Registro dei Trattamenti

Articolo 30 RGPD "Registri delle attività di trattamento"

Misure interne di sicurezza per il trattamento dei dati

1. Scopo

Il presente Documento è adottato, ai sensi **del Regolamento UE 679/2016 General Data Protection Regulation n. 679 del 24-05-2016**, per definire le politiche di sicurezza in materia di trattamento di dati personali ed i criteri organizzativi per la loro attuazione.
In particolare, nel Documento vengono definiti:

a) i criteri e le procedure per assicurare l'integrità dei dati;
b) i criteri e le procedure per la sicurezza della trasmissione dei dati, ivi compresi quelli per l'accesso per via telematica;
c) l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

2. Campo di applicazione

Il Documento definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali.
Il Documento si applica al trattamento di tutti i dati personali per mezzo di:

- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (es. cartacei, audio, visivi e audiovisivi, ecc.)

Il Documento deve essere conosciuto ed applicato da tutti gli Uffici di AltaVita-IRA.

3. Riferimenti normativi

- L. n. 675/1996;
- D. Lgs n. 123/1997
- D. Lgs n. 255/1997
- D. Lgs n. 135/1998
- D. Lgs n. 171/1998
- D. Lgs n. 389/1998
- D. Lgs n. 51/1999
- D. Lgs n. 135/1999
- D. Lgs n. 281/1999
- D. Lgs n. 282/1999
- D.P.R. n. 318/1999
- L. n. 325 del 3/11/2000
- D. Lgs n. 196/30-06-2003 Codice di Sicurezza, come modificato con D.Lgs. 101 del 10 agosto 2018.
- D.L. n. 112 del 25 giugno 2008, convertito, con modificazioni, dalla legge 6 agosto 2008 n. 133
- L. n. 120 del 29 luglio 2010,
- D.L. n. 70 del 13 maggio 2011, convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106.
- D.L. n. 5 del 12 febbraio 2012, convertito dalla legge 35 del 4 aprile 2012.
- GDPR 679/2016 Regolamento Generale Europeo del 24 maggio 2016.
- D.Lgs. 101 del 10 Agosto 2018 pubblicato il 4 Settembre 2018.

4. Principi e Liceità del trattamento (artt. 5 e 6 Regolamento UE 679/2016)

Principi applicabili al trattamento di dati personali

1.I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che il trattamento non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e

organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

2.Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

Liceità del trattamento

1.Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

2.Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX.

3.La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita: a) dal diritto dell'Unione; o b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento. La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito.

4.Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:

a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;
c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;
d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

5. Sedi e strumenti (allegato 1: Sedi e strumenti)

5.1. *Inventario delle sedi nelle quali vengono trattati i dati*

Al Titolare del trattamento dei dati o al Referente di Area è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle sedi in cui viene effettuato il trattamento dei dati.

5.2. *Inventario dei sistemi di elaborazione*

Al Titolare del trattamento dei dati o al Responsabile del trattamento è affidato il compito di redigere l'elenco dei sistemi di elaborazione con cui viene effettuato il trattamento dei dati.

6. La distribuzione dei compiti e delle responsabilità (Allegato 2: Lista Utenti; eventuali lettere di incarico e designazione con contratto)

6.1. *Il Titolare del trattamento*

È la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

1.Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

2.Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

3.L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

6.2. *Il Responsabile del trattamento*

«Responsabile del trattamento» è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

1.Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

2.Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

3.I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico; b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
b) adotti tutte le misure richieste ai sensi dell'articolo 32;
c) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;

d) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
e) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
f) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
g) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.
h) Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

4.Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

5.L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 del GDPR o a un meccanismo di certificazione approvato di cui all'articolo 42 del GDPR può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 dell' articolo 28 del GDPR.

6.Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 dell'art. 28 del GDPR, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43 dell'art. 28 del GDPR.

7.La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 dell'art. 28 del GDPR e secondo la procedura d'esame di cui all'articolo 93, paragrafo 2 del GDPR.

8.Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 dell'art. 28 del GDPR in conformità del meccanismo di coerenza di cui all'articolo 63 del GDPR.

9.Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 dell'art. 28 del GDPR è stipulato in forma scritta, anche in formato elettronico.

10.Fatti salvi gli articoli 82, 83 e 84 del GDPR, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.

Amministratore del sistema preposto alla custodia delle credenziali è "il soggetto a cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione", con il compito di gestire, attribuire e revocare le credenziali di autenticazione. Tramite le credenziali è possibile costruire il profilo di autorizzazione, la capacità di ogni incaricato di accedere alle proprie cartelle di lavoro, secondo delle logiche funzionali decise dai responsabili di area e dai dirigenti del Titolare.

6.3. Nomina delle persone autorizzate al trattamento

Al Titolare del trattamento dei dati o al Responsabile è affidato il compito di nominare, con comunicazione scritta, uno o più Incaricati o Persone Autorizzate del trattamento dei dati.
La nomina di ciascun autorizzato del trattamento dei dati deve essere effettuata con una lettera di incarico in cui sono specificati i compiti che gli sono affidati.
Gli autorizzati al trattamento devono ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.
Agli autorizzati deve essere assegnata una parola chiave, e un codice identificativo personale.
La nomina degli autorizzati al trattamento deve essere controfirmata dall'interessato per presa visione.
Agli autorizzati al trattamento deve essere consegnata una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina degli autorizzati al trattamento è a tempo indeterminato, e decade per revoca, per sue dimissioni, o con il venir meno dei compiti che giustificavano il trattamento dei dati personali.

7. L'analisi dei rischi che incombono sui dati

Il Documento è stato redatto in funzione di una preventiva analisi dei rischi che incombono sui dati personali ottenuta confrontando la situazione dell'Ente esistente con quanto imposto dalle misure minime di legge.

8. Misure da adottare per garantire l'integrità e la disponibilità dei dati.

8.1. Misure di sicurezza contro il rischio di accesso non autorizzato

8.1.1. NORME GENERALI DI PREVENZIONE

In considerazione di quanto disposto è fatto divieto di:

- Effettuare copie su supporti magnetici o trasmissioni non autorizzate.
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del Responsabile del trattamento dei dati stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal Responsabile del trattamento dei dati stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

8.1.2. PROCEDURE DI ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE

Il Titolare del trattamento dei dati o il Responsabile definisce le modalità di assegnazione delle Credenziali di autenticazione composte da User-Id (dato pubblico) e password (dato strettamente privato)
Le password sono composte al minimo di 8 caratteri alfanumerici e vengo sostituite ogni 6 mesi.

8.1.3. IDENTIFICAZIONE DEGLI ELABORATORI UTILIZZATI PER IL TRATTAMENTO

Al Titolare del trattamento dei dati o al Responsabile è affidato il compito di redigere e di aggiornare l'elenco dei sistemi di elaborazione utilizzati per il trattamento.

8.1.4. CRITERI E PROCEDURE PER GARANTIRE LA SICUREZZA DELLE TRASMISSIONI DEI DATI

Al fine di garantire la sicurezza delle trasmissioni dei dati, attraverso l'utilizzo di apparecchi di trasmissione dati, quali "Modem" e "Router", il Responsabile del trattamento dei dati stabilisce le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione o di hacker su ogni sistema collegato in rete pubblica.
In particolare, per ogni sistema interessato sono state previste le seguenti specifiche:

- **Presenza di un sistema anti-intrusione (Firewall)**
- **Presenza di un software antivirus costantemente aggiornato**

8.2. Misure di sicurezza contro il rischio di trattamento non consentito

8.2.1. PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI

Al Titolare del trattamento dei dati o al Referente di Area è affidato il compito di redigere e di aggiornare annualmente ad ogni variazione l'elenco degli autorizzati al trattamento dei dati personali.
In caso di dimissioni di un autorizzato al trattamento o di revoca delle autorizzazioni al trattamento dei dati si provvederà a disattivare la possibilità di accesso al sistema per il soggetto in questione.

8.2.2. VERIFICHE PERIODICHE DELLE CONDIZIONI PER IL MANTENIMENTO DELLE AUTORIZZAZIONI

Al Titolare del trattamento dei dati o al Referente di Area è affidato il compito di verificare ogni anno, le autorizzazioni di accesso ai dati oggetto del trattamento e di aggiornare l'elenco degli utenti autorizzati.

9. Criteri e modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento

9.1. Criteri e procedure per garantire l'integrità dei dati

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, il Titolare del trattamento dei dati o al Referente di Area stabilisce la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche di dati trattati.
In particolare, debbono essere definite le seguenti specifiche:

- Le istruzioni ed i comandi necessari per effettuare le copie di back-up. (Procedura)
- La frequenza dei Back-up

9.2. Protezione da virus informatici

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita di dati a causa di virus informatici, il Responsabile del trattamento dei dati stabilisce quali protezioni software adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.
Il Responsabile del trattamento dei dati stabilisce inoltre la periodicità, almeno ogni sei mesi, con cui debbono essere effettuati gli aggiornamenti dei sistemi antivirus utilizzati per ottenere un accettabile standard di sicurezza delle banche dati trattati.

9.3. *Custodia e conservazione dei supporti utilizzati per il back-up dei dati*

Il Titolare del trattamento dei dati o il Referente di Area è responsabile della custodia e della conservazione di supporti utilizzati per il back-up dei dati.

- Deve essere indicato il luogo di conservazione ed i supporti utilizzati per il back-up dei dati.
- Devono essere previste delle verifiche periodiche sul contenuto dei supporti di back-up (prove di ripristino)

9.4. *Manutenzione apparecchiature e dei sistemi di trattamento dei dati*

9.4.1. MANUTENZIONE DI SISTEMI DI ELABORAZIONE DEI DATI

Al Titolare del trattamento dei dati o al Referente di Area è affidato il compito di verificare ogni anno la situazione delle apparecchiature hardware installate con cui vengono trattati i dati, delle apparecchiature periferiche, ed in particolare dei dispositivi di collegamento con le reti pubbliche.

La verifica ha lo scopo di controllare l'affidabilità del sistema, per quanto riguarda:

- La sicurezza dei dati trattati
- Il rischio di distruzione o di perdita
- Il rischio di accesso non autorizzato o non consentito tenendo conto anche dell'evoluzione tecnologica.

9.4.2. MANUTENZIONE DEI SISTEMI OPERATIVI

Al Titolare del trattamento dei dati (o al Responsabile se previsto) è affidato il compito di aggiornare e verificare ogni anno la situazione dei Sistemi Operativi installati sulle apparecchiature con le quali vengono trattati i dati.

La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi, per quanto riguarda:

- La sicurezza dei dati trattati
- Il rischio di distruzione o di perdita
- Il rischio di accesso non autorizzato o non consentito tenendo conto in particolare di:
- Disponibilità di nuove versioni migliorative dei Sistemi operativi utilizzati
- Segnalazioni di Patch, Fix o System-Pack per la rimozione di errori o malfunzionamenti
- Segnalazioni di Patch, Fix o System-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

9.4.3. MANUTENZIONE DELLE APPLICAZIONI DI TRATTAMENTO DEI DATI

Al Titolare del trattamento dei dati o al Referente di Area è affidato il compito di aggiornare costantemente e verificare ogni anno, la situazione delle applicazioni installate sulle apparecchiature con cui vengono trattati i dati.

La verifica ha lo scopo di controllare l'affidabilità del software applicativo, per quanto riguarda:

- La sicurezza dei dati trattati
- Il rischio di distruzione o di perdita
- Il rischio di accesso non autorizzato o non consentito.

tenendo conto in particolare della disponibilità di nuove versioni migliorative delle applicazioni installate che consentano maggiore sicurezza contro i rischi di intrusione o di danneggiamento dei dati.

9.5. *Misure di sicurezza per il trattamento dei dati effettuato con strumenti non automatizzati* (*art. 32* Regolamento UE 679/2016)

9.5.1. ISTRUZIONI AGLI AUTORIZZATI (vedere allegato 3: **Manuale per la Sicurezza**)

Gli autorizzati che trattano atti e documenti contenenti dati personali sono tenuti a conservarli e restituirli al termine delle operazioni.

Qualora i documenti contengano dati particolari (art. 4 p.13,14,15 Regolamento UE 679/2016) gli incaricati sono tenuti a conservarli fino alla restituzione in **contenitori chiudibili**.

L'accesso agli archivi contenenti documenti ove sono presenti dati sensibili o giudiziari è consentito, dopo l'orario di chiusura, previa identificazione e registrazione dei soggetti.

9.5.2. COPIE DEGLI ATTI DEI DOCUMENTI

Quanto indicato nel punto precedente si applica anche a qualunque tipo di copia effettuata sui documenti contenenti dati personali.

10. Criteri da adottare in caso di trattamenti di dati personali affidati all'esterno

10.1. *Trattamento dei dati in out-sourcing*

Il Titolare del trattamento può decidere di affidare il trattamento dei dati in tutto o in parte a soggetti terzi, in out-sourcing, contrattualizzati come Responsabili del trattamento.

In questo caso debbono essere specificati i soggetti interessati e i luoghi dove fisicamente avviene il trattamento dei dati stessi.

Il Responsabile del trattamento dei dati in out-sourcing deve rilasciare una dichiarazione scritta al Titolare del trattamento da cui risulti che sono state adottate le misure adeguate di sicurezza per il trattamento dei dati secondo quanto disposto dall'art.32 del Regolamento UE 679/2016.

10.2. Misure di tutela e garanzia sugli interventi esterni presso la propria struttura

Il Titolare del trattamento deve adottare delle misure minime di sicurezza quando si avvale di soggetti esterni alla propria struttura, in modo che, prima di provvedere alla esecuzione, deve ricevere dall'installatore una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle disposizioni del Regolamento UE 679/2016.

11. *Violazione dei dati*

11.1 Notifica di una violazione dei dati personali all'autorità di controllo Art.33 (C85, C87, C88)

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve almeno:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

11.2 Comunicazione di una violazione dei dati personali all'interessato Articolo 34 (C86-C88)

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

12. Allegati

Il presente Documento è stato redatto nel mese di **settembre 2019** ed è correlato dal seguenti allegati:

1. SEDI E STRUMENTI
   1.1 DPIA PER VIDEOSORVEGLIANZA
2. MANUALE PER LA SICUREZZA E PRIVACY POLICY
3. MODELLO DI GESTIONE INCIDENTI DI SICUREZZA DATA BREACH

Registro dei Trattamenti

ALLEGATO 1

Sedi – Trattamenti- Strumenti

Il Titolare:
AltaVita-Istituzioni Riunite di Assistenza-IRA
Padova 35137 – Piazzale Mazzini, 14 - P.IVA 00558060281
Contatto:
Tel. 049.8241511 Fax 049.8241531 Mail: segreteriagenerale@altavita.org WEB: www.altavita.org

Il Responsabile della Protezione dei Dati (RPD) o Data Protection Officer (DPO):
UNINDUSTRIA SERVIZI & FORMAZIONE TREVISO PORDENONE S.C.AR.L.
contatto:
rpd@altavita.org.

AltaVita - I.R.A. è dotato di quasi 600 posti letto in queste sedi operative:

- Struttura residenziale "Beato Pellegrino" con quattro residenze in via Beato Pellegrino 192 - Padova
- Struttura residenziale "G. A. Bolis" con tre nuclei in Piazza Beatrice de Claricini, 12 - Selvazzano Dentro (PD)
- il Pensionato Piaggi in Piazzale Mazzini 16 - Padova
- il Centro Diurno "Casa Famiglia Gidoni" per anziani non autosufficienti in Via Mons. Fortin, 34 - Padova
- il Centro Diurno "Monte Grande", per anziani non autosufficienti, in Piazza Beatrice de Claricini, 12 - Selvazzano Dentro (PD)

Luoghi fisici

1) Sede legale e amministrativa

Città:	Piazzale Mazzini, 14 - Padova
Indirizzo Sede:	Sede disposta in un palazzo storico disposto su 3 piani. E' dotato di sistemi di sicurezza quali Videosorveglianza gestita dalla struttura ospitante, sistemi di controllo degli accessi, sistemi di allarme.

2) Unità Locale "Pensionato Piaggi"

Città:	Piazzale Mazzini, 16 - Padova
Indirizzo Sede:	Pensionato Piaggi è una residenza per anziani (Casa-Albergo) con 60 posti letto residenziali per fornire ospitalità e assistenza agli **anziani autosufficienti**, per i quali non sia più possibile la permanenza nel proprio ambiente familiare. Agli ospiti viene offerto un servizio di tipo alberghiero, con stanze singole o matrimoniali climatizzate, con bagno, terrazzo e telefono con linea privata. Nel Pensionato sono presenti diverse figure professionali.

3) Unità Locale "Centro Servizi G. A. Bolis"

Città:	Piazza Beatrice de Claricini, 12 - Selvazzano Dentro (Padova)
Indirizzo Sede:	Il Centro Servizi "G.A. Bolis" dispone di RESIDENZE PER ANZIANI **NON AUTOSUFFICIENTI** • Residenza Monte Rua: per ospiti non autosufficienti n° 60 posti letto • Residenza Monte Venda: per ospiti non autosufficienti n° 40 posti letto Sono stati concessi in locazione all'Azienda Ospedaliera di Padova alcuni locali ove ha sede il Centro Regionale per lo Studio e la Cura dell'invecchiamento cerebrale.

