VALUTAZIONE DI IMPATTO

CANALE DI SEGNALAZIONE - D.LGS. 24/2023 – WHISTLEBLOWING

VALUTAZIONE DI IMPATTO

AI SENSI DELL'ART. 35 REG. EU 679/2016

Azienda Unità Sanitaria Locale Umbria 1
tel. 075 54 11 - 075 85 091
Sede Legale
06127 - Perugia Via Guerra 21/17
(l.r. n.18/12.11.2012)
p.iva / c.f. 03301860544

Sommario

Azienda Unità Sanitaria Locale Umbria 1
tel. 075 54 11 - 075 85 091
Sede Legale
06127 - Perugia Via Guerra 21/17
(l.r. n.18/12.11.2012)
p.iva / c.f. 03301860544

Azienda Unità Sanitaria Locale Umbria 1
tel. 075 54 11 - 075 85 091
Sede Legale
06127 - Perugia Via Guerra 21/17
(l.r. n.18/12.11.2012)
p.iva / c.f. 03301860544

Team

- **Maria Gabriella Stortoni**, Responsabile IFO "Supporto funzioni istituzionali, adempimenti in materia di Privacy e Trasparenza amministrativa" nell'ambito della UOC "Affari Generali, Istituzionali e Gestione Legale dei Sinistri" - Compilazione

- **Alessandro Frillici**, Responsabile della Protezione dei Dati (DPO) – Valutazione

- **Enrico Martelli**, Direttore Amministrativo- Approvazione

Valutazioni

- Il RPD/DPO ha espresso valutazione favorevole alla implementazione con le seguenti motivazioni: *"Vista la valutazione di impatto che appare idonea, considerate le risultanze che forniscono un livello di rischio adeguato, nulla appare essere ostativo al trattamento. valutati inoltre i livelli di rischio residuo non si ritiene necessaria la consultazione preventiva ex art. 36 GDPR*" .

- Non è stato chiesto il parere degli interessati per le seguenti ragioni: *"considerati gli scopi e le modalità di trattamento, considerato altresì che si procede secondo finalità istituzionali, non è apparso necessario richiedere preventivamente il parere degli interessati che, comunque potranno far pervenire i loro feedback".*

Azienda Unità Sanitaria Locale Umbria 1
tel. 075 54 11 - 075 85 091
Sede Legale
06127 - Perugia Via Guerra 21/17
(l.r. n.18/12.11.2012)
p.iva / c.f. 03301860544

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Si tratta del canale interno di segnalazione degli illeciti denominato "Whistleblowing", al fine di permettere agli aventi diritto di effettuare le segnalazioni, nel rispetto della vigente normativa applicabile nazionale ed europea, nel contesto della Azienda USL Umbria 1.

Quali sono le responsabilità connesse al trattamento?

Titolare del trattamento è l'Azienda USL Umbria 1 che si avvale, quale canale di segnalazione telematico, della piattaforma online "whistleblowing.it" messa a disposizione da "Whistleblowing Solutions Impresa Sociale S.r.l." quale responsabile del trattamento.

Ci sono standard applicabili al trattamento?

Il trattamento è attualmente disciplinato dal D.lgs 24/2023 e dalle Linee Guida ANAC del 12/7/2023.

Valutazione : Accettabile
Commento di valutazione :le informazioni appaiono corrette e coerenti.

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Il segnalante può agire in forma anonima, ove registrato sono raccolti i dati identificativi, dati di contatto e dati inerenti alla specifica segnalazione. Possono essere presenti i dati identificativi, di contatto di segnalati, facilitatori, altri soggetti coinvolti a diverso titolo dalla segnalazione. Tali dati sono conservati per il periodo necessario a dare seguito alla segnalazione e quindi conservati per dieci anni a decorrere dalla chiusura della segnalazione al fine di tutelare possibili interessi dell'Ente o di terzi, salvo proroghe o sospensioni come per legge.

Alle informazioni accede la "Responsabile della Prevenzione della Corruzione - RPC" e gli

Azienda Unità Sanitaria Locale Umbria 1
tel. 075 54 11 - 075 85 091
Sede Legale
06127 - Perugia Via Guerra 21/17
(l.r. n.18/12.11.2012)
p.iva / c.f. 03301860544

eventuali altri soggetti dell'Ente che devono essere coinvolti per il seguito della segnalazione debitamente autorizzati o nominati.

I dati potrebbero essere comunicati ad Autorità Giudiziarie ove strettamente necessario. Possono infine accedere ai dati i manutentori della piattaforma e gli amministratori di sistema dipendenti di Whistleblowing Solutions Impresa Sociale S.r.l. (Responsabile del trattamento).

