file submission;
- ✓ Disponibilità di funzionalità di Slowdown per i tentativi di login falliti;
- ✓ Gestione delle policy per la corretta gestione di Strict-Transport, Content-Security, Cross-Origin-Embedder, Cross-Origin-Resource, Cache-Control;
- ✓ Application sandboxing: AppArmor by default per una esecuzione sicura dell'applicazione;
- ✓ Network sandboxing: layer dedicato di firewall software integrato con iptables;
- ✓ Implementazione logiche applicative di DoS Resiliency;
- ✓ Crittografia applicativa dei dati con chiavi a 256 bit ed utilizzo di:
 - Crittografia asimmetrica: Libsodium SealedBoxes (Curve25519, XSalsa20, Poly1305);
 - Crittografia simmetrica: Libsodium SecretBoxes (XSalsa20, Poly1305);
- ✓ - Sistema di eliminazione sicura dei dati.

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 dispone di 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 in utilizzo

				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 operativo 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 della configurazione standard iniziale
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Tutte le immagini di installazione utilizzate sono sempre 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 sistema, delle variazioni dei permessi di file e cartelle.	Tutti i dispositivi utilizzano la verifica della firma digitale dei software 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 sia come procedura stessa del ciclo di sviluppo dell'applicativo Globaleaks, sia periodicamente dal nostro reparto tecnico con cadenza al massimo annuale. La piattaforma è inoltre periodicamente verificata anche da organismi indipendenti con periodicità stabilita dagli sviluppatori.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Le verifiche vengono svolte sia come procedura stessa del ciclo di sviluppo dell'applicativo Globaleaks, sia periodicamente dal nostro reparto tecnico con cadenza al massimo annuale. La piattaforma è inoltre periodicamente verificata anche da organismi indipendenti con periodicità stabilita dagli sviluppatori.
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.	I software utilizzati per le verifiche vengono continuamente aggiornati con modalità sia automatiche che manuali quando necessario.

				Utilizzandole per aggiornare le attività di scansione	
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	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.).	Il piano di gestione dei rischi, ed in generale lo scenario e la matrice degli utilizzatori sono stati definiti durante il design del software e vengono aggiornati sulla base di ogni modifica allo scenario (https://docs.globaleaks.org/en/main/security/index.html)
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 alternative 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 cili di sviluppo software e le relative verifiche vengono effettuate in ambienti di collaudo separati da quelli di produzione

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, anche quelli non riusciti, vengono registrati nel log delle attività dell'applicazione e nei log di servizio. Si specifica che gli accessi amministrativi utilizzati dagli operatori ISWEB, non consentono la visualizzazione o gestione dei dati delle segnalazioni Whistleblowing, ma solo gli aspetti di configurazione dell'ambiente, utilizzati per la predisposizione dei requisiti funzionali richiesti dal committente.
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. Si specifica che gli accessi amministrativi utilizzati dagli operatori ISWEB, non consentono la visualizzazione o gestione dei dati delle segnalazioni Whistleblowing, ma solo gli aspetti di configurazione dell'ambiente, utilizzati per la predisposizione dei requisiti funzionali richiesti 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, che si

					occupa anche di registrare eventuali eccezioni o anomalie delle funzioni disponibili.
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 funzione dedicata alla gestione delle utenze amministrative.
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 supportata ed attivabile sul servizio Whistleblowing dietro richiesta da parte del committente.
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 supportata ed attivabile sul servizio Whistleblowing. La piattaforma supporta inoltre ulteriori regole per la costruzione di password robuste.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Le password vengono valutate in tre livelli: forte, accettabile, inutilizzabile. Una password forte deve essere formata da lettere maiuscole, lettere minuscole, numeri e simboli, essere lunga almeno 12 caratteri e includere una varietà di almeno 10 input diversi. Una password accettabile dovrebbe essere formata da almeno 3 input diversi su lettere maiuscole, lettere minuscole, numeri e simboli, contenere almeno 10 caratteri e includere una varietà di almeno 7 input diversi.
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	L'ambiente applicativo controlla che

				possano essere riutilizzate a breve distanza di tempo (password history).	ogni nuova password impostata non sia uguale a quella già utilizzata 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.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Questo aspetto è gestito dal committente, tramite l'individuazione dei propri operatori e dei relativi account.
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	Gli accessi amministrativi a livello servizio vengono utilizzati esclusivamente quando strettamente necessario al tipo di operazioni. Le utenze di questo tipo sono assegnate esclusivamente agli AdS assegnati al relativo servizio.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le password non sono mai memorizzate in chiaro sul sistema, ma vengono memorizzate con un hash costruito da un salt randomico a 128bit e l'algoritmo Argon2
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Nel caso di utilizzo di chiave private come nel caso di attivazione di PGP, il mantenimento di queste è in carico agli AdS individuati dal committente in quanto il reparto tecnico di ISWEB non ha accesso ai dati inerenti il servizio.

ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	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 rimovibili al momento della loro connessione.	Le funzionalità sono incluse negli strumenti software antivirus e firewall utilizzati da ogni postazione utilizzata
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	Le funzionalità sono incluse nelle policy di business continuity. Inoltre

				informazioni strettamente necessarie per il completo ripristino del sistema.	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 informazioni riservate contenute dal servizio sono crittografate nativamente dall'ambiente applicativo.
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 relativi 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	Nell'ambito del servizio Whistleblowing, l'analisi è stata effettuata già a monte del software design (https://docs.globaleaks.org/en/main/security/index.html)
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 utilizzati.

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 Tiburtina Valeria Km. 112,500 - 67068 - Cappelle dei Marsi (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 di L'Aquila

P.IVA, C.F. e numero d'iscrizione: 01722270665