4) Unità Locale "CENTRO DIURNO MONTE GRANDE"

Città:	Piazza Beatrice de Claricini, 12 - Selvazzano Dentro (Padova)
Indirizzo Sede:	Il Centro Diurno per anziani non autosufficienti "Monte Grande" offre un servizio di semi-residenzialità di natura socio-assistenziale, con attività diurne finalizzate al mantenimento delle potenzialità e delle autonomie socio-relazionali della persona anziana. Dispone di 30 posti. Alla sera è previsto il rientro a casa dell'anziano ospite. Il centro diurno Monte Grande rappresenta un servizio di "sollievo" per il nucleo familiare che si trova in difficoltà nella gestione quotidiana dell'anziano non autosufficiente. Il Centro Diurno si trova all'interno della struttura "G. A. Bolis".

5) Unità Locale "CENTRO DIURNO CASA FAMIGLIA GIDONI"

Città:	Via Monsignor Fortin, 34 - Padova
Indirizzo Sede:	"Casa Famiglia" Gidoni è un centro diurno per anziani non autosufficienti che offre un servizio di semi-residenzialità di natura socio-assistenziale, con attività diurne finalizzate al mantenimento delle potenzialità e delle autonomie socio-relazionali della persona anziana. Dispone di 30 posti. Alla sera è previsto il rientro a casa dell'anziano ospite. Il centro diurno "Casa Famiglia" Gidoni rappresenta un servizio di "sollievo" per il nucleo familiare che si trova in difficoltà nella gestione quotidiana dell'anziano non autosufficiente. Al piano terra si trovano l'accettazione gli ambulatori la palestra, fisioterapia, ludoterapia. Accanto, collegati al resto della struttura e affacciati sulla piazza

	pedonale del Centro residenziale Civita, si trovano il servizio bar e ristorante in regime di convenzione con il Centro Diurno. Il primo piano, raggiungibile con un ascensore su misura per gli anziani ospiti, è suddiviso in due zone. La zona di servizio con: i locali di soggiorno per gli ospiti, i bagni assistiti, i servizi particolari, due stanze per il riposo pomeridiano. Lo spazio comune con: i servizi amministrativi, la sala polivalente e una sala per il volontariato.

6) Unità Locale "CENTRO SERVIZI BEATO PELLEGRINO"

Città:	Via Beato Pellegrino, 192 – Padova 35137
Indirizzo Sede:	Il Centro Servizi Beato Pellegrino dispone di: RESIDENZE PER ANZIANI **NON AUTOSUFFICIENTI** • Residenza **Rose**: per ospiti non autosufficienti n° 120 posti letto • Residenza **Tulipani**: ospiti non autosufficienti n° 100 posti letto • Residenza **Mimose**: >ospiti non autosufficienti n° 21 posti letto >ospiti non autosufficienti livello medio n° 72 posti letto (nuclei Residenza Sanitaria Assistenziale Anziani R.S.A.) • Residenza **Fiordalisi**: >ospiti non autosufficienti n° 35 posti letto >ospiti non autosufficienti livello medio n° 48 posti letto (nuclei Residenza Sanitaria Assistenziale Anziani – R.S.A.)

Tipologia dati trattati
Il Titolare nell'ambito della propria attività può trattare:
- Dati personali e particolari relativi agli ospiti;
- Dati personali relativi ai parenti o tutori degli ospiti;
- Dati personali fornitori (fatture, preventivi, eventuali documenti di trasporto, appalti, etc.);
- Dati personali e particolari dei dipendenti;
- Dati personali e particolari del personale somministrato;
- Dati personali e particolari dei collaboratori e consulenti;
- Dati personali e particolari LPU, Tirocini e alternanza scuola lavoro e personali del personale appartenente alle Associazioni di volontariato;
- Dati personali relativi alla videosorveglianza.

Base giuridica e Finalità dei trattamenti
La finalità dei trattamenti sopradescritti e svolti sono obbligatori per poter ottemperare alle normative ai fini fiscali (Ospiti, fornitori), fiscali e previdenziali (personale dipendente, collaboratori), di legge.
Come successivamente esplicitato i dati sono adeguatamente protetti e le strutture terze che possono accedervi sono contrattualizzate ed edotte sui rischi derivanti dal rapporto in essere.

Misure
La sicurezza logica degli edifici si basa sul controllo degli accessi, sulla presenza di un sistema antintrusione e un sistema di videosorveglianza di cui si evidenzia specifica D.P.I.A. (Data Privacy Impact Analisys). Sulle attrezzature sono state accese polizze contro i rischi di incendio, furto oltre alla Responsabilità Civile per l'attività svolta e professionale per i Professionisti.

Archivi Cartacei
Ogni archivio cartaceo è dotato di idonei armadi con serrature di sicurezza e sono ubicati in stanze e vani chiudibili a chiave, ad accesso controllato e limitato.

In ogni sede od unità locale i documenti cartacei vengono suddivisi per area:
- Archivio dati ospiti e parenti/Amministratori di Sostegno in faldoni presso Ufficio Assistenti Sociali.
- Archivio cartelle sanitarie presso ogni Ambulatorio medico di riferimento.

Nella sede amministrativa si trovano:
- Archivio dati personale dipendente e collaboratori per fini fiscali, adempimenti contabili, previdenziali e fascicoli sanitari ai fini del D.Lgs. n. 81/2008.
- Archivio Settore Acquisti Contabilità e Bilancio con i dati contabili posto al primo piano che divide con la sala server ovviamente chiusa e protetta.
- Archivio Settore Segreteria Generale.

DESCRIZIONE DELLE TIPOLOGIE DI TRATTAMENTI

TRATTAMENTO DEI DATI AREA DEL PERSONALE DIPENDENTE E FIGURE ASSIMILATE (personale somministrato, lavoratori di pubblica utilità, alternanza scuola-lavoro, personale volontario)

BASE GIURIDICA DEL TRATTAMENTO
I dati personali indicati sono trattati dal Titolare del trattamento nell'esecuzione dei propri compiti di interesse privato e pubblico o comunque necessari all'assolvimento degli obblighi di legge e contrattuali. I dati non vengono trasferiti verso paesi extra UE.

Tempi di conservazione e di cancellazione
I dati vengono trattati secondo le disposizioni consultabili all'interno del Piano di Conservazione approvato dall'Ente, ove è previsto un termine massimo di trattamento illimitato. Per le figure assimilate il termine di conservazione è quello previsto dal codice civile di prescrizione ordinaria (10 anni).

Modalità di Trattamento e categorie di dati personali degli Interessati
Il trattamento dei dati personali, particolari e giudiziari del personale dipendente e familiari viene effettuato per consentire ad AltaVita-Istituzioni Riunite di Assistenza-IRA di gestire i rapporti di lavoro in essere e quelli di futura costituzione nonché per finalità contabili, previdenziali, fiscali e di tutela legale; in particolare, il trattamento viene effettuato per consentire, nei termini che verranno di seguito meglio specificati: a) la gestione della dotazione organica; b) la gestione giuridico/economica e previdenziale del personale; c) i rapporti con i soggetti interni; d) i rapporti con i soggetti esterni; e) adempimenti in materia di sicurezza nei luoghi di lavoro, f) attività varie.
Quanto al trattamento ***sub* a) Gestione della dotazione organica** si precisa che essa si sostanzia nella:
1) Sintesi definizione e controllo della dotazione organica,
2) Predisposizione bandi e Indizione procedure selettive per assunzioni,
3) Esame della regolarità delle domande per ammissione a selezioni pubbliche;
4) Predisposizione provvedimenti e approvazione risultanze delle procedure selettive per le assunzioni;
5) Liquidazione del compenso delle Commissioni Giudicatrici delle procedure selettive per l'assunzione;
6) Gestione di domande di assunzione extra selezioni;
7) Gestione mobilità tra enti;
8) Pratiche relative all'accertamento dell'idoneità specifica al lavoro per l'assunzione;
9) Verifica delle condizioni di idoneità alle mansioni del personale dipendente;
10) Pratiche relative al riconoscimento di inabilità o infermità da causa di servizio ed equo indennizzo.

Quanto al trattamento ***sub* b) Gestione giuridico/economica e previdenziale del personale** - si precisa che essa si sostanzia nella:
1) Gestione assunzione personale dipendente;
2) Gestione e stipula di contratto di lavoro subordinato e autonomo;
3) Gestione proroghe incarichi a tempo determinato;
4) Gestione cessazione rapporto di lavoro;
5) Gestione sospensione rapporto di lavoro;
6) Gestione variazioni giuridiche rapporto di lavoro;
7) Attribuzione personale dipendente del trattamento economico in base al CCNL e al CCI e alla normativa vigente;
8) Elaborazione ed emissione dei cedolini paga;
9) Dichiarazioni contributive mensili a INPS e fiscali all'Agenzia delle Entrate;
10) Gestione dell'assegno del nucleo familiare;
11) Controllo fatturazione dei servizi dell'Agenzia di somministrazione del personale;
12) Pratiche donazioni sangue personale dipendente;
13) Pratiche pignoramento e sequestro retribuzioni del personale dipendente;
14) Gestione delle visite fiscali;
15) Pratiche ricongiunzione periodi contributivi versati presso altre casse;
16) Pratiche riscatto a fini pensionistici e/o indennità di fine servizio;
17) Pratiche in caso di morte di dipendenti;
18) Redazione denuncia annuale ai sensi della L. 68/99;
19) Gestione cessioni di quote di stipendio personale dipendente;
20) Gestione pratiche sovvenzioni dietro cessione del quinto, personale dipendente;
21) Gestione amministrativa ed economica dei volontari del Servizio civile Nazionale e regionale;
22) Gestione assistenza fiscale CAAF esterni (mod 730)

23) Redazione della denuncia annuale fiscale e contributiva (Mod. 770);
24) Redazione denuncia annuale e autoliquidazione posizioni INAIL;
25) Alte pratiche INAIL (ad es. malattie professionali, questionari INAIL, infortuni, ecc.);
26) Redazione certificazioni fiscali (mod. CU);
27) Redazione denuncia annuale ONAOSI;
28) Pratiche per l'attribuzione del trattamento pensionistico e suo aggiornamento;
29) Pratiche per l'erogazione del trattamento di fine servizio;
30) Verifiche emissione ruoli contributivi arretrati INPS;
31) Gestione archivi informatici anagrafica, formazione, situazione sanitaria a fini statistici interni.

Quanto al trattamento ***sub*** **c) Rapporti con soggetti interni** - si precisa che esso comporta:
1) L'istruzione e la predisposizione di delibere del Consiglio di Amministrazione e di determine della Dirigenza;
2) Posizione di staff rispetto a vari adempimenti d'Istituto;
3) Elaborazione di dati e statistiche a supporto della direzione;
4) Predisposizione previsione di spesa del personale del Bilancio annuale.

Quanto al trattamento ***sub*** **d) Rapporti con soggetti esterni** - precisa che esso comporta:
1) Relazioni con R.S.U. e O.O.SS territoriali;
2) Attività di sportello di informazione al pubblico;
3) Rapporti con cooperative per servizi sostitutivi di personale;
4) Vari rapporti con Enti previdenziali/assicurativi/ EELL/Ministeriali/ARAN ecc;
5) Procedure elezione R.S.U.;
6) Pratiche risarcimento danni causati da terzi;
7) Redazione ed emissione certificazioni varie;
8) Gestione procedimenti disciplinari.

Quanto al trattamento **sub e) Adempimenti in materia di sicurezza nei luoghi di lavoro**
1) Visite mediche preassuntive e periodiche;
2) Rapporti con il medico competente;
3) Formazione obbligatoria.

Quanto al trattamento ***sub*** **f) Varie** - si precisa che esso si sostanzia nella:
1) Determinazione monte ore permessi sindacali;
2) Gestione permessi sindacali;
3) Attività di aggiornamento studio e ricerca;
4) Archiviazione dati e pratiche varie;
5) Gestione corrispondenza postale telematica e telefonica;
6) Tenuta scadenzari vari.

Incaricati
UFFICIO RISORSE UMANE – SEGRETERIA/AFFARI GENERALI – AREA TECNICA - UFFICIO ORGANIZZAZIONE DEL PERSONALE
Collaboratori esterni incaricati degli adempimenti amministrativi, retributivi, contributivi, fiscali e di sicurezza sul lavoro.

Destinatari
I dati possono essere comunicati a consulenti esterni nei limiti delle finalità contabili, fiscali e di tutela legale, nonché di ogni altra finalità indicata alla lett. A) in tutte le specificazioni di cui sopra, ovvero alle competenti autorità per l'adempimento degli obblighi di legge.
Si precisa inoltre che AltaVita-IRA può rivolgersi ad Enti pubblici o privati, soggetti o società esterne a cui far pervenire i dati necessari per l'espletamento delle attività di costituzione e/o gestione del rapporto di lavoro, tra i quali in particolare: l'Amministrazione finanziaria, Enti previdenziali ed assistenziali, Enti del SSN, Istituti di credito, Organizzazioni rappresentative dei lavoratori, medici competenti per la sicurezza sul lavoro e laboratori di analisi e diagnostica, società che forniscono prodotti informatici e relativa assistenza, altri soggetti cui la normativa in vigore o impegni contrattuali prevedono l'obbligo di comunicazione.

Trasferimento dei dati
Non si effettua né si effettueranno trasferimento di dati verso paesi Extra UE.

TRATTAMENTO DEI DATI AREA OSPITI E AREA ACQUISTI

Base Giuridica
Il trattamento dei dati degli Ospiti, Obbligati principali e coobbligati, viene effettuato per consentire ad AltaVita-IRA di adempiere correttamente e completamente agli obblighi di legge derivanti dal fornire ospitalità e assistenza e ogni altro servizio ad esso connesso o comunque richiesto o che può essere fornito, nonché per finalità contabili, fiscali, di tutela legale, socio-sanitarie e sanitarie.

Tempi di conservazione e di cancellazione
I dati vengono trattati secondo le disposizioni consultabili all'interno del Piano di Conservazione, ovvero per un periodo di tempo illimitato. Per l'area acquisti il tempo di conservazione varia a seconda della tipologia di procedura: illimitato per aste, gare, appalti/aggiudicazioni e relativi contratti, quinquennale per fornitura, acquisizione, gestione, alienazione beni mobili, quinquennale per manutenzione beni mobili.

Modalità di Trattamento dei dati personali e particolari degli Interessati (Ospiti)
Il trattamento viene effettuato per consentire, nei termini che verranno di seguito meglio specificati: a) la gestione delle rette degli Ospiti; b) la riscossione delle rette di ospitalità; c) la gestione delle pensioni degli Ospiti; d) la gestione dei rapporti di locazione e di affitto, e) la gestione di fornitori, professionisti e collaboratori.

AREA OSPITI

Quanto al trattamento ***sub* a) Gestione rette Ospiti** si precisa che:
1) Ad ogni ingresso deve attivarsi una posizione anagrafico/contabile dell'Ospite in cui indicarsi oltre i dati anagrafici, lo stato civile, il numero di tessera sanitaria e C.F., l'eventuale sottoposizione dell'Ospite a tutela, curatela o ad amministrazione di sostegno (in tal caso sarà necessario indicare specificamente i poteri dell'Amministratore di sostegno di cui al decreto di nomina), l'ammontare della retta applicata, il soggetto tenuto al pagamento della stessa. I dati devono essere tempestivamente aggiornati ad ogni variazione;
2) Entro la scadenza di ogni mese devono essere registrati tutti i movimenti in uscita ed entrata degli Ospiti (permessi e ricoveri ospedalieri), il cambiamento dell'autosufficienza in non autosufficienza e vengono imputati eventuali costi extra retta;
3) All'inizio del mese si procede alla rendicontazione delle impegnative di residenzialità, all'ULSS di competenza, secondo quanto previsto dalla convenzione vigente e alla successiva emissione delle fatture;
4) Per quanto riguarda gli Ospiti Non Autosufficienti, all'inizio di ciascun mese, viene trattato il tabulato degli Ospiti presenti, suddivisi per livello assistenziale e per centro servizi e con indicazione dei seguenti dati: nominativo dell'Ospite, presenze e assenze (per ricovero ospedaliero o per permesso), data di cessazione (decesso, dimissione o trasferimento), indicazione del medico curante;
5) Periodicamente vengono elaborate delle statistiche di organizzazione interna (copertura posti letto, età media degli Ospiti, maschio o femmina, ecc.);
6) Ad ogni uscita definitiva si provvede alla chiusura contabile della scheda dell'Ospite ed alla restituzione del deposito cauzionale degli Ospiti paganti in proprio.