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Il processo si divide nelle seguenti fasi:

1) Compilazione della segnalazione
questa fase si avvia accedendo al link disponibile nel sito internet dell'Ente. Attraverso questo link il segnalante viene trasferito attraverso un collegamento sicuro al sito internet del gestore della piattaforma. Attraverso un modulo strutturato il segnalante è guidato nella immissione delle informazioni inerenti alla segnalazione. Al completamento premendo il pulsante invio, la segnalazione è inoltrata alla piattaforma ed al segnalante è restituito un codice identificativo univoco attraverso il quale può seguirne l'esito.

2) Gestione della segnalazione
La RPC riceve comunicazione della avvenuta segnalazione ed attraverso un processo di strong authentication può accedere alla piattaforma nel pannello dedicato. La RPC valutata la segnalazione ne cura il seguito coinvolgendo, ove del caso, gli eventuali uffici interessati. Attraverso la piattaforma è possibile dialogare in modo anonimo con il segnalante salvo che lo stesso accetti di far conoscere la propria identità. Attraverso la piattaforma è possibile "chiudere" la segnalazione.

3) Archiviazione
Nella piattaforma restano conservate le informazioni e gli eventuali documenti caricati a supporto della segnalazione. L'archivio può essere consultato dalla RPC. Al termine del trattamento i dati sono cancellati in modo definitivo. In caso di necessità i dati possono essere esportati in formati comuni.

Quali sono le risorse di supporto ai dati?

L’architettura di sistema è principalmente composta da:

- Un cluster di due firewall perimetrali;
- Un cluster di due server fisici dedicati;
- Una Storage Area Network pienamente ridondata.

La piattaforma informatica di segnalazione è basata sul software libero ed open-source GlobaLeaks di cui Whistleblowing Solutions è co-autore e coordinatore di progetto. In aggiunta a GlobaLeaks, utilizzato in via principale per l’implementazione del servizio, per finalità di pubblicazione, documentazione e supporto del progetto vengono utilizzate altre tecnologie a codice aperto e di pubblico dominio la cui qualità è indipendentemente verificabile. Vengono anche in modo limitato utilizzate alcune note tecnologie proprietarie e licenziate necessarie per finalità di gestione infrastrutturale e backup professionale.

Azienda Unità Sanitaria Locale Umbria 1
tel. 075 54 11 - 075 85 091
Sede Legale
06127 - Perugia Via Guerra 21/17
(l.r. n.18/12.11.2012)
p.iva / c.f. 03301860544

Vengono primariamente utilizzati le tecnologie open source:

● Debian/Linux (principale sistema operativo utilizzato);
● Postfix (mail server);
● Bind9 (dns server);
● OPNSense (firewall);
● OpenVPN (vpn).
Le limitate componenti software di natura proprietaria impiegate sono le seguenti:
● VMware, software di virtualizzazione;
● Veeam, software di backup;
● Plesk, software per realizzazione siti web di facciata del progetto. Predisposizione dei sistemi virtualizzati:
● I server eseguono software VMware e vCenter abilitando funzionalità di High Availability;
● Su VMware vengono istanziate macchine virtuali Debian/Linux nelle sole version Long Term Support (LTS);
● Ogni macchina virtuale Debian implementa configurazione securizzata con: Full Disk Encryption (lvm/crypto), SecureBoot, Apparmor, Iptables;
● Entrambi i server fisici eseguono una macchina virtuale di Key Management System (KMS) per consentire continuità di servizio con immediato automatico riavvio dei sistemi senza intervento amministrativo anche in caso di totale fallimento di uno dei due server fisici componenti il cluster.

L'architettura di rete prevede:
● un firewall perimetrale e segregazione della rete in molteplici VLAN al fine di isolare le differenti componenti secondo loro differente natura al fine di limitare ogni esposizione in caso di vulnerabilità su una singola componente;
● Una VPN consente l'accesso alla gestione dell'infrastruttura a un limitato e definito insieme di amministratori di sistema;
● Ogni connessione di rete implementa TLS 1.2+;
● Ogni macchina virtuale istanziata vede esposizione di rete limitata all'effettiva necessità;
● Tutti i dispositivi utilizzati quali l'applicativo GlobaLeaks, Log di sistema e Firewall sono configurati per non registrare alcun tipo di log e/o informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP e User Agents;
● L'applicativo GlobaLeaks abilita la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.

Valutazione : Accettabile
Commento di valutazione : Le misure adottate appaiono coerenti ed adeguate

Azienda Unità Sanitaria Locale Umbria 1
tel. 075 54 11 - 075 85 091
Sede Legale
06127 - Perugia Via Guerra 21/17
(l.r. n.18/12.11.2012)
p.iva / c.f. 03301860544

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento è finalizzato principalmente all'adempimento di obblighi di legge che discendono dal D.lgs 24/2023 cui l'Ente è soggetto ed in via eventuale per la tutela di interessi dell'Ente stesso o di terzi.

