COMUNE DI MARANO SUL PANARO
Provincia di Modena

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

Deliberazione n. 97 del 03/12/2018

OGGETTO: ADEGUAMENTO AL REGOLAMENTO EUROPEO UE/2016/679 O GDPR (GENERAL DATA PROTECTION REGULATION) - APPROVAZIONE E ADOZIONE DEL MODELLO DI GESTIONE INCIDENTI DI SICUREZZA E DEL DISCIPLINARE PER L'USO DEI SISTEMI INFORMATIVI NELL'UNIONE TERRE DI CASTELLI E NEI COMUNI ADERENTI

L'anno **duemiladiciotto** addì **tre** del mese di **dicembre** alle ore **17:30** nella Casa Comunale, previa l'osservanza di tutte le formalità prescritte dalla vigente legge comunale e provinciale, vennero oggi convocati a seduta i componenti la Giunta Comunale, che nelle persone seguenti risultano presenti alla trattazione della proposta di deliberazione in oggetto:

MURATORI EMILIA	SINDACO	Presente
GALLI GIOVANNI	VICE SINDACO	Presente
RONDELLI MAURO	ASSESSORE	Presente
DANI ELIO	ASSESSORE	Presente
ZANANTONI RITA	ASSESSORE	Presente

Presenti n. 5 **Assenti n. 0**

Partecipa il SEGRETARIO COMUNALE MARTINI MARGHERITA che provvede alla redazione del presente verbale.

Presiede la seduta, nella sua qualità di SINDACO, il Sig. MURATORI EMILIA che dichiara aperta la trattazione dell'oggetto sopra indicato.

Deliberazione n. 97 del 03/12/2018

OGGETTO: ADEGUAMENTO AL REGOLAMENTO EUROPEO UE/2016/679 O GDPR (GENERAL DATA PROTECTION REGULATION) - APPROVAZIONE E ADOZIONE DEL MODELLO DI GESTIONE INCIDENTI DI SICUREZZA E DEL DISCIPLINARE PER L'USO DEI SISTEMI INFORMATIVI NELL'UNIONE TERRE DI CASTELLI E NEI COMUNI ADERENTI

LA GIUNTA COMUNALE

PREMESSO che:

- il 25 maggio 2018 è entrato in vigore il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito GDPR) il quale ha abrogato la direttiva 95/46/CE;
- il GDPR detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, ivi comprese le pubbliche amministrazioni;
- il GDPR individua inoltre diversi attori che intervengono nei trattamenti di dati personali effettuati dalle organizzazioni, ciascuno con funzioni e compiti differenti;
- il D.lgs. n. 196/2003 "*Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*", capo IV, art. 2 *quaterdecies*, come modificato dal D.lgs. 101/2018, stabilisce che il titolare del trattamento può prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate che operano sotto la propria autorità e che il titolare del trattamento individua le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta;

RICHIAMATE le proprie precedenti deliberazioni:

- n. 98 del 20/12/2017 mediante la quale è stato nominato il Responsabile della transizione digitale nella persona della Dott.ssa Elisabetta Manzini e contestualmente sono stati individuati i contenuti dell'elenco delle Misure minime per la sicurezza ICT delle pubbliche Amministrazioni poi sottoscritti dal suddetto Responsabile entro il 31/12/2017 come prescritto dalla normativa in materia;
- n. 44 del 21/05/2018, con cui:
  - veniva designato quale Responsabile della Protezione dei Dati (RPD) del Comune di Marano sul Panaro la società Lepida S.p.A., con sede in Bologna – Via della Liberazione, 15 - 40128 Bologna;
  - veniva individuato quale Referente dell'Ente, incaricato di operare in qualità di coordinatore delle attività nei confronti dei soggetti interni e dialogare direttamente con il Responsabile della Protezione dei Dati (RPD), il Responsabile del Settore Amministrativo del Comune;
- n. 48 del 6/06/2018, con cui veniva adottato un modello organizzativo volto a presidiare il trattamento dei dati personali, dando atto del ruolo di supporto svolto dal Servizio "Sistemi Informativi" in collaborazione con il Referente dell'Ente nei confronti del RPD in tema di risorse strumentali e competenze e nel segnalare le eventuali violazioni dei dati ai fini della notifica al Garante;

RICHIAMATI inoltre:

- gli artt. 32 e 33 del GDPR che dispongono rispettivamente che devono essere approntate misure tecniche e organizzative adeguate per garantire un livello adeguato di sicurezza dei dati personali e che in caso di violazione dei dati personali, il titolare deve notificare tale violazione all'Autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza;

- le "*Linee Guida sulla notifica delle violazioni dei dati personali ai sensi de regolamento (UE) 2016/679*", adottate il 3 ottobre 2017, poi emendate ed adottate in data 6 febbraio 2018 dal Gruppo di lavoro articolo 29 per la protezione dei dati personali (cioè l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata) nelle quali vengono forniti dettagli sugli obblighi di notifica e di comunicazione delle violazioni sanciti dal GDPR, nonché alcune misure che i titolari del trattamento possono adottare per soddisfare i nuovi obblighi;

CONSIDERATO che in tema di sicurezza del trattamento dei dati personali il GDPR stabilisce che:

- le misure tecniche ed organizzative adottate dal Titolare del trattamento devono poter garantire un livello di sicurezza *adeguato* al rischio, tenuto conto di:
  - stato dell'arte e costi di attuazione;
  - natura, oggetto, contesto e finalità di trattamento;
  - rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche;
- nella valutazione dei livelli di sicurezza occorre tener conto dei rischi del trattamento derivanti da: distruzione, perdita, modifica, divulgazione non autorizzata, accesso accidentale o illegale ai dati personali trasmessi, conservati o comunque trattati;
- nel caso di violazione di dati personali (c.d. *data breach*), il Titolare dovrà procedere alla sua notifica al Garante, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui viene rilevata, previa valutazione dei rischi per i diritti e le libertà degli interessati;

DATO ATTO che la corretta gestione degli incidenti di sicurezza permette di evitare o minimizzare la compromissione dei dati dell'Ente 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;

DATO ATTO inoltre che la nuova normativa europea fa carico alle Pubbliche Amministrazioni di non limitarsi alla semplice osservanza di un mero adempimento formale in materia di privacy, conservazione e sicurezza dei dati personali, ma attua un profondo mutamento culturale e concettuale con un rilevante impatto organizzativo da parte dell'Ente nell'ottica di adeguare le norme di protezione dei dati ai cambiamenti determinati dalla continua evoluzione delle tecnologie (*cloud computing*, digitalizzazione, social media, cooperazione applicativa, interconnessione di banche dati, pubblicazione automatizzata di dati on line) nelle amministrazioni pubbliche;