Quanto **ai trattamenti derivanti dall'attività di assistenza e ospitalità,** si precisa inoltre che:
- l'Assistente Sociale provvede specificamente all'inserimento dell'Ospite, a partire dall'accoglimento, nonché a garantire il sostegno sociale dello stesso e allo svolgimento delle pratiche di tipo amministrativo che lo interessano (domande di invalidità, richieste di ausilii, domande pensionistiche ecc.);
- il Capo Reparto coordina e vigila sulle attività degli Infermieri, degli Operatori Addetti all'Assistenza e degli Operatori di Appoggio ai Servizi Istituzionali, secondo la procedura di erogazione dei servizi di assistenza globale. Custodisce, inoltre, la Cartella Personale dell'Ospite;
- l'Educatore Professionale /Animatore cura la formulazione e l'attuazione di progetti educativi e animativi caratterizzati da intenzionalità e continuità, volti a promuovere e contribuire al massimo sviluppo delle potenzialità dell'ospite secondo la procedura del servizio educativo - animativo;
- il Fisioterapista opera secondo la procedura del servizio di riabilitazione con l'obiettivo di migliorare la qualità di vita degli ospiti non autosufficienti mediante l'attivazione e il potenziamento delle capacità residue, il mantenimento del massimo grado di autonomia possibile, la limitazione dei danni dovuti all'immobilizzazione e all'inattività fisica e mentale, il mantenimento dell'autostima, la stimolazione delle capacità di relazione interpersonale e di percezione psicomotoria;
- lo specialista in Scienze Motorie svolge attività per prevenire complicanze e mantenere o migliorare lo stato psico-fisico della persona negli atti quotidiani della vita;
- l'Infermiere Professionale svolge attività di assistenza infermieristica secondo le indicazioni mediche e la procedura di erogazione dei servizi di assistenza globale;
- il Logopedista si occupa dei disturbi della voce, della parola, del linguaggio orale e scritto (lettura e scrittura),

della comunicazione e dei disturbi della deglutizione nell'ambito dell'età adulta e anziana. A tale scopo pratica autonomamente, in relazione alla diagnosi e alla prescrizione del medico, l'attività terapeutica per la rieducazione funzionale delle abilità comunicative e cognitive;
- il Medico svolge l'attività regolata dalla convenzione con l'ULSS e dalla procedura di erogazione dei servizi di assistenza globale. In particolare monitora gli Ospiti, effettua la valutazione medica, prescrive la terapia farmacologica, gli esami, le visite specialistiche, partecipa alla formulazione dei progetti personalizzati sull'Ospite (piano assistenziale individualizzato). Tiene, inoltre, aggiornata la documentazione sanitaria contenuta nella Cartella Personale dell'Ospite e verifica gli aggiornamenti dell'Unità Operativa interna;
- lo Psicologo si occupa dell'assistenza psicologica degli Ospiti e delle famiglie che sono in difficoltà nella gestione della relazione con l'Ospite, fornisce consulenza e effettua attività di supervisione psicologica agli operatori in conformità alla procedura di servizio psicologico.

Quanto al trattamento ***sub* b) Riscossione rette di ospitalità** - si precisa che esso comporta:
1) La gestione mensile del flusso dei pagamenti delle rette tramite addebito SEPA-SDD (ex RID);
2) L'emissione dell'ordinativo di incasso a fronte dei provvisori di entrata registrati sul giornale di cassa del Tesoriere/Cassiere dell'Istituto;
3) Individuazione delle rette non ancora saldate con ritardo superiore ai trenta giorni e invio di sollecito all'ospite e/o all'impegnato al pagamento; in caso di esito negativo, la pratica verrà trasmessa al legale dell'Ente.

Quanto al trattamento ***sub* c) Gestione pensioni Ospiti** si precisa che esso comporta:
1) Nel caso di accoglimento di ospiti con integrazione economica della retta da parte dei Comuni, l'ospite (o il tutore o l'amministratore di sostegno) delega Segretario-Direttore Generale pro-tempore, alla riscossione delle pensioni e viene attivata la posizione anagrafico/contabile che comprende tutti i dati necessari per la gestione delle pensioni di cui è titolare l'Ospite;
2) Tale delega, da rendersi da parte dei soggetti di cui al punto precedente in sede di accettazione, riguarda l'apertura di un c/c bancario, senza spese e interessi, e la comunicazione all'Ente pensionistico del cambiamento delle modalità di riscossione;
3) Mensilmente il Tesoriere/Cassiere invia al Segretario-Direttore Generale pro-tempore il tabulato delle pensioni da riscuotere, che deve essere aggiornato dall'ufficio competente con indicazione degli eventuali decessi, dimissioni e/o trasferimento presso altra struttura;
4) Le pensioni vengono accreditate sul conto di tesoreria di AltaVita-IRA che provvede alla regolarizzazione con emissione di ordinativo di incasso e alla registrazione contabile sui rispettivi conti contabili. La quota per spese vita di relazione che i Comuni lasciano agli Ospiti viene accreditata nel deposito fiduciario nominativo;
5) Mensilmente vengono elaborate le stampe di riepilogo delle pensioni riscosse a scomputo della retta di ospitalità, da fatturare ai Comuni;
6) In caso di decesso o dimissione o trasferimento presso altra struttura, si procede alla chiusura contabile.

Quanto al trattamento ***sub* d) Gestione rapporti di locazione e di affitto** - si precisa che esso si concreta nella:
1) Riscossione di canoni di locazione, fitti e registrazione su scheda contabile individuale;
2) Rendicontazione semestrale e/o annuale delle anticipazioni di spesa effettuate a favore dei conduttori e fittavoli (utenze, pulizie, riscaldamento, ascensore, ecc.);
3) Corrispondenza varia, solleciti di pagamento, contenzioso.

AREA ACQUISTI

Quanto al trattamento ***sub* e) Gestione fornitori, professionisti e collaboratori** - si precisa che:
1) Per ogni fornitore, professionista o collaboratore viene attivata una scheda anagrafica contenente i dati anagrafici e l'indicazione delle modalità di pagamento;
2) Ogni fattura viene registrata e imputata alla contabilità generale e successivamente inviata all'Ufficio competente per la sua liquidazione;
3) Le fatture liquidate e complete di tutti i dati necessari (economia o contratto, provvedimento di liquidazione, registrazione della spesa, importo liquidato, firma di chi ne attesta la regolarità) vengono evase attraverso l'emissione di ordinativi di pagamento per il Tesoriere/Cassiere dell'Istituto.

Il trattamento viene effettuato con modalità informatizzate e manuali, i dati verranno conservati negli archivi informatici e cartacei di AltaVita-Istituzioni Riunite di Assistenza-IRA, siti in Piazzale Mazzini 14, 35137 Padova, e nelle strutture assistenziali, nel rispetto delle prescrizioni del Regolamento 679/2016 UE.

I dati potranno essere comunicati a consulenti esterni nei limiti delle finalità contabili, fiscali e di tutela legale, nonché di ogni altra finalità indicata nelle modalità di trattamento, in tutte le specificazioni di cui sopra, ovvero alle competenti autorità per l'adempimento degli obblighi di legge.

Si precisa inoltre che AltaVita-IRA può rivolgersi ad Enti pubblici o privati, soggetti o società esterne a cui far pervenire i dati necessari per l'espletamento delle attività di ospitalità e assistenza, tra i quali in particolare: Enti previdenziali ed assistenziali, Enti del SSN, Istituti di credito, medici, società che forniscono prodotti informatici e relativa assistenza, consulenti incaricati dall'amministrazione, altri soggetti cui la normativa in vigore o impegni contrattuali prevedono l'obbligo di comunicazione.

Incaricati
UFFICIO ACQUISTI, CONTABILITA' E BILANCIO-SERVIZIO ASSISTENZIALE/SERVIZIO SOCIALE-UFFICIO ORGANIZZAZIONE DEL PERSONALE – AREA TECNICA
Collaboratori esterni incaricati degli adempimenti amministrativi, retributivi, contributivi, fiscali e di sicurezza sul lavoro. Dipendenti e collaboratori addetti all'assistenza ed all'organizzazione lavorativa e contabile.

Destinatari
I dati possono essere comunicati a consulenti esterni nei limiti delle finalità contabili, fiscali e di tutela legale, nonché di ogni altra finalità indicata in tutte le specificazioni di cui sopra, ovvero alle competenti autorità per l'adempimento degli obblighi di legge. Enti previdenziali e assicurativi necessari per contratto, parenti o tutori.

Trasferimento dei dati
Non si effettua né si effettueranno trasferimento di dati verso paesi Extra UE.

TRATTAMENTO DEI DATI AREA TECNICO PATRIMONIALE

BASE GIURIDICA DEL TRATTAMENTO
I dati personali indicati sono trattati dal Titolare nell'esecuzione dei propri compiti di interesse privato e pubblico o comunque necessari all'assolvimento degli obblighi di legge.
In particolare il trattamento viene effettuato per consentire, nei termini che verranno di seguito meglio specificati: a) l'instaurazione e gestione dei rapporti con i fornitori; b) l'instaurazione e gestione degli appalti di LL. PP.; c) l'instaurazione e gestione dei rapporti di locazione e di affitto; d) l'affidamento e la gestione di incarichi professionali e l'instaurazione e gestione di contratti d'opera; e) la sorveglianza sanitaria per la sicurezza sul lavoro a norma di Legge e dei rapporti consequenziali.

Tempi di conservazione e distruzione
I dati vengono trattati secondo le disposizioni consultabili all'interno del Piano di Conservazione approvato, ossia 5 anni per gli adempimenti fiscali, 10 anni per gli adempimenti contrattuali e durata illimitata per attività connesse alla sorveglianza sanitaria per la sicurezza sul lavoro.

Modalità di Trattamento
Il trattamento dei dati dei propri fornitori, professionisti, inquilini, fittavoli e controparti in genere, verrà effettuato per consentire ad AltaVita-Istituzioni Riunite di Assistenza - IRA di adempiere correttamente e completamente alle obbligazioni derivanti dalla stipula dei contratti di fornitura di beni e servizi, in particolare alla liquidazione di eventuali fatture, nonché per finalità contabili, fiscali e di tutela legale.
Quanto al trattamento ***sub* a) e b) - instaurazione e gestione dei rapporti con i fornitori;** si precisa che:
1) Per ogni fornitore, professionista o collaboratore viene attivata una scheda anagrafica, analogica o digitale, contenente i dati anagrafici e l'indicazione delle modalità di pagamento;
2) Ogni fattura viene registrata e imputata alla contabilità generale e successivamente inviata all'Ufficio competente per la sua liquidazione;
3) Le fatture liquidate e complete di tutti i dati necessari (economia o contratto, registrazione della spesa, provvedimento di liquidazione, firma del Responsabile che ne attesta la regolarità) vengono evase attraverso l'emissione di ordinativi di pagamento tratti sull'Istituto bancario dell'Ente.
4) per ogni partecipante a qualsiasi procedura di gara vengono raccolti dati personali ai sensi della normativa vigente in materia di appalti e normativa ad essa collegata.

Quanto al trattamento ***sub* c) – instaurazione e gestione dei rapporti di locazione e di affitto** si precisa che esso si concreta nella:

1) Stipula dei contratti di locazione di immobili urbani e terreni agricoli;
2) Rendicontazione semestrale e/o annuale delle anticipazioni di spesa effettuate a favore dei conduttori e fittavoli (utenze, pulizie, riscaldamento, ascensore, ecc.);
3) Corrispondenza varia, solleciti di pagamento, contenzioso;
4) Verifica di documentazione personale (anagrafica, economica);
5) Piano di Valorizzazione del Patrimonio di cui alla DGRV n. 780/2013.

I dati possono essere comunicati a consulenti esterni nei limiti delle finalità contabili, fiscali e di tutela legale,

nonché di ogni altra finalità indicata nelle modalità di trattamento, in tutte le specificazioni di cui sopra ovvero a soggetti o alle competenti autorità per l'adempimento di obblighi contrattuali o di legge. In particolare potrà esservi la comunicazione di dati all'Osservatorio Regionale e al Ministero delle Infrastrutture e Trasporti e all'ANAC (Autorità Nazionale Anticorruzione).

Incaricati
UFFICIO ACQUISTI, CONTABILITA' – AREA TECNICA
Collaboratori esterni incaricati degli adempimenti amministrativi, retributivi, contributivi, fiscali e di sicurezza sul lavoro. Dipendenti e collaboratori addetti all'assistenza ed all'organizzazione lavorativa e contabile.

Destinatari
I dati possono essere comunicati a consulenti esterni nei limiti delle finalità contabili, fiscali e di tutela legale, nonché di ogni altra finalità indicata in tutte le specificazioni di cui sopra, ovvero alle competenti autorità per l'adempimento degli obblighi di legge. Enti previdenziali e assicurativi necessari per contratto, parenti o tutori.

Trasferimento dei dati
Non si effettua né si effettueranno trasferimento di dati verso paesi Extra UE.

TRATTAMENTO DI DATI PERSONALI DI CLIENTI, OSPITI, LAVORATORI E COLLABORATORI	
FINALITÀ	***VIDEOSORVEGLIANZA AI FINI DI PROTEZIONE DELLE PERSONE, DELLA PROPRIETÀ E DEL PATRIMONIO AZIENDALE***
Interessati	*Clienti, ospiti, lavoratori, collaboratori e fornitori*
Base giuridica	*Perseguimento di un legittimo interesse del titolare, per fini di tutela delle persone e dei beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo e per finalità di prevenzione incendi e di sicurezza del lavoro*
Incaricati	*AREA TECNICA – SERVIZI ASSISTENZIALI/SERVIZIO SOCIALE* *Responsabili e incaricati preposti ed identificati* *Addetti alla sicurezza*
Categorie di dati personali	*Immagini*
Destinatari	*Addetti alla sicurezza - Forze dell'ordine*
Trasferimento verso paesi extraUE	*No (X) Si ( )*
Termini di cancellazione	*Termini indicati nell'allegato 1.1. D.P.I.A.*

Risorse Hardware

Le risorse hardware utilizzate per trattare i dati personali sono qui elencate ex Art.32:

Numero Personal computer/ Server (o terminali)	Sistemi operativi utilizzati	Sistemi di backup adottati e sicurezza (Ex Art.25 C.1-2)
4 Server fisici (dominio + gestionali + condivisioni) 88 personal computer desktop 4 notebook Dati su SAN in Fiber Channel	• Microsoft Windows Server 2012 R2 • Microsoft Windows 7 Professional SP1 e 10 Professional per client Settori amministrativi. • Microsoft Windows 7 Professional SP1 e alcuni XP Professional SP3 per client Settori Sanitari • Microsoft Windows 7 Professional SP1 e alcuni XP Professional SP3 per Settori Servizi	Server fisici configurati in raid 5-6 o 10. I server fisici sono protetti da adeguati gruppi di continuità che proteggono anche la rete telematica (centralini). Per il Backup viene utilizzato VEEAM e si attiva su Storage Loader LTO 3 e NAS con HD in raid. Antivirus Kaspersky Server ogni PC client regolarmente licenziati, con console centralizzata di gestione e monitoraggio gestite dai responsabili esterni incaricati dell'assistenza sistemistica; Firewall hardware per la protezione della rete locale lan, e per la gestione delle connessioni VPN per gli utenti remoti se attivati. Ogni connessione VPN è nominativa. Tutti gli utenti hanno un profilo che consente loro di accedere solo ai dati per i quali sono autorizzati e le relative password hanno scadenza a 90 giorni con l'obbligo di utilizzare almeno 8 caratteri alfanumerici e caratteri speciali.

I PC con sistema operativo Windows Professional SP1 dovranno essere sostituiti entro il 31 dicembre 2020.
Si prevede un TEST per il Disaster Recovery con cadenza annua da effettuarsi sotto la supervisione del Responsabile esterno al fine di verificare l'efficienza della rete e la disponibilità del dato.

Analisi generale dei rischi

Evento		Impatto sulla sicurezza dei dati		Contromisure
Comportamento degli operatori		Descrizione	Gravità Stimata	
	Furto di credenziali di autenticazione	Le password potrebbero essere rubate	BASSA	L'accesso agli elaboratori è protetto da password con cambio automatico richiesto dal sistema.
	Carenza di consapevolezza, disattenzione o incuria	I dati potrebbero essere utilizzati erroneamente	MEDIA	Non tutti gli incaricati al trattamento sono stati edotti sulle responsabilità e sui rischi relativi al trattamento dati.
	Comportamenti fraudolenti	Sottrazione di dati Da parte di dipendenti/ collaboratori	MEDIA	Le periferiche di memorizzazione esterna non sono disabilitate ed esiste un sistema di tracking degli accessi ai dati.
	Errore umano	cancellazione	MEDIA	La presenza di un backup giornaliero automatizzato anche se datato, con conservazione in-site dei supporti, fornisce una buona garanzia di ripristino di dati erroneamente cancellati. Un secondo sistema di backup aumenterebbe la sicurezza.
Eventi relativi agli strumenti	Azione di Malicious Code	Il sistema potrebbe essere infettato da virus	BASSA	La presenza di un software antivirus di classe professionale su Server, gestito e monitorato da struttura esterna, riduce al minimo il rischio di infezione.
	Spamming	Eccessiva posta spazzatura potrebbe bloccare la casella di posta	BASSA	La posta elettronica viene gestita, che integra un efficace servizio antispam.
	Malfunzionamento degli strumenti	Gli elaboratori potrebbero non funzionare correttamente	MEDIO ALTA	Esiste un contratto di assistenza per l'intervento on site e la riparazione. Vi sono ancora nella rete PC con S.O. obsoleto e pericoloso.
	Accessi esterni non autorizzati	Un Hacker potrebbe introdursi Sfruttando il collegamento xDSL	BASSA	La presenza di un firewall hardware, e di connessioni VPN monitorate e nominative, riduce sensibilmente il rischio di accessi non autorizzati.
Eventi relativi al contesto	accessi non autorizzati a locali/reparti ad accesso ristretto	Accesso a locali non consentito	BASSA	I locali sono controllati da personale addetto e da sistema di accesso controllato. Esiste inoltre un sistema antintrusione, oltre a un sistema di videosorveglianza oi ogni sede e unità locale.
	eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Incendio, furto, inondazione, ecc.	MEDIA	L'azienda ha una copertura assicurativa sui danni accidentali, il furto, l'incendio e la responsabilità civile.