Valutazione : Accettabile
Commento di valutazione : Trattandosi di adempimento di obbligo di legge gli scopi sono definiti dalle norme stesse.

Quali sono le basi legali che rendono lecito il trattamento?

Art. 6 par. 1, lett. c) per quanto riguarda la finalità primaria;
Art. 6, par. 1, lett. f) per quanto riguarda la finalità secondaria precisando che l'interesse legittimo azionato è quello di difendere gli interessi dell'Ente quale titolare o di eventuali terzi, fermo restando il bilanciamento degli interessi.

Valutazione : Accettabile
Commento di valutazione : Le basi giuridiche sono adeguatamente individuate

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

La piattaforma imposta la segnalazione di default come anonima non consentendo all'Ente di conoscere l'identità del segnalante. Soltanto ove fosse necessario conoscerne l'indentità questa potrà essere fornita direttamente dall'interessato. La RPC ha il controllo della segnalazione e valuta di volta in volta le necessità di trattamento dei dati.

Valutazione : Accettabile
Commento di valutazione : La strutturazione del percorso di segnalazione è garanzia adeguata

Azienda Unità Sanitaria Locale Umbria 1
tel. 075 54 11 - 075 85 091
Sede Legale
06127 - Perugia Via Guerra 21/17
(l.r. n.18/12.11.2012)
p.iva / c.f. 03301860544

I dati sono esatti e aggiornati?

I dati sono forniti direttamente dall'interessato, che li imputa nella piattaforma e, si assume la responsabilità della veridicità ed esattezza, potendo, successivamente, integrare o modificare gli stessi.

Valutazione : Accettabile
Commento di valutazione : Le modalità sono tali da garantire il rispetto del principio

Qual è il periodo di conservazione dei dati?

Per la finalità primaria il trattamento è limitato al periodo necessario all'esame e al seguito della segnalazione.
Per la finalità secondaria i dati sono conservati per il periodo di 5 anni (termine previsto dall'art. 14 comma 1 D.lgs. 24/2023) a decorrere dalla chiusura della segnalazione fatti salvi proroghe o sospensioni come per legge.

Valutazione : Accettabile
Commento di valutazione : La durata del trattamento è definita dalla Legge.

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Nella pagina ove è presente il link di collegamento alla piattaforma è messa a disposizione l'informativa ex artt. 12 e seg. ti GDPR che può essere conosciuta nel sito internet dell'Ente.
L'invio della segnalazione richiede di confermare la visione ed accettazione della informativa.

Valutazione : Accettabile
Commento di valutazione :le modalità di comunicazione appaiono adeguate

Azienda Unità Sanitaria Locale Umbria 1
tel. 075 54 11 - 075 85 091
Sede Legale
06127 - Perugia Via Guerra 21/17
(l.r. n.18/12.11.2012)
p.iva / c.f. 03301860544

Ove applicabile: come si ottiene il consenso degli interessati?

Considerate le basi giuridiche il consenso non è richiesto, tuttavia l'identità dell'interessato non può essere conosciuta dall'ente se egli stesso non fornisce spontaneamente i propri dati identificativi e di contatto.

Valutazione : Accettabile
Commento di valutazione : Il consenso non è richiesto.

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Nell'informativa fornita agli interessati sono indicati i punti di contatto del Titolare e del Responsabile della Protezione dei Dati cui possono essere inoltrate le richieste di esercizio dei diritti.
Nel Documento di Conformità dell'Ente è contenuta la Procedura per la soddisfazione dei diritti degli interessati.
Per quanto concerne il diritto alla portabilità dei dati ai sensi dell'art. 20 GDPR si precisa che per quanto riguarda i dati trattati dall'ente esso non trova applicazione poiché la base giuridica non rientra tra quelle richiamate dall'articolo citato.

Valutazione : Accettabile
Commento di valutazione : Gli strumenti per l'esercizio dei diritti degli interessati appaiono adeguati.

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

L'interessato può autonomamente accedere alla segnalazione mediante il codice identificativo univoco ed integrare o modificare la segnalazione stessa. Per quanto riguarda la cancellazione, ove sussistano le condizioni, il diritto può essere richiesto al Titolare o per mezzo del Responsabile della Protezione dei Dati: per quanto concerne i dati conservati nel sistema informativo dell'Ente, il titolare provvede direttamente alla cancellazione, mentre per quanto riguarda le informazioni eventualmente conservate nei sistemi informativi del gestore della piattaforma il titolare provvede secondo le funzionalità dello strumento a disposizione, ovvero facendone espressa richiesta al gestore.