RITENUTO, pertanto, necessario realizzare un "modello organizzativo" sulla base di una preliminare analisi dei rischi e di un'autovalutazione finalizzata all'adozione delle migliori strategie volte a presidiare i trattamenti di dati effettuati, abbandonando l'approccio meramente formale del D.Lgs. 196/2003, limitato alla mera adozione di una lista "minima" di misure di sicurezza, realizzando, piuttosto, un sistema organizzativo caratterizzato da un'attenzione multidisciplinare alle specificità della struttura e della tipologia di trattamento, sia dal punto di vista della sicurezza informatica e in conformità agli obblighi di legge, sia in considerazione della gestione dei dati trattati. Tutto questo prevedendo, al contempo, non solo l'introduzione di nuove figure che dovranno presidiare i processi organizzativi interni per garantire un corretto trattamento dei dati personali, tra cui ad es. la figura del Responsabile della Protezione dei dati personali (RPD), ma altresì l'adozione di nuove misure tecniche ed organizzative volte a garantire l'integrità e la riservatezza dei dati, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, nonché la verifica e la valutazione dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

RITENUTO NECESSARIO quindi adottare uno specifico documento che, tenuto conto dell'organizzazione dell'Ente, disciplini all'interno del Comune l'uso dei sistemi informativi e fornisca indicazioni tecniche ed organizzative da applicare per garantire la sicurezza dei dati trattati con strumentazioni informatiche, nonché uno specifico documento che in caso di incidenti di sicurezza, informatica e non, che possono occorrere ai servizi e ai dati gestiti dal Comune, ne regolamenti la gestione;

TENUTO CONTO che la gestione dei servizi informativi è stata delegata all'Unione Terre di Castelli ma che l'interazione tra il Servizio Sistemi Informativi e i servizi/uffici dell'Ente è continua e costante;

VISTO l'allegato "Disciplinare per l'uso dei sistemi informativi nell'Unione Terre di Castelli e nei Comuni aderenti" (all. A) volto a fornire una disciplina sull'uso dei sistemi informativi che si propone anche lo scopo di impedire, o comunque ridurre, il rischio che eventuali problemi di sicurezza su una postazione o su un punto della rete si propaghino sfruttando l'interconnettività e l'interdipendenza fra le componenti del sistema informativo del Comune;

VISTO inoltre l'allegato modello di gestione degli incidenti di sicurezza (All. B) che oltre a prevedere la costituzione di una struttura operativa competente (c.d. "gruppo per la Gestione della Sicurezza ICT") in

grado di intervenire secondo le procedure operative prestabilite, individua, con specifico riferimento all'obbligo di cui all'art. 33 del GDPR n. 679/2016:

- le violazioni dei dati personali (c.d. *data breach*) che ricadono nell'ambito della normativa in materia di protezione dei dati, tenendo conto del fatto che tutte le violazioni dei dati personali sono incidenti di sicurezza, ma non tutti gli incidenti di sicurezza sono necessariamente violazioni di dati personali;
- i casi in cui l'Ente deve notificare i *data breach* al Garante ed agli interessati;
- le misure atte a trattare il rischio e la documentazione da produrre;

VALUTATO che la struttura operativa deputata ad intervenire secondo le procedure operative prestabilite (c.d. "gruppo per la Gestione della Sicurezza ICT") debba essere costituita dalle seguenti figure:

- un dipendente del Servizio "Sistemi Informativi" dell'Unione;
- il Responsabile del Settore Amministrativo, già incaricato, con la richiamata deliberazione di Giunta n. 44 del 21.05.2018, quale referente nei rapporti con il RPD dell'Unione;
- il Responsabile del Settore nell'ambito del quale si è verificato la violazione;
- eventuali altri soggetti coinvolti nel trattamento dei dati oggetto di violazione che il gruppo riterrà necessario interessare a seconda della tipologia di incidente e della tipologia di dati coinvolti;

VISTO il parere reso dal RPD dell'Unione, prot. UNI n. 46097 del 9.11.2018, che ha confermato la coerenza del documento con i principi del GDPR;

RITENUTO, infine, in attuazione dell'art. 33, paragrafo 5, del GDPR (il quale prevede che il titolare del trattamento "*documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per provi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo*") ed in ossequio al principio di *accountability* come suggerito dalla Linee guida in materia adottate dal Gruppo di lavoro articolo 29 per la protezione dei dati, di istituire un registro interno delle violazioni in cui documentare tutte le violazioni, sia quelle notificabili che non notificabili, da tenere a cura del Responsabile del Settore Amministrativo, nella sua funzione di componente del Gruppo per la Gestione della sicurezza nonchè referente nei rapporti con il RPD dell'Unione;

VISTI:

- il D.Lgs. n. 267/2000;
- il GDPR 2016/679, ed in particolare gli artt. 32, 33 e 34 del Regolamento europeo;
- il D.Lgs. n. 196/2003, nel testo integrato con le modifiche introdotte dal D.Lgs. n. 101/2018;
- le "*Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679*", adottate il 3 ottobre 2017 ed emendate ed adottate in data 6 febbraio 2018 dal Gruppo di lavoro articolo 29 per la protezione dei dati;
- lo Statuto Comunale;
- il vigente Regolamento degli uffici e dei Servizi;

VISTO il parere favorevole espresso ai sensi dell'art. 49, comma 1, e dell'art. 147 bis, comma 1, del D.Lgs. n. 267/2000 dal Responsabile del Settore Amministrativo in merito alla regolarità tecnica della proposta di deliberazione di cui sopra, parere allegato al presente atto quale parte integrante e sostanziale dello stesso;

DATO ATTO che ai sensi dell'art. 49, comma 1, del medesimo D.Lgs. n. 267/2000 il Responsabile del Settore Economico Finanziario non ha espresso alcun parere sulla regolarità contabile della proposta in oggetto in quanto la stessa è priva di rilevanza contabile e finanziaria;

Con voto unanime, favorevolmente espresso nei modi e forme di legge;

DELIBERA

1) Di approvare il "**Disciplinare per l'uso dei sistemi informativi nell'Unione Terre di Castelli e nei Comuni aderenti**", allegato al presente atto quale parte integrante e sostanziale (**all. A**), rivolto di impedire, o comunque ridurre, il rischio del verificarsi di problemi di sicurezza;
2) Di approvare, in attuazione degli adempimenti previsti dal Regolamento Europeo UE/2016/679, il "**Modello di gestione degli incidenti di sicurezza**", allegato al presente atto quale parte integrante e sostanziale (**all. B**) che definisce le procedure che il Comune di Marano sul Panaro adotta in caso di violazione dei dati personali;
3) Di disporre, contestualmente all'approvazione, l'immediata adozione da parte dell'Ente del suddetto modello che prevede, tra l'altro, la costituzione di una struttura operativa (c.d. "Gruppo per la Gestione della Sicurezza ICT") deputata ad intervenire in caso di incidente di sicurezza secondo le procedure operative prestabilite e costituita dalle seguenti figure:

- un dipendente del Servizio “Sistemi Informativi” dell'Unione;
- il Responsabile del Settore Amministrativo, già incaricato, con la richiamata deliberazione di Giunta n. 44 del 21.05.2018, quale referente nei rapporti con il RPD dell’Unione;
- il Responsabile del Settore nell’ambito del quale si è verificato la violazione;
- eventuali altri soggetti coinvolti nel trattamento dei dati oggetto di violazione che il gruppo riterrà necessario interessare a seconda della tipologia di incidente e della tipologia di dati coinvolti;

4) Di disporre, in attuazione dell’art. 33, paragrafo 5, del GDPR e delle “*Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679*” adottate dal Gruppo di lavoro articolo 29 per la protezione dei dati, in ossequi al principio di *accountability*, la tenuta di un apposito “**Registro delle violazioni di dati personali**” secondo il modello allegato (**all. C**) a cura del Responsabile del Settore Amministrativo;
5) Di pubblicare nella rete intranet dell’Ente, in apposita sezione, il presente atto, unitamente alla indicazione dei riferimenti di contatto del “Gruppo per la Gestione della Sicurezza ICT” nonché della procedura da attivare in caso di sospetta violazione di dati personali.