Criteri e procedure per il ripristino della disponibilità dei dati

Salvataggio Database	Dati Contenuti	Procedure operative per il salvataggio	Ubicazione di conservazione delle copie	Struttura operativa incaricata del salvataggio
CONT	Contabilità	Backup policy	Sala server	Incaricati backup
MAIL	Posta Elettronica	Backup policy	Sala server	Incaricati backup
MKTG	Marketing	Backup policy	Sala server	Incaricati backup
CLIENTI	Archivio Clienti	Backup policy	Sala server	Incaricati backup
FORN	Archivio Fornitori	Backup policy	Sala server	Incaricati backup

Pianificazione degli interventi formativi previsti

Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di incaricati interessati	Tempi previsti
Fornire le conoscenze fondamentali sul GDPR 679/2016 "General Data Protection Regulation" o Regolamento Europeo.	Titolare Responsabile Incaricati Responsabile sistemi informativi	Entro dicembre 2019
Fornire conoscenze e competenze per affrontare le tematiche sulla gestione dei sistemi informativi aziendali in relazione alle più recenti normative in tema di trattamento dei dati.	Responsabile sistemi informativi	Entro dicembre 2019

Registro dei Trattamenti

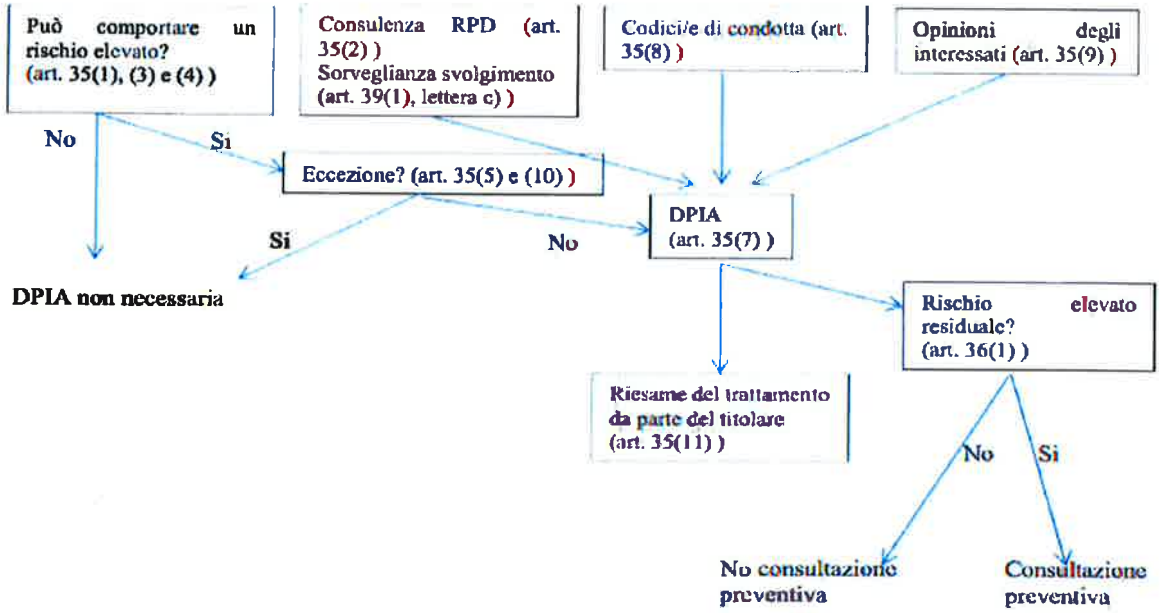
ALLEGATO 1.1

D.P.I.A.

Data Privacy Impact Analisys

Videosorveglianza

D.P.I.A. Data Privacy Impact Analisys
Videosorveglianza



Tipo di trattamento.Art.35.1

Dati raccolti su Impianti di registrazione immagini (DVR).

Impatto Art.35.3

La videosorveglianza sistematica su larga scala di una zona accessibile al pubblico può comportare un rischio per gli interessati se vi fosse la possibilità di utilizzare i dati per fini non dichiarati e leciti.

Valutazione Art.35.7

La finalità del trattamento è aumentare il livello di sicurezza delle Unità Locali sottoelencate e proteggere gli ospiti ed il personale:
"CENTRO SERVIZI BEATO PELLEGRINO" sito in Via Beato Pellegrino, 192 a Padova 35137
"Pensionato Piaggi" sito in Piazzale Mazzini, 16 a Padova 35137,
"Centro Servizi Palazzo Bolis" sito in Piazza Beatrice De Claricini, 12 a Selvazzano Dentro (Padova) 35030,
e nelle aree di seguito descritte.
Tutti i sistemi sono stati autorizzati dal Dipartimento Territoriale del Lavoro di Padova e sono quindi rispettosi del Provvedimento del Garante in materia di videosorveglianza - 8 aprile 2010 e dell'Ar.4 L.300/1970 definito come statuto dei lavoratori.

"CENTRO SERVIZI BEATO PELLEGRINO"
Autorizzazione installazione da parte del Dipartimento Territoriale del Lavoro di Padova n. 3135 del 01.02.2017.
Il personale di portineria è il personale incaricato del trattamento dei dati.
Il sistema attualmente non prevede la videoregistrazione e non consente l'accesso remoto alla visione.

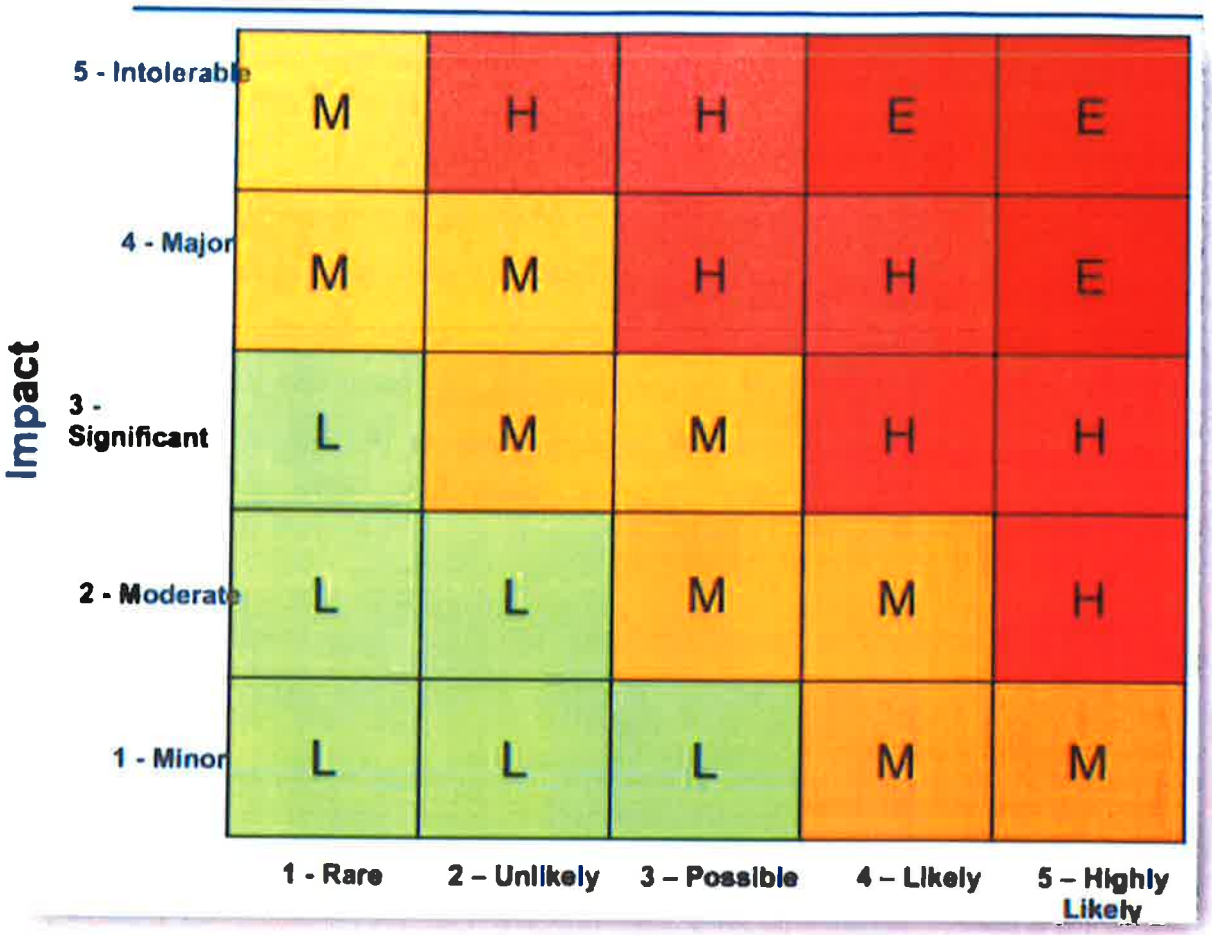
Telecamere:3 dotate di ottica fissa che insistono sugli accessi alla struttura: ingresso pedonale e 2 passi carrai.
Video e sistema: 1 pc con monitor per visualizzazione in diretta delle immagini collocato presso il bancone portineria atrio di ingresso piano terra ad uso esclusivo dei portieri per il monitoraggio accessi.
1 dispositivo di registrazione dotato di monitor necessario per il funzionamento dell'impianto. La registrazione delle immagini è bloccata.

"Centro Servizi Palazzo Bolis"
Autorizzazione del 29.12.2016 con provvedimento prot. 43406 del 29.12.2016 da parte del Dipartimento Territoriale del Lavoro di Padova.
Immagini vengono registrate per 24 H.
Referenti con accesso alle immagini registrate a doppia chiave e password:
per Altavita: dott.ssa Mazzucato Micaela in rappresentanza della Direzione e dott.ssa Dal Ben Sara in rappresentanza dei lavoratori.
per Lunazzurra (Responsabile Esterno designato): Sig. Gobbo Denis in rappresentanza della Direzione e sig.ra Turchetto Lucia in rappresentanza dei propri lavoratori.
Telecamere: 6 a copertura del perimetro esterno e 3 interne posizionate in aree di accesso.
Video
1 pc dotato di monitor per la sola visualizzazione delle immagini in tempo reale posizionato sul bancone della portineria nell'atrio di ingresso piano terra.
1 dispositivo di registrazione dotato di monitor posizionato nel locale "reti" interrato della struttura.
"Pensionato Piaggi"
Autorizzazione n. 3744 del 06.02.2015 annullata e sostituita da n. 15236 del 22.05.2017 da parte del Dipartimento Territoriale del Lavoro di Padova.
Le immagini vengono registrate e conservate per 24 H.
Referenti con accesso alle immagini registrate a doppia chiave e password:
per Altavita: Dott.ssa Arsie per datore di lavoro e Sig. Menegon Paolo in rappresentanza dei lavoratori;
per S.C.Società Cooperativa(Responsabile Esterno designato):Sig.ra Baldo Flavia in rappresentanza dei lavoratori.
Telecamere:4 esterne a copertura del perimetro della struttura e del giardino e 9 telecamere interne posizionate negli accessi ai vari reparti (le telecamere interne sono state conteggiate escludendo quelle ubicate al 4° e 5° piano destinati a Casa Vacanze).
Video: 1 DVR 4 ingressi, 1 monitor 19", 1 monitor 32"di sola visualizzazione e 1 sistema di registrazione. Collocati all'interno dell'area di controllo degli accessi presso Portineria Pensionato.

Rivalutazione Art.35.11

Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

Esempio di valutazione adottata



LEGENDA:

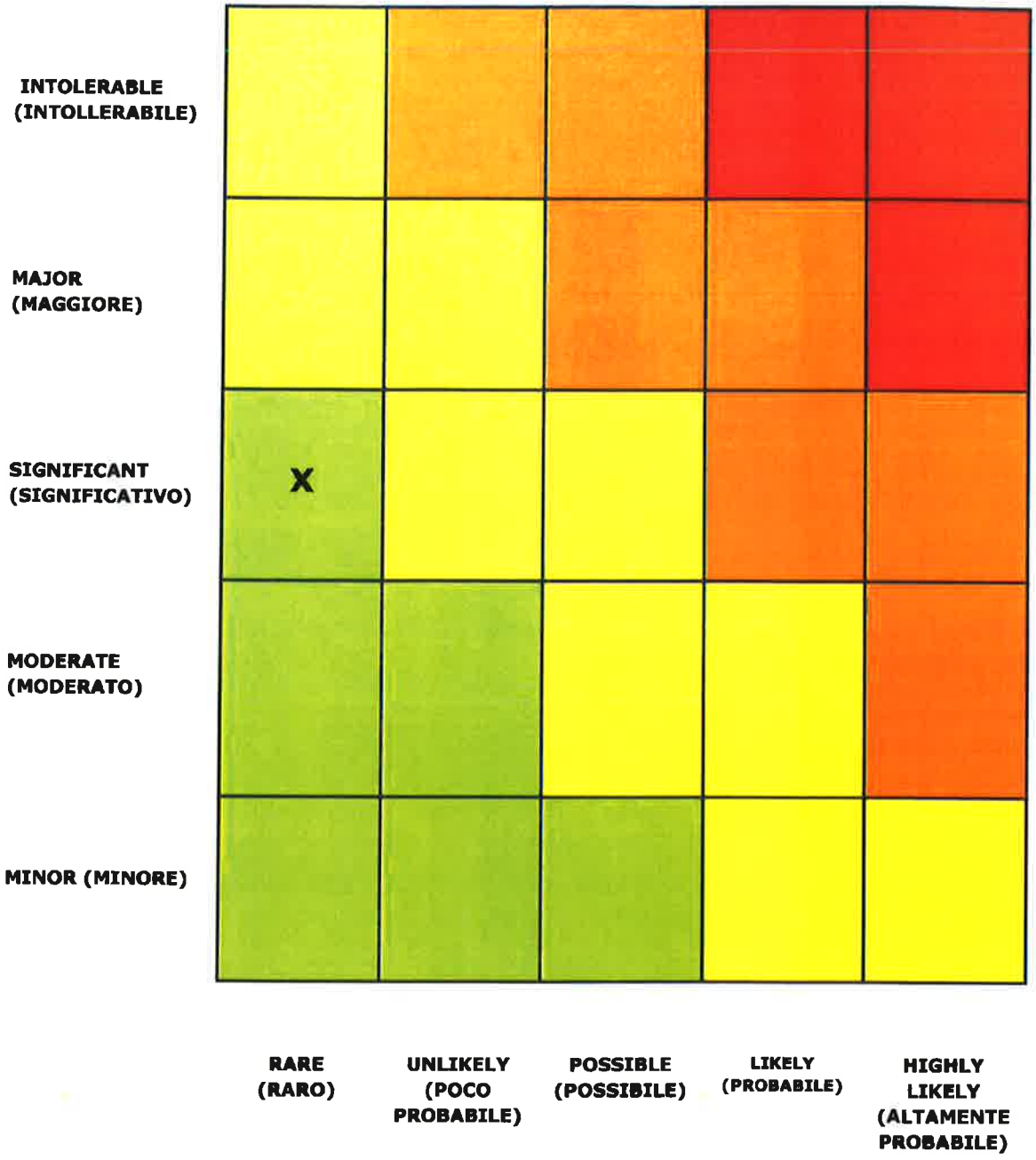
L = LOW (BASSO)

M = MEDIUM (MEDIO)

H = HIGH (ALTO)

E = EXPLOSIVE (DISASTROSO)

Risultante della valutazione



Dall'analisi effettuata e dai sistemi adottati il trattamento effettuato risulta Significativo per quanto attiene il livello di rischio e Raro per quanto attiene la possibilità di reiterazione di un trattamento illecito.

Non si ritiene necessario procedere ad una Rivalutazione ex Art.35.11

Registro dei trattamenti

ALLEGATO 2

Manuale per la sicurezza e Privacy policy

Questo documento fornisce agli autorizzati del trattamento elementi di conoscenza utili ad individuare le responsabilità loro spettanti, rispetto alla gestione ed allo sviluppo della sicurezza dell'informazione. Nell'ambito informatico, il termine "sicurezza" si riferisce a tre aspetti distinti:

Riservatezza: Prevenzione contro l'accesso non autorizzato alle informazioni;
Integrità: Le informazioni non devono essere alterabili da incidenti o abusi;
Disponibilità: Il sistema deve essere protetto da interruzioni impreviste.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi; misure soltanto tecniche, per quanto possano essere sofisticate, non saranno efficienti se non usate propriamente.
In particolare, le precauzioni di tipo tecnico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

Linee guida per la sicurezza

1. **UTILIZZATE LE CHIAVI!**
   Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio alla fine della giornata e chiudete i documenti a chiave nei cassetti ogni volta che potete.

2. **CONSERVATE I SUPPORTI IN UN LUOGO SICURO**
   Per i supporti si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. A meno che non siate sicuri che contengano solo informazioni non sensibili, riponeteli sotto chiave non appena avete finito di usarli.

3. **UTILIZZATE LE PASSWORD**
   Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:
   - La password di accesso al computer impedisce l'utilizzo improprio della vostra postazione, quando per un motivo o per l'altro non vi trovate in ufficio.
   - La password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ufficio.
   - La password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato.
   - La password del salvaschermo, infine, impedisce che una vostra assenza momentanea permetta a una persona non autorizzata di visualizzare il vostro lavoro.