Valutazione : Accettabile
Commento di valutazione : Vedi sopra

Azienda Unità Sanitaria Locale Umbria 1
tel. 075 54 11 - 075 85 091
Sede Legale
06127 - Perugia Via Guerra 21/17
(l.r. n.18/12.11.2012)
p.iva / c.f. 03301860544

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

L'esercizio del diritto di opposizione, ove ammissibile a norma dell'art. 21 GDPR e dell'art. 2-undecies Codice Privacy e del diritto di limitazione possono essere richiesti al Titolare o al Responsabile della Protezione dei Dati, che, dopo averne valutata l'ammissibilità, in caso positivo richiedono all'Ente di provvedere direttamente sui propri sistemi informativi, ovvero, di farne richiesta al gestore della piattaforma.

Valutazione : Accettabile
Commento di valutazione : vedi sopra

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

I rapporti tra Titolare e Responsabile sono definiti in uno specifico accordo.

Valutazione : Accettabile
Commento di valutazione :L'accordo è coerente con i requisiti previsti dall'art. 28 GDPR

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

I dati non sono esportati.

Valutazione : Accettabile
Commento di valutazione : Non ci sono trasferimenti.

Azienda Unità Sanitaria Locale Umbria 1
tel. 075 54 11 - 075 85 091
Sede Legale
06127 - Perugia Via Guerra 21/17
(l.r. n.18/12.11.2012)
p.iva / c.f. 03301860544

Rischi

Misure esistenti o pianificate

Crittografia

L'applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'Open Technology Fund di Washington. Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2+ con SSLLabs rating A+. Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con chiave asimmetrica personale e protocollo a curve ellittiche per ciascun utente avente accesso al sistema e ai dati delle segnalazioni. Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento. Il sistema è installato su sistema operativo Linux su cui è attiva Full Disk Encryption (FDE) a garanzia di maggiore tutela dei sistemi integralmente cifrati in condizione di fermo e in condizione di backup remoto. Protocollo crittografico: https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html

Valutazione : Accettabile
Commento di valutazione : La misura appare adeguata

Controllo degli accessi logici

L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali. Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password. Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238. Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.

Valutazione : Accettabile
Commento di valutazione : La misura appare adeguata

Tracciabilità

L'applicativo GlobaLeaks implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema in compatibilità con la massima confidenzialità richiesta dal processo di whistleblowing. Ogni log di audit viene mantenuto per un periodo massimo di 5 anni, fatto salvo il caso specifico dei log pertinenti le segnalazioni che vengono mantenuti per tutto il tempo di conservazione delle stesse.
I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali

Azienda Unità Sanitaria Locale Umbria 1
tel. 075 54 11 - 075 85 091
Sede Legale
06127 - Perugia Via Guerra 21/17
(l.r. n.18/12.11.2012)
p.iva / c.f. 03301860544

indirizzi IP e User Agent. I log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog e registri remoti centralizzati.

Valutazione : Accettabile
Commento di valutazione : La misura appare adeguata

Archiviazione

L'applicativo GlobaLeaks implementa un database SQLite integrato acceduto tramite ORM. Le configurazioni effettuate sono tali da garantire elevate garanzie di sicurezza grazie al completo controllo da parte dell'applicativo delle funzionalità sicurezza del database e delle policy di data retention e cancellazione sicura.

Valutazione : Accettabile
Commento di valutazione : La misura appare adeguata

Vulnerabilità

L'applicativo GlobaLeaks e la relativa metodologia di fornitura SaaS sono periodicamente soggetti ad audit di sicurezza indipendenti di ampio respiro su base almeno annuale e tutti i report vengono pubblicati per finalità di peer review. A questi si aggiunge la peer review indipendente realizzata dalla crescente comunità di stakeholder composta da un crescente numero di società quotate, fornitori e utilizzatori istituzionali che su base regolare commissionano audit indipendenti che vengono forniti al progetto privatamente. Audit di sicurezza: https://docs.globaleaks.org/en/main/security/PenetrationTests.html

Valutazione : Accettabile
Commento di valutazione : La misura appare adeguata

Backup

I sistemi sono soggetti a backup remoto con frequenza di 8 ore e policy di data retention di 7 giorni necessari per finalità di disaster recovery garantendo dunque una RPO di 8 ore

Valutazione : Accettabile
Commento di valutazione :la misura appare adeguata

Manutenzione

È prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza.
Per i server applicativi virtuali che realizzano il servizio di whistleblowing è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti. Per i sistemi che compongono l'infrastruttura fisica, di backup e firewall è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions e del relativo fornitore SaaS attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.

Valutazione : Accettabile
Commento di valutazione : La misura appare adeguata

Sicurezza dei canali informatici

Tutte le connessioni sono protette tramite protocollo TLS 1.2+ Le connessioni amministrative privilegiate sono mediate tramite accesso VPN e connessioni con protocollo SSH.