INDI

LA GIUNTA COMUNALE

Successivamente con votazione unanime e palese

stante l’urgenza di procedere per consentire il tempestivo adeguamento dell’Ente alle disposizioni del Regolamento Europeo UE/2016/679 in materia di sicurezza dei dati personali.

DELIBERA

- di rendere immediatamente eseguibile la presente deliberazione, ai sensi dell’art. 134, 4° comma del D.Lgs. 18 agosto 2000, n. 267

COMUNE DI MARANO SUL PANARO
Provincia di Modena

Letto, approvato e sottoscritto digitalmente ai sensi dell'art. 21 D.L.gs n 82/2005 e s.m.i.

IL SINDACO	IL SEGRETARIO COMUNALE
MURATORI EMILIA	MARTINI MARGHERITA

Disciplinare per l'uso dei sistemi informativi nell'Unione Terre di Castelli e nei comuni aderenti

Parte I – Aspetti generali e comportamentali

Art. 1 - Finalità del presente documento

Il presente documento rientra tra le misure minime adottate dalle amministrazioni entro il 31/12/2017 in attuazione della Direttiva 1 agosto 2015 del Presidente del Consiglio dei Ministri e intende fornire indicazioni tecniche ed organizzative da applicare per garantire la sicurezza dei dati trattati con strumentazioni informatiche.

Finalità del presente documento è permettere una crescita tecnologica ed organizzativa dei sistemi informativi dei Comuni dell'Unione Terre di Castelli, in un'ottica di omogeneità tecnologica e di sviluppo, al fine di estendere l'uso delle tecnologie sia nell'organizzazione degli enti che nel rapporto con cittadini, professionisti e imprese, senza mettere a rischio la sicurezza dell'intero sistema; la corretta applicazione di regole comuni e condivise ha lo scopo di impedire, o comunque ridurre il rischio che eventuali problemi di sicurezza su una postazione o su un punto della rete si propaghino sfruttando l'interconnettività e l'interdipendenza fra le componenti del sistema informativo dell'Unione.

Art. 2 - Ambito di applicabilità

L'ambito di applicabilità è esteso a tutti i soggetti che utilizzano postazioni di lavoro e operano sui dati e sulle informazioni contenute in elaboratori elettronici: dipendenti, collaboratori, amministratori, imprese che hanno rapporti contrattuali con l'Ente o altri soggetti che ne abbiano titolo.

Quanto riportato nel presente documento non esaurisce la disciplina applicabile, dovendosi garantire il rispetto di tutte le prescrizioni contenute nelle vigenti normative civili e penali.

Art. 3 - Definizioni

Di seguito vengono fornite alcune definizioni per rendere più comprensibile il documento.

Sistema Informativo: complesso di strumentazioni hardware e sistemi software.

Struttura Sistemi Informativi (di seguito SI): organizzazione all'interno dell'Unione Terre di Castelli che, in base alle vigente convenzione, gestisce la funzione informatica dei Comuni dell'Unione.

Comitato SI: tavolo, costituito ai sensi della Convenzione vigente, al quale partecipa un rappresentante per ogni comune. I membri del Comitato SI mantengono i rapporti di comunicazione tra SI e Comuni.

Referente del Comune: rappresentante del Comune nel comitato che cura i rapporti tra il Comune e il SI. Di solito è una figura apicale del suo comune e nell'attività di comunicazione può essere supportato da altro dipendente con funzioni operative.

Rete sovracomunale interna (o rete interna): rete informatica accessibile dai locali dei Comuni e dell'Unione.

Rete esterna: rete pubblica a cui accedono ordinariamente cittadini, imprese e professionisti, in sostanza la rete Internet.

Rete intracomunale locale : rete informatica che permette la trasmissione dati tra le sedi sul territorio dello stesso dei Comune.

Rete intracomunale territoriale : rete informatica che permette la trasmissione dati tra le sedi dei Comuni appartenenti all'Unione Terre di Castelli.

Rete intranet: rete informatica che permette la trasmissione dati tra le reti intercomunali locali e intercomunali territoriali, (intra.uni.priv).

Firewall: dispositivi fisici o logici che separano la rete esterna da quella interna ai fini di proteggere la rete interna.
Utilizzatori dei sistemi informativi : dipendenti, collaboratori stabili (stagisti, borse lavoro, contratti di lavoro temporaneo), amministratori (Sindaci e Assessori), Consiglieri. Gli utilizzatori accedono con profili diversi al sistema in base alle funzioni svolte sia di tipo tecnico che politico.
Utilizzatori occasionali: sono soggetti che accedono occasionalmente alla rete interna, quali ad esempio fornitori.
Operatori del servizio informatico : tecnici del servizio informatico che con profili diversi svolgono le funzioni di amministratore dei sistemi informatici: rete, server, database, ecc.
Postazione di lavoro (o postazione client) : computer fisso o mobile utilizzato per l'attività lavorativa.
Postazione di lavoro virtuale: computer a cui non è associabile in modo diretto un sistema hardware accessibile fisicamente all'utilizzatore; la postazione di lavoro virtuale viene utilizzata solitamente con un collegamento di una postazione fisica e ha le stesse funzionalità della postazione di lavoro ordinaria.
Server : computer utilizzato per fornire servizi a più utilizzatori della rete interna. Non prevede di solito la connessione diretta degli utilizzatori come avviene per le postazioni di lavoro fisiche o virtuali.
Data Center : struttura utilizzata per alloggiare sistemi informatici costituiti da server, dispositivi di archiviazione e apparati di telecomunicazioni.
Sistema di LOG : insieme di file che raccolgono gli eventi di un determinato programma o sistema, esempio il flusso di posta elettronica inviata e ricevuta o siti internet visitati, in caso di indagini per reati informatici http://www.commissariatodips.it la polizia postale ne richiede la visione.
Coordinatore interno per la protezione dei dati: ai sensi del nuovo GDPR, è persona fisica interna all'Ente, nominata dal Titolare al trattamento di dati personali (art. 29 D. Lgs. n. 196/2003).
Responsabile del trattamento: ai sensi del nuovo GDPR è la persona fisica o giuridica che effettua i trattamenti per conto del titolare designata con apposito atto dal Titolare stesso o da suo delegato ai sensi dell'art. 28 del GDPR stesso.