   Imparate a utilizzare questi quattro tipi fondamentali di password, e mantenete distinta almeno quella di tipo *a*, che può dover essere resa nota, almeno temporaneamente, ai tecnici incaricati dell'assistenza. Scegliete le password secondo le indicazioni della sezione successiva.

4. **ATTENZIONE ALLE STAMPE DI DOCUMENTI RISERVATI**
   Non lasciate accedere alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania recatevi quanto prima a ritirare le stampe. Distruggete personalmente le stampe quando non servono più.

5. **NON LASCIATE TRACCIA DEI DATI RISERVATI**
   Quando rimuovete un file, i dati non vengono effettivamente cancellati ma soltanto marcati come non utilizzati, e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei dati; solo l'utilizzo di un programma apposito garantisce che sul supporto non resti traccia dei dati precedenti. Nel dubbio, è sempre meglio usare un supporto nuovo.

6. **PRESTATE ATTENZIONE ALL'UTILIZZO DEI PC PORTATILI**
   I PC portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido, e utilizzate una procedura di backup periodico.

7. **NON FATEVI SPIARE QUANDO STATE DIGITANDO LE PASSWORD**
   Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura.

8. **CUSTODITE LE PASSWORD IN UN LUOGO SICURO**
   Non scrivete la vostra password, meno che mai vicino alla vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria. Se avete necessità di conservare traccia delle password per scritto, non lasciate in giro i fogli utilizzati.

9. **NON FATE USARE IL VOSTRO COMPUTER A PERSONALE ESTERNO A MENO DI NON ESSERE SICURI DELLA LORO IDENTITÀ**
   Personale esterno può avere bisogno di installare del nuovo software/hardware nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro PC.

10. **NON UTILIZZATE APPARECCHI NON AUTORIZZATI**
    L'utilizzo di modem su postazioni di lavoro collegati alla rete offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la rete ed è quindi vietata. Per l'utilizzo di altri apparecchi, consultatevi con il Referente di Area.

11. **NON INSTALLATE PROGRAMMI NON AUTORIZZATI**
    Solo i programmi acquistati dal titolare con regolare licenza sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici, consultatevi con il Referente di Area.

12. **APPLICATE CON CURA LE LINEE GUIDA PER LA PREVENZIONE DA INFEZIONI DI VIRUS**
    La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati.

13. **CONTROLLATE LA POLITICA LOCALE RELATIVA AI BACKUP**
    I vostri dati potrebbero essere gestiti da un *file server*, oppure essere gestiti in locale e trasferiti in un server solo al momento del backup. Verificate con il personale locale la situazione.

Linee guida per la prevenzione dei virus

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

COME SI TRASMETTE UN VIRUS:

1. Attraverso programmi provenienti da fonti non ufficiali;
2. Attraverso le macro dei programmi di automazione d'ufficio.

COME *NON* SI TRASMETTE UN VIRUS:

1. Attraverso file di dati non in grado di contenere macro (file di testo, html, pdf, ecc.);
2. Attraverso mail non contenenti allegati.

QUANDO IL RISCHIO DA VIRUS SI FA SERIO:

1. Quando si installano programmi;
2. Quando si copiano dati da supporti;
3. Quando si scaricano dati o programmi da Internet.

QUALI EFFETTI HA UN VIRUS?

1. Effetti sonori e messaggi sconosciuti appaiono sul video;
2. Nei menù appaiono funzioni extra finora non disponibili;
3. Lo spazio disco residuo si riduce inspiegabilmente;

COME PREVENIRE I VIRUS:

14. **USATE SOLTANTO PROGRAMMI PROVENIENTI DA FONTI FIDATE**
    Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzate programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.

15. **ASSICURATEVI DI NON FAR PARTIRE ACCIDENTALMENTE IL VOSTRO COMPUTER DA SUPPORTO**
    Infatti, se il supporto fosse infettato, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri files.

16. Proteggete i vostri supporti da scrittura quando possibile

In questo modo eviterete le scritture accidentali, magari tentate da un virus che tenta di propagarsi. I virus non possono in ogni caso aggirare la protezione meccanica.

17. Assicuratevi che il vostro software antivirus sia aggiornato

La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus. Questi file di identificativi sono rilasciati, di solito, con maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus. Informatevi con il responsabile del trattamento dati per maggiori dettagli.

Come *NON* prevenire i virus:

18. Non diffondete messaggi di provenienza dubbia

Se ricevete messaggi che avvisano di un nuovo virus pericolosissimo, ignoratelo: le mail di questo tipo sono detti con terminologia anglosassone *hoax* (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete. Questo è vero anche se il messaggio proviene dal vostro migliore amico, dal vostro capo, da vostra sorella o da un tecnico informatico. È vero anche e soprattutto se si fa riferimento a "una notizia proveniente dalla Microsoft" (sono gli *hoax* più diffusi).

19. Non partecipate a "catene di S. Antonio" e simili

Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono *hoax*. Anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi o grande fortuna; sono tutti *hoax* aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche. Queste attività sono vietate dagli standard di Internet e contribuire alla loro diffusione può portare alla terminazione del proprio accesso.

Scelta delle password

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

Cosa NON fare

1. NON dite a nessuno la Vostra password. Ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le Vostre risorse o possa farlo a Vostro nome.
2. NON scrivete la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
3. Quando immettete la password NON fate sbirciare a nessuno quello che state battendo sulla tastiera.
4. NON scegliete password che si possano trovare in un dizionario. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per vedere quale sia quella giusta.
5. NON crediate che usare parole straniere renderà più difficile il lavoro di scoperta, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
6. NON usate il Vostro nome utente. È la password più semplice da indovinare
7. NON usate password che possano in qualche modo essere legate a Voi come, ad esempio, il Vostro nome, quello di Vostra moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc.

Cosa Fare

1. Cambiare la password a intervalli regolari. Chiedete al Vostro amministratore di sistema quali sono le sue raccomandazioni sulla frequenza del cambio; a seconda del tipo di sistema l'intervallo raccomandato per il cambio può andare da tre mesi fino a due anni.
2. Usare password lunghe almeno otto caratteri con un misto di lettere, numeri e segni di interpunzione.
3. Utilizzate password distinte per sistemi con diverso grado di sensibilità. In alcuni casi le password viaggiano in chiaro sulla rete e possono essere quindi intercettate, per cui, oltre a cambiarla spesso, è importante che sia diversa per quella usata da sistemi "sicuri". Il tipo di password in assoluto più sicura è quella associata a un supporto di identificazione come un supporto o una carta a microprocessore; la password utilizzata su un sistema di questo tipo non deve essere usata in nessun altro sistema. In caso di dubbio, consultate il vostro amministratore di sistema.

ISTRUZIONI FINALIZZATE AL CONTROLLO E LA CUSTODIA DEGLI ATTI E DOCUMENTI CONTENENTI DATI PERSONALI

Istruzioni particolareggiate applicabili al trattamento di dati personali

- AltaVita-IRA ha messo a disposizione archivi e scaffali (luogo sicuro), ove sono di norma custoditi i documenti contenenti dati personali; come regola generale, tali documenti non devono essere asportati da tale luogo sicuro e, ove ciò avvenga, la asportazione deve essere ridotta al minimo tempo necessario per effettuare le operazioni di trattamento.
- Dal luogo sicuro devono essere asportati solo i documenti strettamente necessari per le operazioni trattamento e non intere pratiche, se ciò non è necessario.
- Al termine delle operazioni di trattamento, i documenti devono essere immediatamente riposti nel luogo sicuro
- Per tutto il periodo in cui i documenti sono all'esterno del luogo sicuro, l'incaricato non deve mai perderli di vista, adempiendo ad un preciso obbligo di custodia dei documenti stessi.
- L'incaricato deve inoltre controllare che i documenti, composti da numerose pagine o più raccoglitori, siano sempre completi, verificando che sia il numero dei fogli che l'integrità del contenuto, rispetto a quanto presente, all'atto del prelievo dal luogo sicuro.
- Se si debbono abbandonare, ad esempio di sera, in ufficio o al termine dell'orario di lavoro, gli anzidetti documenti, l'incaricato deve identificare un luogo sicuro di custodia che dia sufficienti garanzie di protezione da accessi non autorizzati (un armadio chiuso a chiave, un cassetto chiuso a chiave, una cassaforte, un armadio blindato, un classificatore chiuso a chiave); ove si utilizzi un contenitore chiuso a chiave, di qualunque natura, occorre accertarsi che non esistano duplicati abusivi delle chiavi e che tutte le chiavi siano in possesso solo di incaricati autorizzati.
- I documenti di cui sopra non devono essere mai lasciati incustoditi sul tavolo durante il giorno.
- Ci si deve in particolare accertare che un visitatore o terzo (addetto alla manutenzione, addetto alle pulizie, collega non autorizzato) possa entrare in ufficio anche non invitato o per cause accidentali, non possa venire a conoscenza dei contenuti dei documenti (attenti alla lettura alla rovescia!).
- Si deve limitare al minimo assoluto il numero di fotocopie effettuate, mantenendo una traccia scritta delle copie effettuate e degli incaricati e responsabili, cui le copie sono state inviate.
- Si deve adottare una procedura per la consegna delle copie ai destinatari, che dia tutte le garanzie di sicurezza, in particolare utilizzando buste di sicurezza sigillate, oppure effettuando la consegna personalmente, di modo da ridurre al minimo la possibilità che soggetti terzi non autorizzati possano prendere visione del contenuto, od addirittura fotocopiarlo dall'insaputa del mittente e destinatario.
- Documenti contenenti dati sensibili o dati che, per una qualunque ragione, siano stati indicati dal responsabile come meritevoli di particolare attenzione, in fase di affidamento, devono essere custoditi con misure più spinte, rispetto a quelle sinora indicate (per eventuali ulteriori informazioni, rivolgersi al responsabile).
- Nel caso la consegna degli originali o delle fotocopie dei documenti avvenga per posta, si utilizzi la spedizione per assicurata convenzionale, che è l'unica che da la garanzia di un continuo tracciamento del movimento del documento ed offre ben più elevate garanzie di sicura consegna al destinatario, rispetto alle più tradizionale raccomandata.
- Quale che sia il tipo di spedizione adottato, ci si accerti che esso consenta di avere prova certa del fatto che il destinatario ha effettivamente ricevuto i documenti inviati e che essi sono giunti integri, e quindi non manomessi o alterati in fase di trasporto.
- Eventuali fotocopie non riuscite bene debbono essere distrutte in un apposito distruggi-documenti, se disponibile, oppure devono essere strappate in pezzi talmente piccoli, da non consentire in alcun modo la ricostruzione del contenuto, che deve essere comunque illeggibile.
- È tassativamente proibito utilizzare le fotocopie non riuscite come carta per appunti.
- È parimenti tassativamente proibito trasportare all'esterno del posto di lavoro fotocopie non riuscite, da utilizzare altrove come carta per appunti.
- Quando i documenti devono essere trasportati all'esterno del luogo di lavoro, l'incaricato deve tenere sempre seco la cartella o la borsa, nella quale i documenti sono contenuti; deve inoltre evitare che sia possibile esaminare, da parte di un soggetto terzo non autorizzato, anche solo la copertina del documento in questione.
- Durante il trasporto, la cartella non deve essere mai lasciata incustodita e preferibilmente deve essere tenuta chiusa a chiave o devono essere azionate le serrature a combinazione di presenti sulla cartella o valigia.
- È tassativamente proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il corrispondente sia un incaricato, il cui profilo di autorizzazione sia tale da potere trattare i dati in questione.
- Si raccomanda vivamente non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando cellulari all'esterno dell'azienda o anche all'interno, in presenza di terzi non autorizzati, per evitare che dati personali possano venire a conoscenza di terzi non autorizzati, anche accidentalmente. Queste precauzioni diventano particolarmente importanti, quando il telefono è utilizzato in luogo pubblico od aperto al pubblico.
- Si faccia molta attenzione all'utilizzo di macchine fotocopiatrici di ultima generazione, che possono catturare l'immagine del documento, memorizzarlo su hard disk inserito all'interno della macchina, e successivamente stamparla, talvolta conservando file elettronico del documento. In questo caso la fotocopiatrice non va classificata come strumento non elettronico, ma come strumento elettronico, ed a tutti gli effetti si applicano pertanto le particolari cautele, previste per questa tipologia di strumenti.
- In caso di dubbio sulle modalità di applicazione di quanto sopra illustrato, o per chiedere ulteriori chiarimenti in merito, l'incaricato deve rivolgersi al proprio titolare o responsabile.

Policy Aziendale per l'utilizzo delle risorse informatiche

La presente Policy viene redatta da **AltaVita-Istituzioni Riunite di Assistenza- IRA, con sede in Padova 35137 – Piazzale Mazzini, 14 - P.IVA 00558060281 - Tel. 049.8241511 Fax 049.8241531 Mail:** segreteriagenerale@altavita.org **WEB:** www.altavita.org, di seguito definito Titolare.

Tale Policy si prefigge di pianificare un uso corretto delle risorse informatiche del Titolare.
Le finalità sono di natura operativa e di rispetto della sicurezza informatica.
La natura della presente Policy è obbligatoria, vincolante e informativa. Le prescrizioni del Regolamento si aggiungono ed integrano i) le specifiche istruzioni già fornite ai Responsabili e agli incaricati in materia di privacy che devo intendersi qui espressamente richiamate.
Il suo fine è regolamentare l'utilizzo delle risorse informatiche del Titolare da parte del personale dipendente e non dipendente, comunque ad essa legato da un contratto di lavoro subordinato, di prestazione d'opera occasionale, di prestazione coordinata e continuativa, di lavoro interinale.
Una copia della presente Policy viene consegnata ad ogni dipendente, collaboratore, che restituisce al Titolare una copia sottoscritta, così facendone integralmente proprio il contenuto.
L'inosservanza delle regole di comportamento contenute nella presente Policy configura illeciti disciplinari ai sensi di legge e di contratto, ferme restando le altre responsabilità civili, amministrative, penali.
La legge impone all'Ente di controllare il corretto impiego degli strumenti aziendali per la produzione e di dettare le disposizioni per il corretto utilizzo degli stessi, di cui essa assume le responsabilità nei confronti del personale dipendente e non dipendente nonché nei confronti dei terzi.
La presente Policy si pone l'obiettivo di creare una "buona pratica" nelle relazioni di lavoro improntate alla trasparenza, all'accordo e all'uniformità dei comportamenti.
Essa intende, pertanto, garantire il datore di lavoro, il quale ha diritto di richiedere una corretta esecuzione della prestazione lavorativa; ma anche i lavoratori che vengono, in tal modo, resi edotti della politica aziendale in materia di utilizzo di risorse informatiche.

Rispetto dello Statuto dei Lavoratori e della Disciplina della Privacy
La presente Policy intende regolamentare l'esercizio del potere di controllo, direttivo e disciplinare del Titolare nei confronti dei lavoratori nei limiti di legge e di contratto.
Il Titolare garantisce, in ogni caso, che non esistono presso AltaVita-IRA né intende adottare impianti audiovisivi e altre apparecchiature per finalità di controllo a distanza dei lavoratori; e garantisce in ogni caso di uniformare la propria attività a tutte le disposizioni di legge, regolamentari nonché di contratto vigenti.

Controllo del corretto utilizzo delle strutture aziendali
Gli artt. 2086 e 2104 C.C. riconoscono al Titolare il diritto di controllare il corretto utilizzo delle strutture dell'Ente.
L'art. 2087 C.C. impone al Titolare un generale obbligo di tutela dell'ambiente di lavoro e delle sue turbative.
Il Titolare è pertanto tenuto a controllare il corretto impiego degli strumenti dell'Ente e dettare le disposizioni per il corretto utilizzo degli stessi, di cui AltaVita-IRA assume la piena responsabilità nei confronti dei lavoratori e dei terzi.

Responsabilità nell'utilizzo delle risorse informatiche
I lavoratori sono tenuti ad un uso corretto delle risorse e attrezzature messe a loro disposizione per l'esecuzione dell'attività lavorativa. Essi rispondono dei danni eventualmente occorsi sia durante l'esecuzione della prestazione lavorativa sia al di fuori della medesima, fintanto che risorse e attrezzature rientrino nella loro disponibilità.

Obbligo di segretezza e responsabilità dei dati
I lavoratori si impegnano a non divulgare a terzi estranei al Titolare del Trattamento dati e informazioni di cui vengano a conoscenza per motivi di lavoro.
In particolare, essi si impegnano a mantenere il segreto e la massima riservatezza sull'anagrafe clienti, fornitori, contratti, documenti, progetti. Essi sono responsabili dell'uso non corretto di tali dati e informazioni.
E' fatto altresì divieto l'utilizzo di apparecchi riproducenti immagini quali macchine fotografiche o funzioni di smartphone o tablet per fotografare personale o strumenti o aree all'interno della proprietà del titolare senza una codificata autorizzazione del Titolare.