Valutazione : Accettabile
Commento di valutazione : La misura appare adeguata

Sicurezza dell'hardware

I datacenter del fornitore IaaS dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 7x24 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 7x24. I datacenter del fornitore IaaS sono certificati ISO27001.

Valutazione : Accettabile
Commento di valutazione : La misura appare adeguata

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Whistleblowing Solutions ha definito una procedura per la gestione delle violazioni dei dati personali.
Nel Documento di Conformità è inserita la "Procedura per la gestione dei Data Breach".

Valutazione : Accettabile
Commento di valutazione : La misura appare adeguata

Azienda Unità Sanitaria Locale Umbria 1
tel. 075 54 11 - 075 85 091
Sede Legale
06127 - Perugia Via Guerra 21/17
(l.r. n.18/12.11.2012)
p.iva / c.f. 03301860544

Lotta contro il malware

Tutti i computer del personale di Whistleblowing e dei sub-responsabili nominati eseguono firewall e antivirus come da policy aziendale ed il personale riceve continua e aggiornata formazione al passo con lo stato dell'arte in materia di lotta contro il malware. Parimenti le utenze del servizio di whistleblowing vengono sensibilizzate sulla tematica tramite formazione diretta o documentazione online.

Valutazione : Accettabile
Commento di valutazione : La misura appare adeguata

Contratto con il responsabile del trattamento

I rapporti tra Ente e gestore della segnalazione sono regolati dal "Contratto di servizio" nell'aggiornamento del 20/9/2023.

Valutazione : Accettabile
Commento di valutazione : La misura appare adeguata

Politica di tutela della privacy

Nel Documento di Conformità sono inseriti i principi alla base della politica di tutela della Privacy adottatati dall'Ente.

Valutazione : Accettabile
Commento di valutazione : La misura appare adeguata

Gestione dei rischi

Nel Documento di Conformità è inserita l'analisi dei rischi collegata ad un sistema di livelli crescenti della protezione dei dati.

Valutazione : Accettabile
Commento di valutazione :la misura appare adeguata

Azienda Unità Sanitaria Locale Umbria 1
tel. 075 54 11 - 075 85 091
Sede Legale
06127 - Perugia Via Guerra 21/17
(l.r. n.18/12.11.2012)
p.iva / c.f. 03301860544

Gestione postazioni

È onere di ciascun responsabile di Punto Organizzativo (a qualsiasi livello in proporzione ai poteri affidati e nei limiti degli ambiti assegnati) assicurare la corretta tenuta delle postazioni del personale a lui affidato.

Valutazione : Accettabile
Commento di valutazione : La misura appare adeguata

Gestione del personale

I compiti e le responsabilità del personale che tratta i dati sono adeguatamente definiti e descritti nel documento di conformità che è periodicamente aggiornato.

Valutazione : Accettabile
Commento di valutazione : La misura appare adeguata

Vigilanza sulla protezione dei dati

La vigilanza sulla protezione dei dati è costante a cura dell'owner del processo e responsabile del sistema informativo. Il DPO svolge controlli a campione periodici.

Valutazione : Accettabile
Commento di valutazione : La misura appare adeguata

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Considerata la delicatezza dei contenuti possibili delle segnalazioni con specifico riferimento sia ai segnalanti che ai segnalati l'impatto prodotto potrebbe essere definito ALTO ovvero che l'interessato potrebbe subire conseguenze significative superabili solo con serie difficoltà.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Attacco Hacker, Attività di Social Engineering, Perdita di confidenzialità delle credenziali di autenticazione

Azienda Unità Sanitaria Locale Umbria 1
tel. 075 54 11 - 075 85 091
Sede Legale
06127 - Perugia Via Guerra 21/17
(l.r. n.18/12.11.2012)
p.iva / c.f. 03301860544

Quali sono le fonti di rischio?

Dipendente, Fornitore, Collega segnalante, Collega Facilitatore

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Crittografia, Tracciabilità, Sicurezza dei canali informatici, Sicurezza dell'hardware, Lotta contro il malware, Gestione del personale, Contratto con il responsabile del trattamento, Gestione postazioni

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitata, Il valore indicato è determinato dalla severità dell'impatto che si potrebbe produrre in caso di avveramento del rischio. Le misure di sicurezza adottate contribuiscono a mitigarne la portata.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata, Non ci sono eventi storici che hanno interessato direttamente l'azienda anche se nel settore di appartenenza si sono registrati attacchi hacker ad altri enti. La valutazione è prudente anche se le modalità di esecuzione e le misure adottate fanno ragionevolmente ritenere improbabile l'incidente.

Valutazione : Accettabile
Commento di valutazione :L'analisi appare adeguata e coerente

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Considerata la delicatezza dei contenuti possibili delle segnalazioni con specifico riferimento sia a i segnalanti che ai segnalati l'impatto prodotto potrebbe essere definito ALTO ovvero che l'interessato potrebbe subire conseguenze significative superabili solo con serie difficoltà.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Attacco Hacker, Attività di Social Engineering, Perdita di confidenzialità delle credenziali di autenticazione

Quali sono le fonti di rischio?