Art. 4 - Sicurezza fisica dei locali
L'accesso ai locali e alle postazioni di lavoro è riservato agli utilizzatori in base alle funzioni loro assegnate. L'accesso di personale esterno (quale, ad esempio, fornitori dell'Ente), che per necessità dovesse utilizzare in modo estemporaneo la postazione di lavoro, dovrà essere concordato e autorizzato dalla Struttura Sistemi Informativi ed avviene sotto la responsabilità dell'utilizzatore interno che ne richiede l'intervento.

Art. 5 - Accesso e utilizzo delle postazioni di lavoro
L'accesso alle postazioni di lavoro avviene con account (credenziale) personale e nominativa, ad esclusione di quelle postazioni che, per particolari esigenze di rotazione, consentono l'accesso con un account che identifica il servizio. La parte riservata delle credenziali di accesso (password, pin o altro) viene modificata periodicamente in base alle disposizioni della normativa vigente. Ogni utilizzatore è responsabile della custodia delle password e delle altre credenziali personali di accesso ai sistemi. E' fatto divieto di cedere, o rendere facilmente accessibili, i propri identificativi personali segreti a soggetti terzi.

Le postazioni di lavoro sono fornite dall'Ente (Comune di competenza o Unione). Gli utilizzatori non possono attivare postazioni di lavoro di proprietà nella rete interna, salvo specifica autorizzazione del SI.
L'abilitazione alla rete interna permette l'utilizzo di tutte le postazioni di lavoro fisiche o virtuali. Le autorizzazioni sono assegnate agli utenti e non alle postazioni che sono tendenzialmente intercambiabili, almeno per le funzioni di base.
Quando un utente cessa il servizio presso l'ente, deve essere inviata tempestiva comunicazione al SI e il suo accesso non può essere ceduto ad un altro utente; i dati importanti devono essere memorizzati sulle cartelle di rete condivise. L'accesso verrà disattivato dal SI alla ricezione della comunicazione e verrà cancellato definitivamente dopo 30 giorni.

Art. 6 - Accesso dall'esterno

L'accesso alla rete interna dall'esterno in generale è vietato; può essere abilitato solo a seguito di specifica richiesta scritta:

- per gli amministratori, i dirigenti e i responsabili apicali da parte dell'interessato;
- per i dipendenti che non abbiano funzioni apicali da parte del dirigente o del responsabile apicale dell'area di riferimento.

L'accesso non è immediato ed automatico, ma avviene dopo l'esito favorevole di un'istruttoria effettuata dall'SI allo scopo di verificare le prestazioni minime indispensabili della connettività utilizzata; oltre a ciò, l'accesso è autorizzato solo tramite postazioni di lavoro fornite dall'ente;

Art. 7 - Utilizzo delle postazioni di lavoro

La proprietà delle postazioni di lavoro è dell'Amministrazione (Comune o Unione) e l'utilizzo è consentito unicamente per i fini lavorativi e istituzionali inerenti l'utilizzatore.
L'utilizzatore non vanta alcun diritto sulla postazione di lavoro e non può memorizzarvi dati personali che non abbiano attinenza con l'attività lavorativa o istituzionale.
Gli utilizzatori salvano i dati nelle unità di rete appositamente predisposte; non è garantito il salvataggio dei dati memorizzati sulla postazione di lavoro locale, né è garantito il passaggio di tali dati, in caso di sostituzione della postazione. I dati memorizzati sulla postazione di lavoro locale non sono soggetti a nessuna politica di backup.
Gli operatori possono richiedere anche l'attivazione di una cartella personale, sempre sul server di rete, nella quale poter memorizzare dati che richiedono il massimo livello di riservatezza. La quota per ciascuna cartella è di 50 Gb.
Gli operatori che hanno un accesso roaming per particolari esigenze di servizio (servizio sociale professionale, polizia municipale, biblioteca di Vignola) non possono attivare la cartella di archiviazione in quanto i loro documenti sono già salvati in automatico su un server. Lo spazio complessivo per ogni utente roaming è di 100 Gb.
Per particolari esigenze di servizio, dovranno essere adottate specifiche politiche di salvataggio dei dati per gli operatori che utilizzano le postazioni di lavoro mobili in accordo con il servizio informatico.
Alla fine della sessione di lavoro gli utilizzatori spengono la postazione oppure, in subordine, effettuano la semplice disconnessione dalla rete, lasciando acceso il computer, nel caso siano necessari collegamenti remoti successivi.

In caso di momentaneo abbandono della postazione di lavoro, qualora ciò non avvenga automaticamente, gli utilizzatori sono tenuti a bloccare la postazione stessa in modo che altri soggetti per accedervi debbano inserire le credenziali.
La postazione di lavoro non può essere collocata al pavimento o in posizioni che ne possono compromettere il funzionamento, (adiacenti a stufe elettriche o termosifoni, a piante che vengono regolarmente annaffiate, sotto finestre aperte).
La postazione di lavoro non deve mai essere scollegata dalla rete e sostituita da altri dispositivi da personale non autorizzato da SI, e neppure collegate a reti diverse da quella per la quale la postazione è identificata.

Art. 8 - Utilizzo di dispositivi mobili

L'utilizzo delle postazioni di lavoro portatili e mobili (notebook, tablet, smartphone) richiede maggiori precauzioni rispetto alle postazioni fisse in ordine ai seguenti elementi:

- attenzione rispetto al furto o allo smarrimento delle stesse;
- attenzione rispetto a virus o codici maligni tramite reti wireless (senza fili);

Le postazioni di lavoro mobili vengono acquistate per esigenze di lavoro specifiche in cui l'utilizzatore ha necessità di frequenti spostamenti, ed assegnate in accordo con i responsabili dei servizi interessati. Si ribadisce il divieto di installare sulle postazioni mobili software non compresi nell'elenco di cui all'art.9.

Art. 9 - Utilizzo del software

Ogni necessità di software sulla postazione di lavoro deve essere comunicata a SI, la quale provvederà a redigere, pubblicare ed aggiornare l'elenco dei software autorizzati, oltre ovviamente ad installare il software sulle postazioni richieste.

L'utilizzo del software avviene nel rispetto del diritto d'autore. Chi richiede l'installazione di un software deve avere acquisito la licenza d'uso ove prevista, o comunque fornire agli operatori SI i relativi termini di licenza o d'uso.

Vige il divieto assoluto di installazione di software da parte degli utilizzatori, salvi differenti e specifici accordi con SI; tale attività è riservata agli operatori SI che ne verificano preventivamente la compatibilità con i sistemi esistenti.

Art. 10 - Assegnazione delle caselle di posta elettronica

I dipendenti e i collaboratori che utilizzano le postazioni di lavoro della rete interna hanno a disposizione una casella di posta elettronica personale o d'ufficio in base ai criteri organizzativi definiti dall'Ente.