Utilizzo delle risorse informatiche dell'Ente per motivi personali
Ai lavoratori è fatto espresso divieto di utilizzo delle risorse informatiche per scopi personali durante l'orario di lavoro.
Ogni restrizione nell'utilizzo delle risorse informatiche dell'Ente è finalizzata a garantire idonee e preventive misure minime di sicurezza così come prescritte dalla disciplina sul trattamento dei dati personali.
AltaVita-IRA garantisce una politica di massimo rispetto della riservatezza dei dati sensibili relativi ai lavoratori. In nessun caso, pertanto, l'Ente procederà al trattamento dei dati sensibili relativi ai lavoratori esclusivamente per finalità diverse dal rapporto di lavoro.
Per garantire la sicurezza dei dati gestiti da figure quali Amministratori di Sistema l'azienda utilizza un software per la registrazione dei log-in e log-off degli utilizzatori del sistema informatico.
Ai lavoratori è pertanto fatto espresso divieto di utilizzare l'accesso alla posta elettronica con account privato durante l'orario di lavoro.
Ai lavoratori è fatto, altresì, espresso divieto di:

- modificare le configurazioni impostate sul proprio computer;
- ascoltare programmi e files audio e musicali;
- inviare catene telematiche (o di Sant'Antonio);
- utilizzare programmi non distribuiti ufficialmente;
- scaricare files contenuti in supporti magnetici od ottici che non abbiano diretta attinenza con la prestazione lavorativa;
- navigare in siti non strettamente attinenti allo svolgimento della prestazione lavorativa, con particolare riferimento a quelli che possano rivelare le preferenze ed opinioni politiche, religiose, sessuali, o sindacali del dipendente.

E' altresì vietata ogni forma di transazione finanziaria e commerciale.

L'utilizzo della casella di posta elettronica con dominio aziendale
I lavoratori assegnatari di una casella di posta elettronica con dominio dell'Ente ricordino che l'invio di una mail con il dominio aziendale comporta la responsabilità di AltaVita-IRA nei confronti dei terzi per tutto quanto è contenuto nella medesima.
Tutte le informazioni aziendali comunicate tramite mail sono "know how" aziendale tecnico o commerciale protetto in base al D.Lgs 30/2005 e pertanto non possono essere diffuse all'esterno (salvo preventiva autorizzazione scritta della Direzione).
E' fatto divieto di utilizzare le caselle di posta elettronica istituzionale per l'invio di messaggi personali o la partecipazione a dibattiti, forum o mail list salva diversa ed esplicita autorizzazione scritta del Responsabile del trattamento competente per Settore, o comunque per inviare messaggi estranei al rapporto di lavoro.
Ciò premesso, i lavoratori non sono titolari di un diritto all'uso esclusivo della posta elettronica con dominio aziendale.
L'azienda si riserva in ogni caso di predisporre indirizzi di posta elettronica condivisi tra più lavoratori (utilizzando il nome dell'ufficio di riferimento urp@.....) da affiancare a quelli individuali.
La password potrà essere autonomamente modificata senza averne dato espresso avviso all'azienda.
AltaVita-IRA si riserva comunque la facoltà di sostituire la password, qualora ciò sia necessario per motivi di lavoro o per ottemperare agli obblighi di legge.
In relazione al carattere strettamente aziendale e non personale dalla casella di posta elettronica gli utenti della stessa sono tenuti ad inserire in calce ad ogni e-mail la clausola di riservatezza.

Titolarità delle risorse informatiche e utilizzo di Terminali mobili non di proprietà in rete (BYOD) telefoni, tablet e/o smartphone istituzionali
Tutto ciò che costituisce la dotazione delle risorse informatiche, l'accesso ad internet e la casella di posta elettronica con dominio istituzionale appartengono al patrimonio dell'Ente tranne il device di proprietà del collaboratore a cui è acconsentito utilizzare la rete.
I lavoratori utilizzano le risorse informatiche solamente ed esclusivamente per fini professionali per il perseguimento degli obiettivi fissati dall'azienda e in base a quanto da essa espressamente autorizzato.
Il titolare nel caso di concessione di utilizzo di device non di proprietà, stabilisce quali applicazioni possano essere utilizzate, quali sistemi di sicurezza adottare e potrà agire in remoto per rimuovere rischi per i dati aziendali. Per la sicurezza della rete i dispositivi potrebbero essere sottoposti a controlli da parte del Responsabile del trattamento dei dati e dal referente del sistema informatico minimo ogni 3 (tre) mesi.
Ai tablet assegnati ai lavoratori per lo svolgimento delle funzioni cui sono incaricati si applicano le disposizioni previste per i pc portatili. In caso di smarrimento o furto gli utenti sono tenuti ad informare immediatamente il CED.

Il telefono aziendale, sia esso fisso o cellulare, costituisce bene aziendale, assegnato al Dipendente esclusivamente per lo svolgimento delle proprie attività lavorative. Non è consentito l'utilizzo di questi strumenti per fini personali se non per esigenze urgenti e indifferibili.
Il telefono fisso aziendale potrà essere utilizzato per scopi personali solo qualora si manifestino esigenze urgenti e indifferibili che possano cagionare danno all'utente o ai suoi congiunti.

Verifiche sulla navigazione internet
Il sistema informatico registra in modo centralizzato la data e l'ora di connessione, spedizione e ricezione nonché il mittente e i destinatari delle e-mail degli ultimi tre mesi.
Le registrazioni di cui sopra potranno essere conservate per un periodo più lungo rispetto a quello indicato nel caso di richieste da parte dell'autorità giudiziaria o della polizia giudiziaria ovvero nel caso in cui il dato risulti indispensabile in un procedimento giudiziario e/o in un procedimento disciplinare.
Gli incaricati dell'assistenza e della manutenzione degli strumenti elettronici possono controllare i tracciati di cui sopra per verificare la funzionalità e la sicurezza del sistema nonché per verificare il rispetto delle disposizioni sull'utilizzo degli strumenti informatici previste dal presente Regolamento.
Al tal fine, le apparecchiature di rete preposte al collegamento verso internet, memorizzano un giornale (file di log) contenente le informazioni relative ai siti che le postazioni di lavoro aziendali hanno visitato, nei limiti dei tempi di registrazione sopra indicati.
Tale archivio memorizza l'indirizzo fisico delle postazioni di lavoro e non i riferimenti dell'utente, garantendo in tal modo il suo anonimato.
Il controllo verrà effettuato rispettando il principio della gradualità ed i principi di pertinenza e non eccedenza
La prima analisi delle registrazioni sarà effettuata senza differenziazione per utente. L'eventuale problema individuato verrà segnalato all'utenza e verrà indicato contestualmente il comportamento da tenere per risolverlo.
In caso di persistenza del problema verrà effettuata una seconda analisi differenziata per gruppo di utenti o per gruppo di computer (se possibile).
L'eventuale problema individuato verrà segnalato all'utenza del gruppo e verrà indicato contestualmente il comportamento da tenere per risolverlo.
Solo nel caso in cui i due controlli di cui sopra e le relative azioni correttive non abbiano sortito alcun risultato sarà effettuata l'analisi individuale.
Anche in quest'ultimo caso l'eventuale problema individuato verrà segnalato all'utente e verrà indicato contestualmente il comportamento da tenere per risolverlo.
Nel caso in cui gli incaricati dell'assistenza e della manutenzione degli strumenti elettronici effettuino controlli sul singolo utente quest'ultimo sarà preventivamente informato in forma scritta e le finalità della verifica dovranno essere espressamente indicate.

Responsabile della sicurezza informatica
AltaVita-IRA potrebbe affidare l'organizzazione, la gestione, la verifica ed il controllo sull'utilizzo di tutti gli strumenti informatici previsti nel presente Regolamento ad una Ditta esterna, con nomina di Responsabile del trattamento dati.
Impregiudicato tutto quanto previsto nelle precedenti specifiche disposizioni del Regolamento, il Responsabile dei sistemi informativi per l'espletamento delle sue funzioni:
a) ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna;
b) può accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento (ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato);
c) può in qualunque momento procedere alla rimozione di ogni file o dell'applicazione che riterrà essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete;
d) provvede a segnalare all'Ufficio del Personale le anomalie sull'utilizzo degli strumenti informatici previsti nel Regolamento che possano essere configurate quali attività non conformi.

Registro dei trattamenti

ALLEGATO 3

Modello di gestione incidenti di sicurezza
DATA BREACH

Sommario

Premessa
Il presente documento rappresenta il riferimento **AltaVita-Istituzioni Riunite di Assistenza- IRA, con sede in Padova 35137 – Piazzale Mazzini, 14 (da ora il Titolare)** per la regolamentazione della gestione degli incidenti di sicurezza informatica che possono occorrere ai servizi ed ai dati gestiti.
La corretta gestione degli incidenti di sicurezza permette di evitare o minimizzare la compromissione dei dati dell'organizzazione in caso di Incidente; permette inoltre, attraverso l'analisi e la comprensione dei meccanismi di attacco e delle modalità utilizzate per la gestione dell'Incidente, di migliorare continuamente la capacità di risposta agli incidenti.
Inoltre, con specifico riferimento all'obbligo di cui all'art. 33 del GDPR n. 679/2016, il presente documento individua quali siano le violazioni che ricadono nell'ambito della suddetta normativa, i casi in cui il Titolare deve notificare i data breach all'Autorità Garante ed agli interessati, le misure atte a trattare il rischio e la documentazione da produrre.
Si rappresenta che l'art. 32 del Regolamento dispone che devono essere approntate misure tecniche e organizzative adeguate per garantire un livello adeguato di sicurezza dei dati personali. Individuare, indirizzare e segnalare tempestivamente un Incidente di sicurezza, come una violazione di dati, è espressione dell'adeguatezza delle misure implementate dal Titolare.
L'ambito di applicazione è rappresentato da sistemi ICT del Titolare e vengono presi in considerazione incidenti che possono scaturire sia attraverso l'azione di un attacco informatico portato da elementi esterni all'organizzazione sia generati da un eventuale comportamento negligente o scorretto, di natura ostile con obiettivi frodatori da parte di un collaboratore del Titolare.
Tutte le violazioni dei dati personali sono incidenti di sicurezza, ma non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali.
L'obbligo di cui agli artt. 33 e 34 del Regolamento trova applicazione nei soli casi in cui la violazione riguardi dati personali, come definiti dall'art. 4 n. 1) del GDPR.
Il presente documento è applicabile alle risorse ed ai servizi di tipo informatico gestiti in modo diretto oppure esternalizzato da parte del Titolare.

Incidente di sicurezza
Ai sensi del presente documento, per Incidente di sicurezza deve intendersi "la violazione, la minaccia imminente di violazione di una politica di sicurezza informatica, di politiche di utilizzo accettabili o di prassi standard di sicurezza, correlato ad una violazione di dati o informazioni. Esempi di incidenti sono:

- un utente malintenzionato esegue operazioni al fine di inviare un numero elevato di richieste di connessione ad un server web, provocando l'arresto anomalo del servizio;
- gli utenti sono indotti ad aprire un file allegato alla mail che in realtà è un malware; l'esecuzione del tool che comporta l'infezione del dispositivo stabilendo connessioni con un host esterno;
- Un utente malintenzionato ottiene dati sensibili e minaccia l'organizzazione di diffonderli se non viene pagato un riscatto in denaro

Data breach ai sensi del GDPR
Il regolamento definisce la violazione dei dati personali come "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".
Le violazioni declinate dalla norma sono sintetizzabili come

- **"Violazione della riservatezza"**, che si ha in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali.
- **"Violazione dell'integrità"**, che si ha in caso di alterazione non autorizzata o accidentale dei dati personali
- **"Violazione della disponibilità"**, che si ha in caso di perdita o distruzioni di dati personali o di impossibilità di accesso ai dati personali da parte di soggetti autorizzati.

Va sottolineato che una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione di queste.
Gli effetti di una violazione possono causare danni fisici, materiali o immateriali, ovverosia la perdita del controllo sui propri dati personali, la limitazione dei loro diritti, discriminazione, furto d'identità o frode, perdita finanziaria, inversione non autorizzata di pseudonimizzazione, danno alla reputazione e perdita di riservatezza dei dati personali protetti dal segreto professionale. Può anche includere qualsiasi altro significativo svantaggio economico o sociale per tali individui.

Notifica al Garante e agli interessati
In caso di data breach il Titolare deve valutare i rischi per i diritti e le libertà delle persone fisiche, registrando le evidenze di tale analisi.
Nell'eventualità che tale valutazione rappresenti elementi di rischio per i diritti e le libertà delle persone fisiche il Titolare effettua la notifica al Garante delle violazioni di dati personali.

Quando le violazioni di dati comportano un rischio che viene valutato come elevato per i diritti e le libertà delle persone fisiche, le stesse devono essere comunicate agli interessati senza ingiustificato ritardo, fornendo loro specifiche informazioni in ordine alle salvaguardie che devono adottare per proteggere loro stessi dalle conseguenze della violazione.
Questo rischio esiste quando la violazione può comportare un danno fisico, materiale o immateriale per le persone i cui dati sono stati violati. Tale rischio è presunto quando il data breach riguarda le categorie particolari di dati di cui all'art. 9 del GDPR.
I criteri che devono guidare la valutazione del suddetto rischio sono i seguenti:

- la tipologia di violazione
- la natura dei dati violati
- il volume dei dati violati
- il numero di individui cui si riferiscono i dati violati
- caratteristiche speciali degli individui cui si riferiscono i dati violati
- il grado di identificabilità delle persone
- la gravità delle conseguenze per gli individui

La valutazione deve essere condotta secondo una metodologia operativa adeguata che viene di dettagliata nel seguito.

Il Titolare notifica la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui è stata rilevata. Oltre tale termine, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni sono fornite in fasi successive senza ulteriore ingiustificato ritardo.
Il termine principia dal momento in cui il Titolare ha consapevolezza della violazione di dati, ovverosia quando si raggiunge un ragionevole grado di certezza che si è verificato un Incidente di sicurezza che ha compromesso i dati personali.
Il Titolare può tardare la notifica all'Autorità Garante, nei casi in cui tale notifica possa produrre effetti negativi sugli individui.
Nei casi in cui il Titolare disponga di informazioni solo parziali della violazione, viene, comunque, effettuata la notifica al Garante.
Il Garante per la protezione dei dati personali può richiedere, in ogni caso, la notifica della violazione agli interessati.
La comunicazione della violazione agli interessati può essere ritardata nei casi in cui tale comunicazione possa pregiudicare le indagini su cause, natura e conseguenze della violazione, anche su indicazione delle varie Autorità di controllo.
Il Titolare utilizza lo strumento più efficace affinchè tale notifica sortisca il maggiore effetto possibile.

Ruoli e responsabilità
La criticità del processo di gestione degli incidenti di sicurezza informatica e del data breach deve essere opportunamente affrontata da una struttura operativa competente, in possesso di adeguata formazione ed in grado di prendere rapidamente le decisioni imposte dalla delicatezza del compito assegnato.
Il Titolare istituisce, con proprio atto, un gruppo per la Gestione della Sicurezza ICT, adeguatamente dimensionato e strutturato, con le seguenti competenze:

- rappresentare il punto di riferimento univoco a cui il personale dell'organizzazione deve rivolgersi per segnalare un potenziale Incidente oppure un comportamento sospetto;
- gestire tutte le attività inerenti l'analisi e la gestione di un Incidente di sicurezza, ivi comprese quelle relative alla sua notifica e documentazione;
- garantire la disponibilità delle liste di contatti (es.: personale dipendente, collaboratori, fornitori), necessarie per la gestione di un Incidente di sicurezza;
- garantire che il processo di gestione incidenti sia sempre adeguato alle esigenze del Titolare, provvedendo che sia sempre aggiornato.

I riferimenti del gruppo (nominativi, indirizzo e-mail, numero di telefono ecc.) devono essere ben identificati e facilmente raggiungibili.
Il gruppo deve includere un **referente per la gestione della sicurezza informatica** che sarà la figura che avrà in carico la gestione degli incidenti.
Nel corso del processo di gestione di un Incidente di sicurezza informatico e, eventualmente, di un data breach, il gruppo potrà essere coadiuvato di volta in volta dal personale della struttura i cui dati sono stati oggetto di data breach e da tutti coloro che il gruppo riterrà necessario coinvolgere a seconda della tipologia di Incidente e della tipologia di dati coinvolti.
Nelle attività del gruppo deve essere coinvolto il Data Protection Officer (DPO) designato, il quale esercita le proprie funzioni di monitoraggio della conformità in caso di data breach, fornendo il proprio parere in ordine alla necessità di effettuare la notifica e, quindi, sulle valutazioni precedentemente descritte.
Il referente per la gestione della sicurezza informatica ha il compito di attivarsi in caso di incidenti di sicurezza, di individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere obbligatorio del DPO, e di segnalare al Responsabile esterno (se individuato) competente in

materia di sicurezza se presente le violazioni dei dati personali ai fini della notifica, ai sensi dell'art. 33 del Regolamento, al Garante per la protezione dei dati personali.
Il Titolare o il Responsabile esterno (se individuato) deve inoltre coinvolgere, a seconda della gravità dell'Incidente, i Referenti di Area competenti per gli aspetti di comunicazione interna ed esterna e nel caso, durante la gestione dell'Incidente, emergano responsabilità da parte di personale interno del Titolare.
Nel caso in cui le attività di analisi dell'Incidente di sicurezza evidenzino particolari difficoltà oppure impatti che si estendono al di fuori del perimetro del Titolare. il Responsabile deve valutare l'opportunità o la necessità, di coinvolgere le strutture di riferimento regionali e nazionali. Inoltre, il Responsabile deve prevedere il coinvolgimento dei propri fornitori di servizi ICT per il supporto all'analisi e per l'ottenimento di informazioni utili oltre alle autorità di pubblica sicurezza nel caso in cui l'Incidente possa presentare risvolti dal punto di vista penale.
In caso di data breach il punto di contatto con il Garante per la protezione dei dati personali è costituito dal Data Protection Officer.
Vi sono comportamenti, attività e regolamenti che ogni organizzazione deve necessariamente attivare per cercare di prevenire gli incidenti di sicurezza, riducendo il livello di rischio e l'esposizione a possibili attacchi informatici. Tali contromisure, che possono essere di natura sia tecnologica che organizzativa, devono essere descritte e adottate dal Titolare per mettere in sicurezza i sistemi ICT.