Collega Facilitatore, Collega segnalante, Dipendente, Fornitore, Segnalante

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici, Tracciabilità, Sicurezza dell'hardware, Sicurezza dei canali informatici, Lotta contro il malware, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vigilanza sulla protezione dei dati, Gestione postazioni, Gestione del personale, Gestione dei rischi, Politica di tutela della privacy

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Limitata, Si ritiene ragionevole attribuire un valore limitato in considerazione della possibilità del responsabile della segnalazione di interagire con l'interessato per fare le verifiche che ritenesse opportune e, nel caso in cui quest'ultimo non intenda interagire, la segnalazione può essere chiusa.

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Limitata, Si ritiene ragionevole attribuire un valore limitato in considerazione delle misure di sicurezza adottate ed in particolare la sicurezza dello HW e SW per la minaccia Hacker; e la formazione, le politiche, e la vigilanza, per quanto riguarda le altre minacce.

Valutazione : Accettabile
Commento di valutazione : Il rischio appare coerentemente valutato

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Per quanto riguarda questo rischio particolare, l'impatto potrebbe ragionevolmente essere considerato lieve perché il sistema permette di interagire con il segnalante e dunque ricostruire gli eventuali dati mancanti.

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Attacco Hacker, Guasto Hardware, Software o della infrastruttura, Attività di Social Engineering, Perdita di confidenzialità delle credenziali di autenticazione

Azienda Unità Sanitaria Locale Umbria 1
tel. 075 54 11 - 075 85 091
Sede Legale
06127 - Perugia Via Guerra 21/17
(l.r. n.18/12.11.2012)
p.iva / c.f. 03301860544

Quali sono le fonti di rischio?

Evento naturale, Evento doloso, Incendio, Evento Hardware

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Archiviazione, Backup, Manutenzione, Sicurezza dei canali informatici, Sicurezza dell'hardware, Lotta contro il malware, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Contratto con il responsabile del trattamento, Politica di tutela della privacy, Gestione del personale, Vigilanza sulla protezione dei dati, Gestione postazioni

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Trascurabile, Ragionevolmente, si può ritenere che l'impatto sia lieve poiché il Responsabile delle Segnalazioni può interagire con il segnalante per ricostruire i dati eventualmente perduti e, a livello di sistema è implementato un backup nonché la ridondanza degli apparati critici.

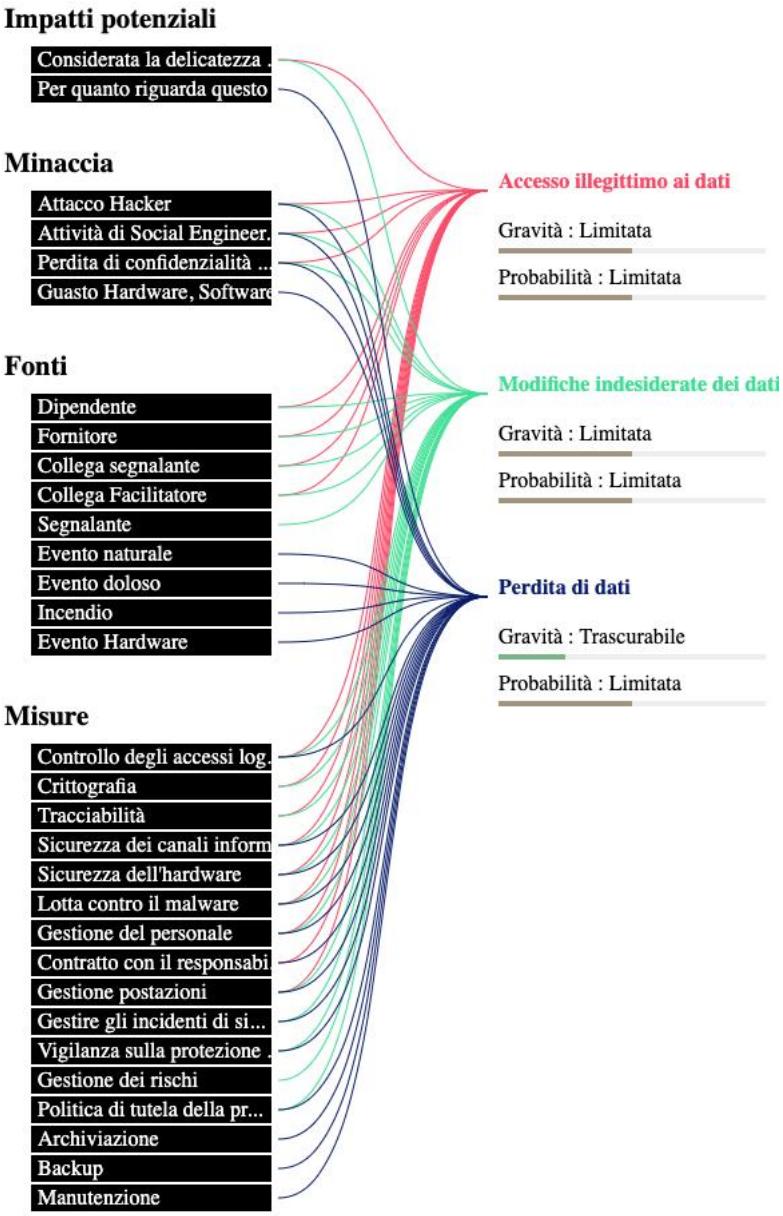
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata, Ragionevolmente il rischio può essere considerato trascurabile poiché le misure di sicurezza appaiono adeguate rispetto alle minacce, con particolare riferimento alle misure di backup e di ridondanza.