La casella di posta elettronica assegnata, personale o relativa all'ufficio, contiene nella parte relativa al dominio il riferimento all'ente di appartenenza. L'utilizzo della casella assegnata avviene per fini istituzionali o per comunicazioni personali attinenti l'attività lavorativa.

Per attivare la condivisione di una casella di posta (solitamente d'ufficio) che deve essere consultata da più persone, il responsabile del servizio inoltra apposita richiesta al SI, che attiva il meccanismo di condivisione via software; il responsabile del servizio ha anche i compito di comunicare eventuali variazioni riguardanti le condivisioni ed eventuali utenti non più attivi nel suo servizio.

A tutti i dipendenti, assessori e consiglieri viene fornita una casella di posta elettronica personale, fatti salvi specifici impedimenti di natura tecnica e organizzativa del soggetto interessato.

I dipendenti sono tenuti ad utilizzare la posta personale fornita per le comunicazioni con l'Ente preferendola rispetto ad altre caselle fornite da soggetti esterni (ad esempio per le comunicazione con l'ufficio personale).

Art. 11 - Utilizzo e gestione della posta elettronica

Gli utenti delle caselle di posta devono rispettare alcune semplici regole:

- nell'invio della posta elettronica gli utenti devono includere tra i destinatari solo gli indirizzi strettamente necessari e cercare di limitare la diffusione di indirizzi di posta elettronica di colleghi o terzi, in quanto tale operazione favorisce la diffusione dello spamming (mail spazzatura);

- per lo stesso motivo e per l'inutile occupazione di spazio sui server sono vietate le cosiddette "Catene di Sant'Antonio" ovvero l'inoltro a varie persone di messaggi che contengono informazioni apparentemente utili e relativi a lodevoli iniziative che si rivelano di solito come bufale;
- è fatto divieto di utilizzare la casella di posta rilasciata dall'ente per iscriversi a servizi di vendita e/o offerte, newsletter e similari non attinenti al proprio servizio;
- è buona norma attivare per lo stretto tempo necessario, la funzione fuori ufficio, qualora ci si assenti dal servizio;
- quando un utente cessa il servizio presso l'ente, deve essere inviata comunicazione al SI e la sua casella di posta personale non può venire ceduta ad un altro utente; deve essere invece attivato il messaggio di fuori ufficio a cura dell'utente stesso che indichi chiaramente che il dipendente non è in servizio;

Il SI definisce le politiche per la conservazione e l'archiviazione dei messaggi di posta elettronica in modo da permetterne la corretta fruizione da parte degli utilizzatori nel rispetto dell'equilibrio complessivo e dimensionamento dei sistemi.
La posta elettronica è un sistema di comunicazione e non di archiviazione delle informazioni, pertanto gli utilizzatori devono, al fine di un migliore utilizzo globale, limitare la crescita della dimensione complessiva della casella, effettuando periodicamente la cancellazione delle e-mail non più necessarie.
Il SI attiva funzioni di controllo antispam e antivirus sui messaggi di posta elettronica sia in entrata che in uscita e traccia attraverso sistema di LOG tutte le mail che transitano sul sistema di posta.

Art. 12 - Navigazione internet

Come prescritto dal Piano Triennale per l'informatica nella Pubblica Amministrazione (cap.3.2) è garantito "l'accesso alla rete Internet a **tutti i dipendenti della PA**, indipendentemente dal ruolo o dai compiti assegnati e senza limiti di tempo o orari. Internet oggi deve essere considerato a tutti gli effetti uno strumento di lavoro indispensabile ed efficace per svolgere ogni tipo di attività: dal trovare numeri di telefono, all'identificare persone e relazioni tra queste persone, riferimenti di un concorso o normativi, documentazione tecnica, strumenti di produttività (traduzioni, orari nel mondo, ecc.), servizi di emergenza o notizie di ogni tipo."
L'accesso a social network, forum, chat o simili è consentito unicamente, previa analisi appunto delle necessità organizzative, su richiesta del responsabile del servizio e in accordo con il SI su tempi e modi di attivazione.
La navigazione in internet è oggi considerata uno strumento per l'attività lavorativa e a tale fine deve essere utilizzata. Il SI predispone un servizio di filtro automatico dei contenuti (content filtering) finalizzato ad evitare siti potenzialmente dannosi e dal contenuto pericoloso. Il sistema di content filtering è aggiornato automaticamente sulla base di un software che tiene conto delle principali black list pubblicate sul web; tale sistema non esaurisce l'elenco dei siti sconsigliati, in quanto variabile ad altissima velocità, intende solo fornire una indicazione di massima; si lascia alla responsabilità dei singoli utilizzatori l'individuazione dei siti corretti sui quali navigare e si raccomanda estrema prudenza nel collegamento a siti sconosciuti.
La classificazione automatica dei siti rischiosi può comportare anche il blocco di siti che in realtà non lo sono, pertanto, in caso il blocco riguardi un sito non pericoloso,

indispensabile per lo svolgimento delle proprie attività, l'utente può chiedere al SI lo sblocco del sito stesso.
Il SI, conformemente alle normative vigenti, mantiene il log dell'attività di navigazione su tutta la rete; **la consultazione dello stesso log è ammessa solo** dietro richiesta delle autorità di polizia postale secondo le norme vigenti.

Art. 13 - Utilizzo di applicazioni internet su dispositivi fissi e mobili
È in generale impedito attraverso content filtering l'utilizzo di programmi ludici, di intrattenimento tramite Internet, file sharing e peer to peer (giochi, chat, ecc.) in quanto tali sistemi, a prescindere dall'impatto sull'attività lavorativa, possono contenere vulnerabilità tali da permettere attacchi informatici con l'obbiettivo di diminuire la sicurezza complessiva del sistema informativo dell'ente.
Chi avesse necessità di utilizzare tali sistemi per fini istituzionali dovrà concordarne preventivamente l'utilizzo con il SI.

Art. 14 - Attività di supporto del servizio informatico
Il SI effettua, tramite personale proprio o fornitori di fiducia, l'attività di supporto nell'utilizzo dei sistemi informativi. Le richieste di assistenza vengono attivate tramite l'apposito strumento per le segnalazioni predisposto sulla Intranet dell'Unione all'indirizzo http://intra.uni.priv.
Per effettuare assistenza gli operatori del SI utilizzano, nei limiti del possibile, sistemi di accesso e controllo remoto delle postazioni di lavoro. L'accesso remoto alle postazioni di lavoro avviene sempre di comune accordo tra l'utilizzatore della postazione e l'operatore del SI.

Art. 15 - Attività di supporto di software house e fornitori esterni
I fornitori di software possono fornire assistenza anche tramite collegamenti da remoto secondo le modalità concordate con il SI. Il collegamento avviene in modo presidiato a seguito di specifica autorizzazione degli operatori del SI. Nel caso in cui l'accesso avvenga in modo diretto l'identificazione deve avvenire in modo personalizzato.
Qualora i fornitori o altri soggetti esterni debbano effettuare attività sulle postazioni di lavoro degli utilizzatori o sui server per installazioni e configurazioni, tali attività dovranno essere concordate preventivamente con il SI.