Procedura di gestione degli incidenti di sicurezza
Deve essere sviluppata, documentata e tenuta aggiornata una procedura per la gestione degli incidenti di sicurezza. Tale procedura ha i seguenti obiettivi:

- preparare il personale;
- identificare un Incidente in corso;
- minimizzare i danni relativi all'Incidente ed impedirne la propagazione;
- gestire correttamente il processo di ripristino dei sistemi e delle applicazioni;
- acquisire nel modo appropriato le eventuali evidenze digitali di reato;
- riconoscere gli errori commessi, assumerne le responsabilità e formulare proposte volte a migliorare la procedura stessa.

La decisione su quali soluzioni adottare è demandata al gruppo di gestione sicurezza con l'eventuale supporto delle figure ritenute necessarie tenendo conto della complessità e variabilità dell'argomento trattato.
Per facilitare la gestione degli incidenti di sicurezza occorre mantenere operativo un workflow che automatizzi le varie fasi, in particolare il flusso delle comunicazioni fra i vari attori. Tale misura ha anche lo scopo di facilitare la produzione del report relativo all'Incidente e di tenere aggiornate le statistiche sugli incidenti di sicurezza.
Oltre ai requisiti di riservatezza ed integrità, occorre considerare anche le esigenze di disponibilità dei dati e dell'infrastruttura ICT preposta all'erogazione dei servizi informatici. Nel caso si verifichi di Incidente di sicurezza che possa pregiudicare per un periodo sufficientemente lungo la disponibilità delle informazioni occorre fare riferimento a disposizioni contenute in un piano di continuità operativa del Titolare adottato con una chiara definizione delle strutture e delle responsabilità della gestione delle emergenze che dovranno operare in stretto coordinamento con il gruppo gestione sicurezza.
Qualora, a seguito di un Incidente relativo alla sicurezza delle informazioni, risulti necessario per Il Titolare intraprendere un'azione legale (civile o penale) contro una persona fisica o giuridica, oppure nel caso in cui ci siano le premesse affinché il Titolare possa essere oggetto di azione legale (civile o penale), le evidenze oggettive devono essere raccolte e conservate e presentate al fine di conformarsi ai requisiti di legge applicabili nelle sedi giurisdizionali competenti. Tutta la fase di raccolta delle evidenze deve essere fatta in modo che le evidenze siano utilizzabili in un processo giuridico. La raccolta delle evidenze può avvenire anche qualora si voglia semplicemente procedere con indagini più approfondite, non necessariamente legate ad un proseguo forense.
La documentazione relativa agli incidenti di sicurezza, comprensiva delle evidenze e delle valutazioni effettuate, viene elaborata in maniera tale da non indicare dati personali. Il tempo di conservazione di tale documentazione è stabilito in 24 mesi nel caso in cui siano presenti dati personali, allo spirare del quale i dati devono essere cancellati e senza limiti di tempo nel caso non siano presenti dati personali.
Tutti i dipendenti e collaboratori del Titolare che accedono alle risorse del Sistema Informatico del Titolare sono tenuti ad osservare i principi contenuti nel presente documento ed a segnalare in modo tempestivo la presenza di condizioni che possano indurre a valutare delle anomalie riconducibili ad attacchi informatici oppure a comportamenti scorretti.
Eventuali amministratori di sistema, che a causa del loro comportamento gravemente negligente o in palese contrasto con le politiche di sicurezza del Titolare, fossero causa diretta o indiretta di Incidente di sicurezza, potranno essere soggetti ad un accertamento di eventuali responsabilità e violazione delle politiche di sicurezza ICT del Titolare.

Dettagli della procedura di gestione degli incidenti di sicurezza

Preparazione

Si tratta di attività necessarie per consentire una adeguata gestione degli incidenti informatici di sicurezza che devono essere eseguite rigorosamente. Si tratta ad esempio di:

- definizione della struttura tecnica di supporto nella gestione degli incidenti e dei necessari interventi di formazione per le risorse potenzialmente coinvolte nella gestione degli incidenti;
- predisposizione degli strumenti hardware e software necessari;
- definire e distribuire le apposite procedure relative alle modalità di comunicazione verso l'esterno dell'accaduto.

Identificazione e analisi dell'Incidente

Si tratta di attività che mira a valutare se un evento riscontrato sia effettivamente riconducibile ad un Incidente di sicurezza oppure si tratti di un cosiddetto falso positivo. Le operazioni di identificazione (Detection and Analysis) devono permettere di verificare, per ogni caso di evento anomalo o sintomo di un Incidente, se si è in presenza di un Incidente reale di sicurezza.

La segnalazione di Incidente di sicurezza può arrivare direttamente da parte di un utente, il quale può per esempio rilevare situazioni di alterazione di un sito web del Titolare, di accesso non autorizzato a dati, di indisponibilità di una risorsa ICT per un tempo prolungato etc. Le segnalazioni degli utenti devono pervenire al referente per la gestione della sicurezza informatica appositamente incaricato per condurre una prima analisi prima di coinvolgere l'intero gruppo.

Nel caso di segnalazioni di Incidente da parte di soggetti terzi, il Titolare avvia senza indugio un'indagine volta a verificare che sia avvenuta effettivamente la violazione di dati segnalata. La notifica viene effettuata al Garante qualora gli esiti della breve e spedita indagine consentano di appurare l'effettiva verificazione della violazione (quindi solo al termine dell'indagine).

Valutazione dell'impatto dell'Incidente
L'analisi degli eventi può portare all'individuazione dei possibili reali incidenti di sicurezza, che si possono classificare in diverse tipologie come segue:

Tipologia Incidente	Descrizione
Accesso non autorizzato	Accesso (sia logico che fisico) a reti, sistemi, applicazioni, dati o altre risorse tecnologiche di proprietà del Titolare da parte di personale non autorizzato.
Denial of Service	Attacco informatico alla disponibilità di una rete o sistema. Qualora abbia successo, comporta la difficoltà all'accesso o la totale indisponibilità di determinati sistemi e/o servizi.
Codice malevolo	Un virus, worm, trojan, spyware, o qualsiasi altro codice malevolo che infetti un sistema.
Uso Inappropriato	Violazione delle politiche di sicurezza e delle disposizioni su corretto utilizzo.
Data leakage	Diffusione di informazioni riservate a seguito di un attacco informatico riuscito.
Alterazione delle informazioni	Modifica del contenuto di dati riservati a seguito di un attacco informatico riuscito.
Phishing	Truffa effettuata su Internet, che sfrutta tecniche di ingegneria sociale, attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso.
Furto/smarrimento totale o parziale di apparecchiature che contengono dati sensibili	Il furto o smarrimento di singoli dispositivi di memorizzazione (hard disk, memorie di massa rimovibili ecc) oppure dei computer/server che li ospitano. Una violazione dei dati personali sensibili contenuti configura una condizione di data breach che richiede, ai sensi del GDPR, l'attivazione delle specifiche procedure di notifica verso l'autorità Garante e gli utenti coinvolti
Multiplo	Incidente di sicurezza che comprende due o più di quelli sopra elencati.
Malfunzionamento grave	Danneggiamento di un componente hardware o software, oppure degrado delle performance per cause esterne che possa arrecare impatti gravi alla disponibilità di servizio.
Disastro	Qualsiasi evento distruttivo, non provocato direttamente da azione di operatori informatici (es.: blackout, incendio, allagamento, terremoto) in grado di condizionare direttamente l'operatività dei sistemi informatici.

E' di fondamentale importanza effettuare una prima valutazione sull'impatto dell'Incidente ai fini di indirizzare in modo efficace le risorse necessarie alla sua gestione. Tale attività consiste in una prima classificazione della sua portata in base ad alcuni parametri di seguito elencati:

- il livello di criticità della risorsa ICT coinvolta, determinato in base alle valutazioni inerente la Business Impact Analysis (in caso di coinvolgimento di più risorse verrà assunto come tale quello a maggiore criticità);
- il numero di risorse informatiche coinvolte, inteso come numero di server/applicazioni;
- il numero di utenti o postazioni di lavoro potenzialmente impattati dalla indisponibilità del servizio informatico;
- l'eventuale coinvolgimento di risorse ICT/utenti esterni all'organizzazione;
- l'esposizione su Internet del servizio;
- il tipo di danno arrecato (economico, immagine, mancato adempimento normativo ecc.);
- gli enti o le organizzazioni coinvolte nell'Incidente;
- l'eventualità di coinvolgere le forze dell'ordine a causa di possibili risvolti di natura penale.

In questa fase il referente della sicurezza informatica del gruppo sicurezza ICT deve anche stabilire la gravità dell'Incidente di sicurezza, per fare ciò può inizialmente avvalersi della matrice contraddistinta da una valutazione di tipo qualitativo, ma la classificazione della gravità dell'Incidente è comunque a sua totale discrezione.

Gravità Incidente di sicurezza	***Descrizione***
Alta	Il grado di compromissione di servizi e/o sistemi è elevato. Si rilevano danni consistenti sugli asset. Il ripristino è di medio o lungo periodo. L'Incidente presenta una tra le seguenti condizioni: • Danni a persone e rilevanti perdite di produttività • Compromissione di sistemi o di reti in grado di permettere accessi incontrollati a informazioni confidenziali • Siti web violati o utilizzati a fini di propagazione di materiale terroristico o pornografico • Frode o attività criminale che coinvolga servizi forniti da AltaVita-IRA • Impossibilità tecnica di fornire uno o più servizi critici a un elevato numero di utenti per un intervallo di tempo superiore ai 30 minuti nell'arco di una giornata • Impossibilità tecnica di fornire uno o più servizi di criticità media per un periodo di tempo superiore ai 2 giorni lavorativi • Significativa perdita economica, di immagine e/o reputazione nei confronti del pubblico o degli utenti
Media	L'Incidente non presenta nessuna condizione che porti alla catalogazione "gravità alta". Il grado di compromissione di servizi e/o sistemi è di una certa rilevanza e possono essere rilevati danni sugli asset di una certa consistenza. Il ripristino ha tempi che non compromettono la continuità del servizio L'Incidente presenta una tra le seguenti condizioni: • Compromissione di server • Degrado di prestazioni relativo ai servizi offerti dal Titolare con perdita di produttività da parte degli utilizzatori • Attacchi che provocano il funzionamento parziale o intermittente della rete • Impossibilità tecnica di fornire uno o più servizi critici ad un elevato numero di utenti per intervalli di tempo inferiori ai 30 minuti di tempo ripetuti su più giornate • Impossibilità tecnica di fornire uno o più servizi critici ad una piccola parte di utenti per un periodo di tempo superiore ai 30 minuti di tempo nell'arco di una o più giornate • Basso impatto in termini di perdita economica, di immagine e/o reputazione nei confronti degli utenti
Bassa	L'Incidente non presenta nessuna condizione che porti alla catalogazione "gravità alta o media". Non vengono compromessi asset o servizi. L'Incidente presenta le seguenti condizioni: • Interruzione dell'attività lavorativa di un numero ristretto di dipendenti e per un breve periodo di tempo. • Contaminazioni da virus in un medesimo sito ma comunque identificate dai sistemi anti-malware • Nessuna o limitata perdita di operatività o di business da parte di un ridotto numero di dipendenti.

Per alcuni incidenti può risultare difficile assegnare un livello di gravità definitivo prima che l'analisi sia completa; in tal caso occorre valutarla sulla base delle evidenze note sino a quel momento, assumendo che la gravità potrebbe molto probabilmente aumentare nel caso non si effettui alcuna operazione di contenimento.

In ogni caso, è opportuno verificare ciclicamente, nel periodo in cui l'Incidente è in corso, la gravità

assegnata allo stesso in quanto essa può variare nel tempo. Al termine della fase di analisi, è necessario informare tempestivamente il gruppo gestione della sicurezza ICT deputata alla gestione incidenti ed il Responsabile della Sicurezza interessato.

Valutazione dei rischi derivanti dal verificarsi del data breach

Per data breach si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

In caso di data breach il Titolare deve valutare i rischi per i diritti e le libertà delle persone fisiche, utilizzando i criteri di seguito indicati:

- la tipologia di violazione, ovverosia il tipo di violazione come declinata nel paragrafo precedente;
- la natura dei dati violati, valutando che più i dati sono "sensibili" e maggiore è il rischio di danni per le persone fisiche;
- il volume dei dati violati, considerando che la violazione di diverse tipologie di dati comporta un rischio maggiore rispetto alla violazione di una sola tipologia;
- il numero di individui cui si riferiscono i dati violati, considerando che, generalmente, maggiore è il numero di individui interessati, maggiore è l'impatto di una violazione. Tuttavia, una violazione può avere un impatto grave anche su un solo individuo, a seconda della natura dei dati personali e del contesto in cui è stato compromesso;
- caratteristiche speciali degli individui cui si riferiscono i dati violati, ad esempio minori o persone vulnerabili;
- il grado di identificabilità delle persone, considerato che l'identificazione potrebbe essere possibile direttamente dai dati personali violati senza alcuna ricerca speciale necessaria per scoprire l'identità dell'individuo, oppure potrebbe essere estremamente difficile abbinare i dati personali a un particolare individuo, ma potrebbe comunque essere possibile a determinate condizioni (sono, quindi, considerati tutti i mezzi di cui ci si possa avvalere per identificare le persone fisiche);
- la gravità delle conseguenze per gli individui: tale criterio è strettamente connesso alla tipologia di dati violati. Deve essere considerato che una violazione di riservatezza può occorrere anche nel caso in cui dei dati personali siano comunicati ad un terzo, pur non autorizzato, ma conosciuto e "fidato". In tali casi, la valutazione di tale criterio abbasserà il livello di gravità delle conseguenze per gli individui. Nel caso in cui i dati personali siano nelle mani di persone le cui intenzioni sono sconosciute o potenzialmente dannose il livello di rischio potenziale sarà più elevato.

In caso di data breach deve essere sempre coinvolto il Data Protection Officer (DPO) se presente per la valutazione dei rischi per i diritti e le libertà delle persone fisiche, il quale esprime anche formale parere sulla necessità di effettuare la notifica.

COMUNICAZIONE DEGLI INCIDENTI

Tutti i potenziali incidenti dovranno essere comunicati come primo punto di contatto alla struttura organizzativa del Titolare adibita alla gestione della sicurezza ICT, via mail, o attraverso le specifiche modalità adottate dal Titolare. L'attivazione della procedura stessa sarà quindi a carico del referente per la gestione della sicurezza informatica che dovrà comunque riportare la situazione al Responsabile della sicurezza secondo le procedure previste.

La notifica della violazione al Garante

Nei casi in cui l'Incidente consista in una violazione di dati personali, il Titolare deve notificare l'Incidente al Garante per la protezione dei dati personali se, sulla scorta della valutazione approfondita, strutturata e documentata di cui al paragrafo precedente, si assuma come probabile che la violazione dei dati personali presenti effettivamente un rischio per i diritti e le libertà delle persone fisiche.

La comunicazione al Garante, da redigere in aderenza all'allegato del presente documento, deve ricomprendere ogni informazione utile, oltre che la descrizione:

- della natura della violazione dei dati personali;
- delle categorie e il numero approssimativo di interessati in questione nonché le categorie[1] e il numero approssimativo di registrazioni[2] dei dati personali in questione;
- delle probabili conseguenze della violazione dei dati personali;
- delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;
- i recapiti del Data Protection Officer.

[1] minori, persone con disabilità, dipendenti, clienti etc.
[2] Informazioni finanziarie, numeri di conti bancari, numeri di passaporto, documenti sanitari, etc.

La notifica della violazione agli interessati

Alcune violazioni di dati, quelle che comportano un rischio elevato per i diritti e le libertà delle persone fisiche devono essere comunicate agli interessati senza ingiustificato ritardo. Tale comunicazione, da redigere in aderenza all'allegato del presente documento, nonché formulata con linguaggio chiaro e comprensibile agli utenti (quindi non in gergo tecnico) deve ricomprendere:

- la descrizione della natura della violazione;
- i recapiti del Data Protection Officer;
- la descrizione delle probabili conseguenze della violazione;
- le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Nel caso in cui il numero di interessati lo consenta, la comunicazione deve essere inviata a mezzo mail (o pec, o sms) e con avviso pubblicato sul sito istituzionale. Nel caso in cui il numero di soggetti coinvolti sia particolarmente alto, è sufficiente effettuare la comunicazione dell'avvenuta violazione di dati utilizzando il sito istituzionale.