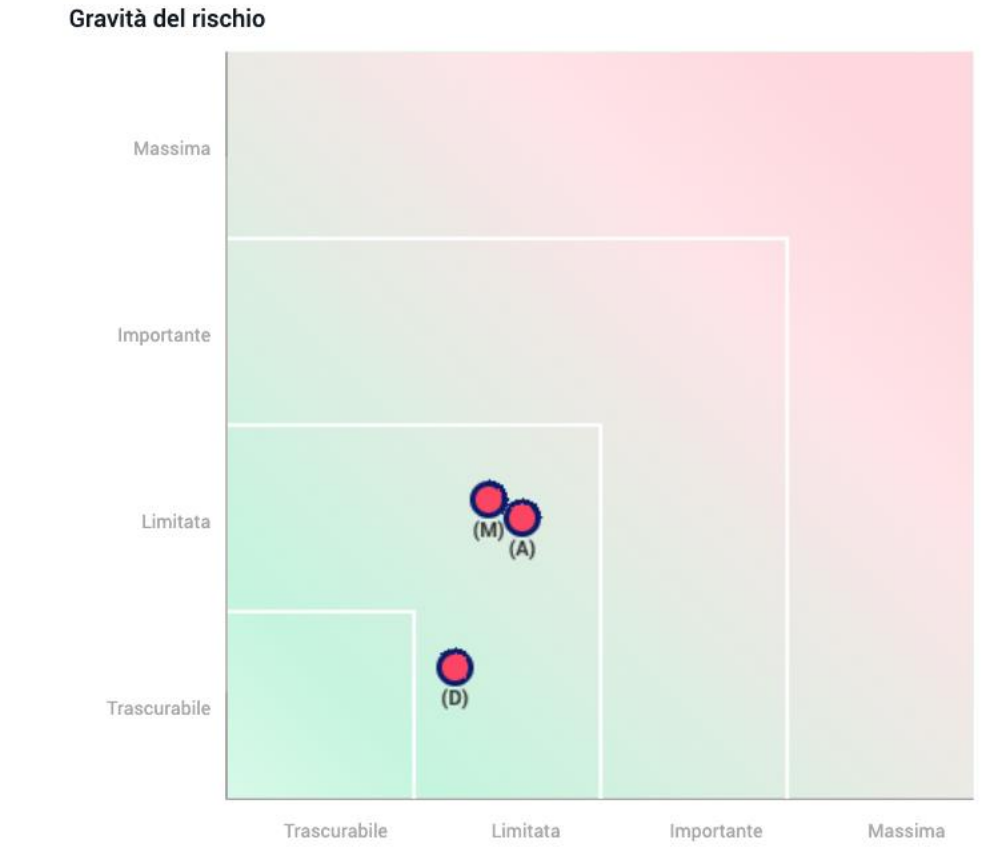
Valutazione : Accettabile
Commento di valutazione : Il rischio appare valutato coerentemente

Azienda Unità Sanitaria Locale Umbria 1
tel. 075 54 11 - 075 85 091
Sede Legale
06127 - Perugia Via Guerra 21/17
(l.r. n.18/12.11.2012)
p.iva / c.f. 03301860544