Art. 16 - Accesso ai dati e alle risorse di rete
L'attivazione di nuovi utenti e le impostazioni per l'accesso ai dati vengono effettuate dal personale del SI a seguito di richiesta da parte del coordinatore interno del servizio di riferimento che provvede, a norma di legge ad aggiornare di conseguenza il registro dei trattamenti, tenuto ai sensi del GDPR.
L'abilitazione alle applicazioni e l'assegnazione di funzioni all'interno dell'applicazione vengono effettuate dal coordinatore interno relativo al servizio a cui l'applicazione si riferisce. Tale attività può essere fatta anche dagli operatori del SI a seguito di istruzioni dettagliate al fine di avere una migliore organizzazione complessiva.
I coordinatori interni dei servizi, comunicano tempestivamente al SI i nominativi degli utilizzatori che devono essere disabilitati e/o le funzioni che devono essere modificate in seguito alla cessazione o mutazione del rapporto lavorativo o istituzionale o variazione di pianta organica.

Art. 17 - Gestione dei registri degli accessi
L'accesso ai sistemi, le operazioni di navigazione, l'invio dei messaggi di posta elettronica (non il testo stesso) vengono registrati nei log (registri) di sistema che sono conservati in base alle normative vigenti. Tali log non sono essere utilizzati per controllo specifico da parte degli operatori del SI, ma possono essere utilizzati per statistiche generali finalizzate

al miglior funzionamento complessivo del sistema. I log di sistema sono disponibili per le richieste dell'autorità giudiziaria.

Art. 18 - Tutela della Privacy

Ogni operazione di trattamento dei dati avviene solo tramite archivi attinenti al proprio lavoro, nel rispetto della normativa vigente in materia di privacy e alle indicazioni del Titolare dei dati e del coordinatore interno relativo al proprio servizio, che darà le opportune disposizioni. Si richiede particolare precauzione nelle memorizzazione di informazioni contenenti dati personali e/o sensibili e nell'uso di cartelle ad accesso condiviso.

Parte II – Aspetti organizzativi ed economici

Art. 19 - Architettura complessiva dei sistemi informativi

L'architettura tecnologica dei sistemi informativi è definita da SI in base agli indirizzi degli organi politici ed alle necessità tecniche.

L'Unione Terre di Castelli e i comuni associati favoriscono l'utilizzo di formati aperti anche nei rapporti con i cittadini e, dove tecnicamente possibile e conveniente, la diffusione di sistemi open source e il riuso del software sia tra i comuni dell'Unione che in ambiti territoriali più ampi (ad esempio Provincia, Regione, altre Unioni)

Il SI ha come indirizzo l'installazione centralizzata dei software sul DATA CENTER dell'Unione e l'utilizzo di postazioni di lavoro il più possibile semplificate.

Al fine di razionalizzare i costi e gli spazi, nonché per una migliore organizzazione, sono preferibili stampanti di rete per uffici e gruppi di lavoro omogenei; l'utilizzo di stampanti direttamente connesse alla postazione di lavoro è utilizzato solo per reali particolari necessità.

Art. 20 - Acquisizione di nuovi sistemi informativi

Sulla base della convenzione per il conferimento dei servizi, e della deliberazione n.35 del 5 aprile 2018, l'acquisto di nuovi software deve essere effettuato seguendo principi di omogeneizzazione e standardizzazione, al fine di mantenere omogeneità tecnologica, verificare la compatibilità tecnica e contenere la spesa corrente inerente i contratti di manutenzione, con esclusione di acquisti inderogabili dovuti ad adeguamenti normativi.

Al fine di attuare corrette previsioni di bilancio, ed una programmazione delle procedure di acquisto i comuni comunicano al Responsabile del SI le necessità del proprio ente ed eventuali modifiche contrattuali previste per l'anno successivo che si rendano necessarie.

Art. 21 - Comitato Servizio Informatico Associato

Il Comitato SI è il tavolo composto dal Responsabile e da un operatore del SI e dal Responsabile per la transizione digitale di ogni comune.

L'obiettivo del Comitato è quello di evidenziare le priorità di sviluppo dei sistemi informativi e monitorare le attività in corso, concordare regole e azioni comuni ed omogenee.

Il Comitato è quindi la sede naturale per lo scambio di comunicazioni tra il SI e i comuni.

Il Responsabile per la Transizione digitale può partecipare direttamente oppure tramite soggetto delegato, anche in base all'argomento trattato nella seduta. Il Comitato viene

convocato almeno una volta all'anno dal Responsabile del SI. Il Comitato può essere convocato anche su richiesta di uno dei componenti.

Parte III - Disposizioni finali e transitorie

Art. 22 - Modalità di diffusione del presente documento

Il presente documento viene portato a conoscenza di tutti i dipendenti ed utilizzatori dei sistemi informativi, e rimarrà pubblicato in modo definitivo sulla intranet del comune, insieme ad eventuali modifiche.

Verrà anche presentato direttamente agli operatori in modo da renderli edotti relativamente ai passaggi più tecnici e alle motivazioni da cui è scaturito.

Nel rispetto e nei limiti del presente documento, ulteriori elementi di dettaglio potranno essere emanati dal Responsabile dell' SI.

Modello di gestione incidenti di sicurezza

Approvato con deliberazione G.C. n. ___ del __/__/____

Sommario

Premessa

Il presente documento rappresenta il riferimento del Comune di Marano sul Panaro 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 l'Ente 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 dall'Ente.
L'ambito di applicazione è rappresentato da sistemi ICT dell'Ente 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 dell'ente.
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 Regolamento stesso.
Il presente documento è applicabile alle risorse ed ai servizi di tipo informatico gestiti in modo diretto oppure esternalizzato da parte del Comune di Marano sul Panaro.

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 distruzione 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 l'Ente 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 l'Ente 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 dettagliata nel seguito.
L'Ente 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 decorre dal momento in cui l'Ente 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.
L'Ente può tardare la notifica all'Autorità Garante nei casi in cui tale notifica possa produrre effetti negativi sugli individui.
Nei casi in cui l'Ente 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.
L'Ente utilizza lo strumento più efficace affinché 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.
L'Ente individua il gruppo per la Gestione della Sicurezza ICT che sarà costituito di volta in volta dalle seguenti figure:

1) **Servizio Sistemi Informativi dell'Unione Terre di Castelli**, con le seguenti competenze:
- rappresentare il primo 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;
- garantire la disponibilità delle liste di contatti (es.: personale dipendente, collaboratori, fornitori) necessarie per la gestione di un incidente di sicurezza;
- collaborare affinché il processo di gestione incidenti sia sempre adeguato alle esigenze dell'Ente, provvedendo che sia sempre aggiornato;
- individuare e proporre eventuali misure organizzative idonee al miglioramento della sicurezza dei trattamenti dei dati personali;
- individuare e proporre eventuali misure tecniche idonee al miglioramento della sicurezza dei trattamenti dei dati personali.