ATTIVAZIONE DELLA PROCEDURA E MONITORAGGIO DELLE ATTIVITÀ

L'attivazione della procedura di gestione incidenti, mediante le opportune segnalazioni nel workflow sarà a carico del referente per la gestione della sicurezza informatica, il quale, a seconda della gravità attribuita in fase di identificazione dell'Incidente, utilizzerà diverse modalità di attivazione e tracking.

Incidente di gravità "Alta"

Il referente per la gestione della sicurezza informatica provvederà a coinvolgere il gruppo Gestione Sicurezza mediante l'invio dell'apposito Rapporto Incidente di sicurezza compilando soltanto le parti che in questa fase è possibile conoscere.
Lo scopo principale di questa prima fase è di attivare il gruppo sicurezza per la gestione dell'Incidente ed eventualmente anche informare il DPO se presente nel caso di un data breach. Il Rapporto Incidente di sicurezza sarà poi completato in tutte le sue parti in fase di chiusura dell'Incidente.
Il Responsabile della Sicurezza competente per l'Incidente in gestione, deve conservare per la durata di cinque anni il Rapporto, in formato elettronico, in una cartella soggetta a backup periodico e ad accesso opportunamente limitato.
E' altresì fondamentale che tutte le operazioni eseguite per la gestione di un eventuale Incidente siano opportunamente tracciate (es. strumento informatico di ticketing o altro), permettendo in tal modo di poter identificare tutte le risorse coinvolte nelle operazioni tecniche di gestione e poterle eventualmente indicare in ambito giudiziale come testimoni.
Le indagini svolte e le operazioni di gestione formeranno quindi una base dati che andrà ad incrementare la conoscenza del Titolare in merito agli incidenti di sicurezza informatica.
Nel caso in cui l'Incidente di sicurezza abbia un impatto sulla continuità operativa per un tempo di disservizio inaccettabile per il cliente, è necessario attivare il gruppo sicurezza e fare riferimento al piano di Business Continuity.

Incidente di gravità "Media" o "Bassa"

In caso di Incidente di gravità media o bassa, l'Incidente può essere completamente gestito dal referente per la gestione della sicurezza informatica fermo restando il coinvolgimento del DPO se presente nel caso di un data breach. In tale caso non è necessaria (anche se è consigliabile comunque) la stesura del Rapporto di Incidente di Sicurezza, ma è comunque necessario tracciare opportunamente le operazioni permettendo in tal modo di poter identificare tutte le risorse coinvolte nelle operazioni tecniche di gestione e poterle eventualmente indicare in ambito giudiziale come testimoni.
Anche in questo caso le indagini svolte e le operazioni di gestione formeranno quindi una base dati che andrà ad incrementare la conoscenza del Titolare in merito agli incidenti di sicurezza informatica.
I dati raccolti saranno resi disponibili attraverso diversi profili di consultazione, anche a fini statistici, al Responsabile della Sicurezza ed ai membri del gruppo sicurezza.

Contenimento, rimozione e ripristino

Le operazioni di contenimento hanno due importati fini:

- evitare che il danno si propaghi od almeno limitarne la diffusione;
- acquisire le eventuali evidenze digitali di reato prima che queste possano essere compromesse.

Quest'ultima attività è molto critica, infatti, è necessario:

- identificare tutti i sistemi che possono essere stati compromessi o sui cui sia possibile raccogliere eventuali evidenze digitali di reato;
- effettuare delle copie delle eventuali evidenze digitali di reato in modo valido dal punto di vista forense;
- documentare in modo dettagliato tutte le operazioni eseguite, onde evitare in un eventuale ambito giudiziale possibili contestazioni sulla correttezza delle operazioni eseguite;
- le attività di contenimento dovranno essere eseguite da personale qualificato, ovvero da sistemisti o esperti applicativi appositamente addestrati per eseguire le operazioni necessarie.

Tutte le operazioni eseguite saranno comunque sotto la responsabilità del referente per la sicurezza informatica il quale dovrà riportare nel Rapporto di Incidente:

- data ed ora delle azioni eseguite sui sistemi, applicazioni o dati;
- le generalità delle risorse che hanno materialmente eseguito le operazioni;
- i risultati conseguiti.

Il referente per la sicurezza informatica dovrà comunicare al Responsabile della sicurezza interessato quanto eseguito al termine di questa fase.
Le operazioni di contenimento possono essere di due tipologie: a breve termine e a lungo termine.

Contenimento a breve termine
Le operazioni di contenimento a breve termine mirano a mettere in sicurezza gli eventuali sistemi interessati da un Incidente, senza alterarne la configurazione o inquinare eventuali evidenze digitali di reato.
Come esempi di azioni di contenimento a breve termine si possono indicare:

- creazione di regole firewall atte a bloccare l'accesso ai sistemi coinvolti;
- disabilitazione di account utente sui sistemi centralizzati di autenticazione;
- cambio di configurazione sui sistemi DNS;
- disconnessione dei sistemi coinvolti dalla rete mediante riconfigurazione di apparati di rete.

Dopo aver messo in sicurezza i sistemi coinvolti nell'Incidente, mediante l'operazione di contenimento a breve termine, è possibile procedere all'acquisizione di eventuali evidenze digitali (es. mediante copia forense dei dischi) oppure procedere con l'esecuzione di normali backup atti a mettere in sicurezza i dati per poterli riutilizzare nella eventuale ricostruzione del sistema colpito dall'Incidente.
E' necessario procedere all'acquisizione forense delle evidenze digitali di reato in ogni caso in cui si prevede un prosieguo in ambito legale come per esempio:

- accessi abusivi a sistemi o informazioni;
- attività illecite commesse da dipendenti o comunque mediante il sistema Informativo gestito del Titolare;
- interruzione di pubblici servizi critici;
- violazioni della privacy di utenti e cittadini;
- utilizzo illegale dei sistemi per perpetrare truffe o diffondere materiale illecito.

Quando invece l'Incidente è causato da malfunzionamenti o errori umani è possibile procedere eseguendo una normale operazione di backup relativa a dati o configurazioni eventualmente presenti sul dispositivo coinvolto nell'Incidente. Questa operazione potrà quindi essere eseguita utilizzando i sistemi ed i programmi utilizzati per effettuare le comuni operazioni di backup ed hanno lo scopo di mettere in sicurezza le informazioni necessarie per una eventuale reinstallazione del dispositivo.

Contenimento a lungo termine
Il contenimento a lungo termine comporta l'esecuzione di operazioni tecniche direttamente sui sistemi coinvolti nell'Incidente, per questo motivo questa azione deve essere eseguita solo dopo aver messo in sicurezza le evidenze digitali di reato o i dati presenti sul sistema impattato.
Tali operazioni mirano a rendere i sistemi coinvolti più sicuri e permettono di lasciarli in attività sino al momento in cui sia possibile procedere ad operazioni più complesse di rimozione delle cause.
Come esempio di operazioni di contenimento a lungo termine si possono elencare:

- installazione di patch o aggiornamenti di sistema e/o applicativi;
- cancellazione di file o dati;
- arresto di servizi o processi malevoli;
- cambio di configurazione di programmi.

Al termine di queste operazioni i sistemi coinvolti nell'Incidente non possono ancora dichiararsi sicuri, ma è possibile utilizzarli temporaneamente sino a quando non sia possibile procedere con le operazioni di rimozione definitiva di quanto ha scatenato l'Incidente.

Durante questa fase, possono emergere diverse necessità, come per esempio:

- allocare risorse economiche per la fase di acquisizione forense/backup e le successive fasi di gestione;
- isolare e/o arrestare eventuali servizi o sistemi critici di produzione coinvolti;
- valutare eventuali conseguenze legali;
- relazionarsi con altri Servizi/Direzioni del Titolare per comunicare eventuali disservizi.

In tali casi il referente per la sicurezza informatica può operare le corrette scelte in autonomia, comunicando al Responsabile della Sicurezza interessato le eventuali azioni che saranno intraprese.

Rimozione

Le operazioni di rimozione sono volte all'eliminazione definitiva del problema o della vulnerabilità utilizzata per compromettere un sistema coinvolto in un Incidente e riportarlo ad un livello di sicurezza elevato.

Le attività che sono solitamente eseguite in questa fase possono essere di diverso tipo, per esempio:

- aggiornamento di release dei sistemi operativi o del software presente (per rimuovere eventuali vulnerabilità di sicurezza);
- rimozione di eventuali servizi o software che, utilizzati in modo malevolo, possono compromettere il sistema stesso (hardening).
- In alcuni casi, come per le infezioni da virus/malware, può essere più semplice e meno oneroso economicamente, ricostruire l'intera macchina reinstallando il software a partire dal sistema operativo.

Le operazioni di rimozione possono essere particolarmente onerose in quanto potrebbe essere necessario:

- acquisire nuovo hardware o licenze software;
- utilizzare risorse interne o esterne per l'esecuzione delle operazioni di rimozione;
- eseguire dettagliati test di funzionamento sui sistemi e sulle applicazioni interessate dall'Incidente.

La valutazione dell'impatto tecnico ed economico delle operazioni di rimozione deve essere eseguita dal gruppo gestione sicurezza, eventualmente coinvolgendo tutti i soggetti interessati e fornendo al Responsabile della sicurezza tramite un report di dettaglio le indicazioni degli eventuali costi da sostenere e tempi necessari al ripristino.

I tempi necessari per poter procedere alla fase di rimozione possono essere relativamente lunghi (anche nell'ordine di 1 o 2 settimane) a causa delle necessità di approvvigionamento sopra descritte, ma non possono protrarsi all'infinito in quanto l'operazione di contenimento a lungo termine non è da considerarsi risolutiva del problema, ma solo ed esclusivamente un'azione a titolo temporaneo.

Ripristino

In questa fase le operazioni eseguite mirano principalmente a verificare che i sistemi coinvolti nell'Incidente siano stati correttamente riattivati e che siano nuovamente sicuri, per considerare l'Incidente effettivamente chiuso.

E' necessario ottenere un elevato grado di certezza che quanto accaduto non possa ripetersi, per questo motivo si rende necessario definire con il dovuto dettaglio tutte le fasi di riattivazione di un sistema coinvolto, sia nei modi che nei tempi attesi per il ripristino, sia nei controlli da effettuare per certificare il ritorno alla normalità.

Attività post-Incidente

La decisione del momento in cui un sistema coinvolto in un Incidente possa ritornare in produzione è in carico al referente per la sicurezza informatica che, in collaborazione con il gruppo gestione sicurezza ed i gruppi di supporto tecnici coinvolti, definisce un piano di riattivazione dei diversi servizi impattati dall'Incidente.

In alcuni casi specifici può essere necessario riattivare i sistemi in un periodo non lavorativo (es. nelle ore notturne oppure nei fine settimana) per dare la possibilità alle strutture che hanno in carico la gestione dei sistemi stessi di operare senza che siano presenti richieste di accesso da parte di utenti che non siano quelli deputati all'esecuzione di eventuali test di funzionamento.

Onde verificare che le operazioni di ripristino siano avvenute correttamente si rende necessario monitorare il corretto funzionamento dei sistemi per un periodo di tempo adeguato, per cui potrebbe esservi la necessità di attivare ulteriori controlli utilizzando gli strumenti di monitoraggio in uso, oppure aumentando il livello di profondità degli eventi da registrare nei file di log applicativi o dei sistemi operativi.

Sarà il referente per la sicurezza informatica a richiedere la modifica o l'implementazione di nuove regole di monitoring ai soggetti preposti.

Tutti gli incidenti di sicurezza devono essere documentati. Tale documentazione, unitamente alle evidenze degli incidenti, devono essere debitamente archiviate.

Sono documentati e archiviati, in modalità distinguibile rispetto agli incidenti di sicurezza, tutti i data breach, seppure non notificati all'Autorità Garante e/o agli interessati.
Dal punto di vista tecnico le operazioni di chiusura dell'Incidente, consistono nella dichiarazione della fine dello stato di Incidente e nella compilazione del report relativo all'Incidente stesso da parte del referente per la sicurezza informatica.
Il report, firmato dal Referente per la gestione della sicurezza informatica tramite procedura di hashing a garanzia della sua integrità, dovrà essere consegnato al gruppo sicurezza e dovrà essere inviata relazione in forma riservata sull'esito dell'Incidente di sicurezza ai vertici del Titolare o i Responsabili di settore competenti.
Il Referente per la gestione della sicurezza informatica coinvolto deve conservare il Rapporto in un repository ad accesso limitato ai membri del proprio staff, per cinque anni o per tutto il tempo ritenuto necessario (ad esempio allo svolgimento di indagini, nel caso di conseguenze penali, o perlomeno alla definitiva rimozione delle cause scatenanti l'Incidente).
In seguito alla chiusura dell'Incidente dovranno essere valutate tutte le operazioni eseguite per la gestione dello stesso, evidenziando sia i punti in cui queste sono state eseguite in armonia con le procedure e le aspettative, sia eventuali problemi sorti durante lo svolgimento delle operazioni.
Le informazioni raccolte durante la gestione dell'Incidente dovranno essere archiviate, in forma anonimizzata nella knowledge base del Titolare (consultabile ad accesso ristretto in base al ruolo ricoperto nel processo di gestione incidenti).
E' fondamentale che i punti critici rilevati durante l'esecuzione delle operazioni siano immediatamente condivisi con i componenti del team di gestione degli incidenti e si provveda nel più breve tempo possibile a predisporre quanto può essere necessario per eliminarli o mitigarli, migliorando quindi sia la procedura tecnica di gestione sia la capacità di operare della struttura preposta, sia agendo sulle infrastrutture e i sistemi.
Di seguito alcuni esempi di punti critici che possono essere rilevati:

- mancanza delle competenze tecniche per operare correttamente su un sistema o applicazione;
- mancanza degli opportuni strumenti tecnici;
- errori nella valutazione della gravità dell'Incidente o nelle sue capacità di diffusione;
- errori o difficoltà nell'interazione con soggetti interni;
- errori nella comunicazione verso terze parti o verso dipendenti e collaboratori

In particolare può essere utile porsi le seguenti domande:

- La procedura di gestione incidenti è stata correttamente eseguita? E' risultata adeguata al contesto?
- Si sono presentati aspetti che hanno rallentato la risoluzione dell'Incidente?
- Si sono presentati elementi che si ritiene siano da cambiare in modo da rendere il processo di gestione degli incidenti più efficace ed efficiente?
- E' necessario aggiornare il metodo di analisi della gravità a valle dell'Incidente?
- Sono necessarie delle azioni correttive da intraprendere in fase di mitigazione dei rischi onde evitare che l'Incidente possa riaccadere?
- E' necessario modificare le policy aziendali dal punto di vista tecnico (es.: aggiungere file con una determinata estensione tra quelli bloccati dal sistema antivirus)?
- E' necessario aggiornare e/o migliorare gli interventi formativi al fine di istruire il personale dell'Ente sulle problematiche inerenti la sicurezza e la privacy dei dati?
- Sono necessarie risorse addizionali (es.: personale, tools, strumenti hardware o software) per rendere il processo di gestione degli incidenti più efficace ed efficiente?
- Sono necessarie modifiche e/o riconfigurazioni del software (es.: aumentare frequenza di aggiornamento delle firme dei software antivirus e/o anti-intrusione e, modificare il livello di dettaglio fornito dai sistemi di difesa perimetrali)?

Questa operazione ha lo scopo di verificare che il processo di gestione incidenti sia risultato adeguato a fronteggiare la situazione e far si che le considerazioni che ne scaturiscono debbano divenire patrimonio comune all'interno del team di gestione degli incidenti.
Per questo motivo occorre che entro breve termine dalla chiusura formale di un Incidente, il referente per la sicurezza informatica convochi tutte le risorse che sono state parte attiva nella gestione, con l'obiettivo di valutare collegialmente l'efficacia della procedura di gestione degli incidenti e scrivere in un apposito verbale le considerazioni e le operazioni che possono portare a migliorare l'intera procedura.

Allegato:Rapporto Incidente di sicurezza

1. Premessa:
(breve descrizione dell'Incidente, dei sistemi coinvolti, degli utenti su cui l'Incidente ha impatto, della durata dell'Incidente, delle modalità attraverso le quali si è venuti a conoscenza dell'Incidente)

2. Descrizione dettagliata dell'Incidente:
(causa che ha determinato l'Incidente);
(sistemi coinvolti);
(eventuali disservizi causati);
(utenti coinvolti);
(eventuali enti esterni coinvolti);
(dettagli tecnici rilevanti: es. log dei sistemi, traffico di rete, schermate, e- mail, ecc.).

3. Rilevazione dell'Incidente:
(modalità attraverso le quali si è venuti a conoscenza dell'Incidente:

- *notifica automatica tramite sistemi di rilevazione*
- *individuazione a seguito di verifiche di sicurezza*
- *segnalazione da parte di un utente*
- *altro).*

4. Contromisure adottate
(descrizione delle azioni intraprese per contenere i danni causati dall'Incidente e per ripristinare i sistemi)

5. Conclusioni
(impatto dell'Incidente sui sistemi o sui servizi);
(elementi che avrebbero consentito di prevenire il verificarsi dell'Incidente);
(ulteriori azioni di approfondimento necessarie).

6. Note
(eventuali considerazioni sull'Incidente, suggerimenti, adeguamenti da effettuare, ecc.).

7. Riferimenti
(eventuali riferimenti ad allegati o altri documenti).

..... , li .....

Il Referente per la Sicurezza informatica

.....