Panoramica dei rischi



Schema di posizionamento valori di rischio

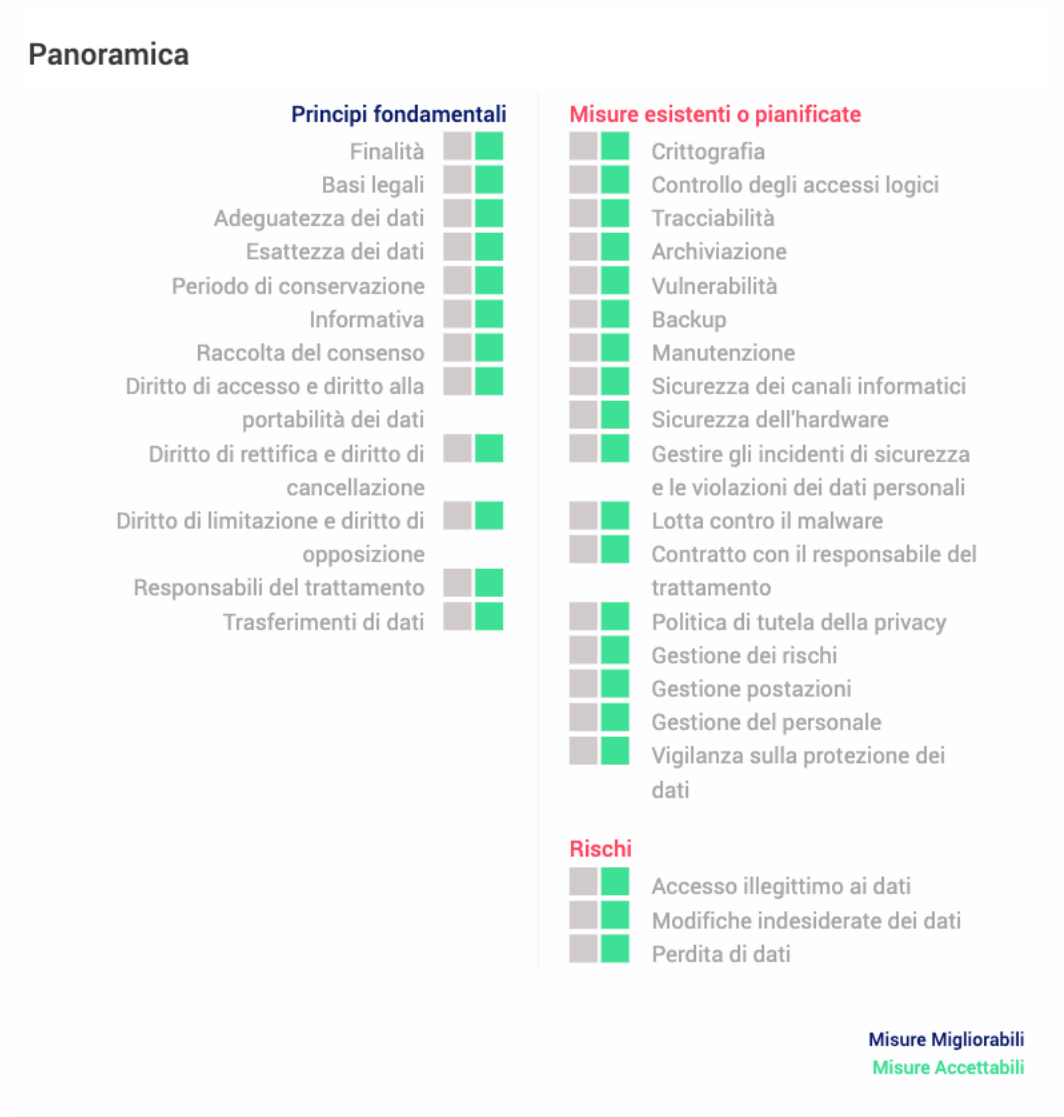


- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

08/04/24

Azienda Unità Sanitaria Locale Umbria 1
tel. 075 54 11 - 075 85 091
Sede Legale
06127 - Perugia Via Guerra 21/17
(l.r. n.18/12.11.2012)
p.iva / c.f. 03301860544

Piano di azione



Azienda Unità Sanitaria Locale Umbria 1
tel. 075 54 11 - 075 85 091
Sede Legale
06127 - Perugia Via Guerra 21/17
(l.r. n.18/12.11.2012)
p.iva / c.f. 03301860544

Questo documento è stato completato a Perugia, alla data dell'ultima sottoscrizione, a cura della Referente Privacy, con il supporto e collaborazione del Responsabile della Protezione dei Dati, e la approvazione del Direttore Amministrativo

Il Referente Privacy	**Dott.ssa Maria Gabriella Stortoni ***	MARIA GABRIELLA STORTONI 20.05.2024 10:27:52 GMT+01:00
Il Responsabile della Protezione dei Dati	**Avv. Alessandro Frillici ***	ALESSANDRO FRILLICI 20.05.2024 10:00:22 GMT+01:00
Il Direttore Amministrativo	**Dott. Enrico Martelli ***	

Azienda Unità Sanitaria Locale Umbria 1
tel. 075 54 11 - 075 85 091
Sede Legale
06127 - Perugia Via Guerra 21/17
(l.r. n.18/12.11.2012)
p.iva / c.f. 03301860544