2) **un Rappresentante dell'Ente** in cui si verifica l'incidente che viene individuato nel dipendente già incaricato quale coordinatore delle attività di adeguamento al GDPR nonché incaricato di dialogare direttamente con il RPD. Tale Rappresentante ha le seguenti competenze:
- attivare e convocare il gruppo incidenti di sicurezza previo preliminare confronto con il Servizio Sistemi Informativi dell'Unione Terre di Castelli nel momento in cui viene a conoscenza di un incidente di sicurezza;
- condividere unitamente al Servizio Sistemi Informativi dell'Unione Terre di Castelli eventuali misure organizzative idonee al miglioramento della sicurezza dei trattamenti dei dati personali;
- effettuare le comunicazioni ufficiali nel confronti del Garante compresa la notifica al Garante per la protezione dei dati personali ai sensi dell'art. 33 del GDPR, sentito il RPD dell'Ente.

3) **il Responsabile del Servizio** i cui dati sono stati oggetto di data breach e da eventuali altri soggetti coinvolti nel trattamento degli stessi dati che il gruppo riterrà necessario coinvolgere a seconda della tipologia di incidente e della tipologia di dati coinvolti, allo scopo di meglio individuare le cause del data breach, gli eventuali effetti sugli interessati e valutare l'applicabilità delle successive misure tecniche ed organizzative di miglioramento per la protezione dei dati personali.

I riferimenti fissi del gruppo, nelle figure del Responsabile del Servizio Sistemi Informativi e del rappresentante del Comune, (nominativi, indirizzo e-mail, numero di telefono, ecc.) devono essere ben identificati e facilmente raggiungibili, anche attraverso la pubblicazione nella intranet del Comune.

Nelle attività del gruppo deve essere coinvolto il Responsabile della Protezione dei Dati (RPD) designato, il quale esercita le proprie funzioni di monitoraggio della conformità in caso di data breach, fornendo il proprio parere (obbligatorio) in ordine alla necessità di effettuare la notifica e, quindi, sulle valutazioni precedentemente descritte.
Il Rappresentante dell'Ente può inoltre coinvolgere, a seconda della gravità dell'incidente, i vertici dell'Ente per gli aspetti di comunicazione interna ed esterna e nel caso in cui durante la gestione dell'incidente emergano responsabilità da parte di personale interno dell'Ente occorre coinvolgere il Servizio Risorse Umane dell'Unione Terre di Castelli che si occupa di gestione del personale.
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 dell'Ente, il Gruppo deve valutare l'opportunità o la necessità di coinvolgere le strutture di riferimento regionali e nazionali (ad esempio Lepida SpA considerando il proprio ruolo nell'ambito della sicurezza della Community Network, CERT-PA, etc.). Inoltre, il Gruppo può prevedere il coinvolgimento dei 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 RPD.

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 dall'Ente 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.
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 un 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 dell'Ente che verrà adottato con una chiara definizione dei Servizi 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 l'Ente intraprendere un'azione legale (civile o penale) contro una persona fisica o giuridica, oppure nel caso in cui ci siano le premesse affinché l'Ente 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 dell'Ente che accedono alle risorse del Sistema Informatico Informativo dell'Ente sono tenuti ad osservare i principi contenuti nel presente documento e 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 dell'Ente, 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 dell'Ente.

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.

Identificazione e analisi dell'incidente

Si tratta di attività che mirano 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

dell'Ente, di accesso non autorizzato a dati, di indisponibilità di una risorsa ICT per un tempo prolungato, etc.
Nel caso in cui venga rilevato un riscontro positivo durante l'analisi di tali eventi viene aperto un incidente di sicurezza che segue la procedura di gestione.
Nel caso di segnalazioni di incidente da parte di soggetti terzi, l'Ente 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 dell'Ente 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.: black out, 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 inerenti 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 gruppo per la Gestione della Sicurezza ICT deve anche stabilire la gravità dell'incidente di sicurezza, per fare ciò può inizialmente avvalersi della seguente 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 dall'Ente ● 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 dall'Ente con conseguente 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.

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 l'Ente 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 evidentemente 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 RPD 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 al Servizio Sistemi Informativi dell'Unione Terre di Castelli attraverso la mail

sicurezza@terredicastelli.mo.it o attraverso contatto telefonico del Servizio stesso disponibile sulla rete intranet dell'Ente, questo per permettere una immediata valutazione tecnica del fenomeno segnalato e di porre in atto le primissime misure da adottare per preservare la sicurezza dell'Ente (ad esempio un eventuale isolamento di apparati o tratti di rete); riconosciuto che si tratta di data breach il Rappresentante dell'Ente provvederà a convocare l'intero gruppo per la sicurezza ICT come sopra individuato.

La notifica della violazione al Garante

Nei casi in cui l'incidente consista in una violazione di dati personali, l'Ente 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 RPD.

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;
- 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;
- i recapiti del RPD;

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 ingente, 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 sarà a carico del gruppo di sicurezza ICT, il quale, a seconda della gravità attribuita in fase di identificazione dell'incidente, utilizzerà diverse modalità di attivazione e tracking.

[1] minori, persone con disabilità, dipendenti, clienti etc.

[2] Informazioni finanziarie, numeri di conti bancari, numeri di passaporto, documenti sanitari, etc.

Incidente di gravità “Alta”
Il gruppo di sicurezza ICT verrà attivato e verrà compilato l’apposito Rapporto incidente di sicurezza compilando soltanto le parti che in questa fase è possibile conoscere.
In caso di data breach verrà tempestivamente informato il RPD. Il Rapporto incidente di sicurezza sarà poi completato in tutte le sue parti in fase di chiusura dell’incidente.

L’Ente 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 dell’Ente 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 l’utente (superiore all'RTO dichiarato in sede di BIA), è necessario fare riferimento al piano di Business Continuity, una volta approvato.

Incidente di gravità “Media” o “Bassa”
In caso di incidente di gravità media o bassa, 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 dell’Ente in merito agli incidenti di sicurezza informatica.
I dati raccolti saranno conservati anche a fini statistici.

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 su 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 supervisione del Gruppo per la sicurezza ICT che 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.

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 dell'Ente;
- 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 ha 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 dell'Ente per comunicare eventuali disservizi.

In tali casi il Servizio Sistemi Informativi dell'Unione Terre di Castelli può operare le corrette scelte in autonomia, comunicando al Rappresentante dell'Ente 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.
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 gruppo per la sicurezza ICT che 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 ai servizi 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.
Saranno valutate eventuali modifiche 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 gruppo per la sicurezza ICT, secondo il modello allegato.
Il report, firmato digitalmente da tutti i componenti del Gruppo sicurezza ICT tramite procedura di hashing a garanzia della sua integrità, dovrà essere inviato in forma riservata ai vertici dell'Ente.
Il Rapporto dovrà essere conservato in un repository ad accesso limitato, 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 dell'Ente (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 del servizio preposto, 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 aziendale 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 sì che le considerazioni che ne scaturiscono debbano divenire patrimonio comune all'interno del team di gestione degli incidenti.
Per questo motivo occorre che in occasione della chiusura del rapporto di incidente il gruppo gestione della sicurezza ICT valuti collegialmente l'efficacia della procedura di gestione degli incidenti riportando nel medesimo rapporto 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).

8. Recapiti RPD

….. , li …….. **Il gruppo sicurezza ICT**

REGISTRO DELLE VIOLAZIONI

	OGGETTO DELLA VIOLAZIONE	DATA E ORA VIOLAZIONE	SORGENTE DELL'INFORMAZIONE SULLA VIOLAZIONE	CAUSE	CONSEGUENZE	DATA E ORA NOTIFICA AD AUTORITA' DI CONTROLLO	MOTIVO DEL RITARDO O DELLA MANCATA COMUNICAZIONE ALL'AUTORITA' DI CONTROLLO	MISURE ADOTTATE A SEGUITO DELLA VIOLAZIONE
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								

COMUNE DI MARANO SUL PANARO
Provincia di Modena
******

Proposta N. 2018 / 500
UNITA' PROPONENTE Amministrativo

OGGETTO: ADEGUAMENTO AL REGOLAMENTO EUROPEO UE/2016/679 O GDPR (GENERAL DATA PROTECTION REGULATION) - APPROVAZIONE E ADOZIONE DEL MODELLO DI GESTIONE INCIDENTI DI SICUREZZA E DEL DISCIPLINARE PER L'USO DEI SISTEMI INFORMATIVI NELL'UNIONE TERRE DI CASTELLI E NEI COMUNI ADERENTI

PARERE IN ORDINE ALLA REGOLARITA' TECNICA

Per i fini previsti dall'art. 49 del D. Lgs 18.08.2000 n° 267, si esprime sulla proposta di deliberazione in oggetto parere *FAVOREVOLE* in merito alla regolarità tecnica.

Marano sul Panaro, 01/12/2018

IL RESPONSABILE DI SETTORE
MANZINI ELISABETTA
(Sottoscritto digitalmente ai sensi
dell'art. 21 D.L.gs n 82/2005 e s.m.i.)

COMUNE DI MARANO SUL PANARO
Provincia di Modena
******

Proposta N. 2018 / 500
UNITA' PROPONENTE Amministrativo

OGGETTO: ADEGUAMENTO AL REGOLAMENTO EUROPEO UE/2016/679 O GDPR (GENERAL DATA PROTECTION REGULATION) - APPROVAZIONE E ADOZIONE DEL MODELLO DI GESTIONE INCIDENTI DI SICUREZZA E DEL DISCIPLINARE PER L'USO DEI SISTEMI INFORMATIVI NELL'UNIONE TERRE DI CASTELLI E NEI COMUNI ADERENTI

PARERE IN ORDINE ALLA REGOLARITA' CONTABILE

Il sottoscritto, in qualità di Responsabile del Settore Economico Finanziario, ai sensi dell'art. 49, comma 1 e dell'art. 147-bis, comma 1, D.Lgs 267/2000, esprime sulla proposta di deliberazione in oggetto parere NON APPOSTO in merito alla regolarità contabile.

Marano sul Panaro, 03/12/2018

IL RESPONSABILE DI SETTORE
ZANNI PATRIZIA
(Sottoscritto digitalmente ai sensi
dell'art. 21 D.L.gs n 82/2005 e s.m.i.)

COMUNE DI MARANO SUL PANARO
Provincia di Modena
******

Certificato di Pubblicazione

Deliberazione di Giunta Comunale N. 97 del 03/12/2018

Amministrativo

Oggetto: ADEGUAMENTO AL REGOLAMENTO EUROPEO UE/2016/679 O GDPR (GENERAL DATA PROTECTION REGULATION) - APPROVAZIONE E ADOZIONE DEL MODELLO DI GESTIONE INCIDENTI DI SICUREZZA E DEL DISCIPLINARE PER L'USO DEI SISTEMI INFORMATIVI NELL'UNIONE TERRE DI CASTELLI E NEI COMUNI ADERENTI.

Ai sensi per gli effetti di cui all'art. 124 del D.Lgs 18.8.2000, n. 267 copia della presente deliberazione viene pubblicata, mediante affissione all'Albo Pretorio, per 15 giorni consecutivi dal 10/12/2018.

Marano sul Panaro, 10/12/2018

L'INCARICATO DELLA PUBBLICAZIONE
MARTINI MARGHERITA
(Sottoscritto digitalmente
ai sensi dell'art. 21 D.L.gs. n. 82/2005 e s.m.i.)

COMUNE DI MARANO SUL PANARO
Provincia di Modena
******

Certificato di Esecutività

Deliberazione di Giunta Comunale N. 97 del 03/12/2018

Amministrativo

Oggetto: ADEGUAMENTO AL REGOLAMENTO EUROPEO UE/2016/679 O GDPR (GENERAL DATA PROTECTION REGULATION) - APPROVAZIONE E ADOZIONE DEL MODELLO DI GESTIONE INCIDENTI DI SICUREZZA E DEL DISCIPLINARE PER L'USO DEI SISTEMI INFORMATIVI NELL'UNIONE TERRE DI CASTELLI E NEI COMUNI ADERENTI.

Si dichiara che la presente deliberazione è divenuta esecutiva decorsi 10 giorni dall'inizio della pubblicazione all'Albo Pretorio on-line di questo Comune.

Marano sul Panaro, 24/12/2018

L'INCARICATO DELLA PUBBLICAZIONE
MARTINI MARGHERITA
(Sottoscritto digitalmente
ai sensi dell'art. 21 D.L.gs. n. 82/2005 e s.m.i.)

COMUNE DI MARANO SUL PANARO
Provincia di Modena
******

Certificato di Avvenuta Pubblicazione

Deliberazione di Giunta Comunale N. 97 del 03/12/2018

Oggetto: ADEGUAMENTO AL REGOLAMENTO EUROPEO UE/2016/679 O GDPR (GENERAL DATA PROTECTION REGULATION) - APPROVAZIONE E ADOZIONE DEL MODELLO DI GESTIONE INCIDENTI DI SICUREZZA E DEL DISCIPLINARE PER L'USO DEI SISTEMI INFORMATIVI NELL'UNIONE TERRE DI CASTELLI E NEI COMUNI ADERENTI.

Si dichiara l'avvenuta regolare pubblicazione della presente deliberazione all'Albo Pretorio on-line di questo Comune a partire dal 10/12/2018 per 15 giorni consecutivi, ai sensi dell'art 124 del D.lgs 18.08.2000, n. 267 e la contestuale comunicazione ai capigruppo consiliari ai sensi dell'art. 125 del D.lgs 18.08.2000, n. 267.

Marano sul Panaro, 07/01/2019

L'INCARICATO DELLA PUBBLICAZIONE
MARTINI MARGHERITA
(Sottoscritto digitalmente
ai sensi dell'art. 21 D.L.gs. n. 82/2005 e s.m.i.)