COMUNE DI GALLIO
Provincia di Vicenza

Via Roma n. 2
C.A.P. 36032

P.I. 00174060244
C.F. 84001130248

Ai Responsabili di Settore
All'Amministratore di Sistema

p.c. Al Sindaco

DIRETTIVA DEL SEGRETARIO COMUNALE

OGGETTO: VERIFICA PERIODICA DEI SISTEMI INFORMATIVI E DELLE PROCEDURE FINALIZZATA ALLA RISERVATEZZA, ALLA DISPONIBILITA', ALL'INTEGRITA' DELLE INFORMAZIONI E DEI DATI E ALLA TRACCIABILITA' DELLE OPERAZIONI.

Il riscontro dello stato di sicurezza, l'identificazione di vulnerabilità e il perfezionamento delle strutture dedicate alla protezione contro minacce ai sistemi informatici dell'Ente sono richiesti, oltre ché dalla normativa sulla *privacy,* dai più comuni *framework* di *cybersecurity* intendendo, con la stessa, la sicurezza delle informazioni e la protezione dei sistemi informativi.

Le informazioni ed i dati detenuti dall'Ente, ormai a carattere esclusivamente digitale, sono parte integrante di qualsiasi nostra attività e la sicurezza è divenuta una componente essenziale da cui l'informazione stessa non può prescindere.

Non è più sufficiente quindi limitarsi ad assicurare la riservatezza ma è necessario garantirne anche la disponibilità e l'integrità.

Il trinomio ***riservatezza (o confidenzialità)***, ***disponibilità*** *e* ***integrità*** (meglio conosciute con l'acronimo ***CIA*** - ***C****onfidentiality,* ***I****ntegrity,* ***A****vailability)* costituisce infatti il target indispensabile di qualsiasi sistema di sicurezza delle informazioni.

La **riservatezza** consiste nel limitare l'accesso alle informazioni e alle risorse informatiche alle sole persone autorizzate a farlo.

La **disponibilità** significa che le informazioni devono essere accessibili agli aventi diritto nel momento in cui essi lo richiedano e quindi i sistemi informatici debbono fornire le prestazioni richieste anche in caso di malfunzionamento.

L'**integrità** riguarda il grado di esattezza, coesione e attendibilità delle informazioni, cioè significa che queste non possano venire alterate, cancellate o modificate.

Dal momento che l'informazione è l'essenza di ogni organizzazione, questa deve adottare tutti i provvedimenti necessari affinché ciò abbia luogo persistendo nel tempo.

Già con l'adozione del Regolamento sull'utilizzo dei sistemi informatici e il periodico aggiornamento del Piano della sicurezza informatica, il Comune di Gallio, oltre ad aver fornito a dipendenti e collaboratori le indicazioni per una corretta e adeguata gestione delle informazioni, ha formalizzato

www.comune.gallio.vi.it
e-mail comune@comune.gallio.vi.it
P.E.C. gallio.vi@cert.ip-veneto.net

tel. +39 0424 447911
fax +39 0424 447922

le misure di sicurezza adottate, descrivendo la strategia adottata per poter soddisfare i requisiti di sicurezza del trinomio CIA, garantendo altresì la **tracciabilità** delle azioni compiute nell'ambito del sistema.

Nell'ottica sopraindicata, la necessità di una coerenza complessiva di sicurezza informatica dev'essere implementata con la previsione di controlli periodici, per saggiare la tenuta della sicurezza delle informazioni.

Ciò premesso, il Segretario comunale

DISPONE

quanto segue:

1. è approvato come da allegato al presente provvedimento il **registro dei controlli periodici** finalizzati alla sicurezza dei sistemi informativi dell'Ente, alla riservatezza, alla disponibilità, all'integrità delle informazioni e dei dati e alla tracciabilità delle operazioni sui dati stessi;
2. l'effettuazione dei controlli è affidata ai soggetti indicati in colonna F del registro stesso;
3. l'effettuazione dei controlli periodici dovrà essere **documentata**, in ottemperanza al principio di *accountability (o responsabilizzazione)* cui è sottoposto il Titolare del trattamento, il quale *deve mettere in atto misure tecniche e organizzative adeguate per garantire, ed* ***essere in grado di dimostrare****, che il trattamento di dati è effettuato conformemente alla normativa sulla protezione di dati personali*.

Gallio, *data della firma digitale*

IL VICESEGRETARIO COMUNALE
dott. Francesco Bertacco

CONTROLLI PERIODICI

col. A oggetto del controllo	col. B tipo di controllo	col. C finalità del controllo	col. D sistemi interessati	col. E tempistica	col. F settori / soggetti interessati
condizioni ambientali locale server (climatizzazione)	• controllare le condizioni ambientali dei locali server	efficienza dei server	locali server	una volta la settimana nei mesi di giugno, luglio e agosto	responsabile settore ove incardinato il servizio ced
condizioni ambientali locale server (presenza estintore)	• verificare la presenza di estintori regolarmente revisionati	prevenzione incendi	locali server	una volta l'anno	responsabile settore ove incardinato il servizio ced
estintori	• verificare la presenza di estintori regolarmente revisionati ai piani	prevenzione incendi	estintori	una volta l'anno	responsabile settore ove incardinato il servizio manutenzioni
gruppi di continuità server	• controllare che i gruppi di continuità cui sono collegati i server siano funzionanti e garantiscano adeguata protezione	garantire l'alimentazione elettrica in caso di blackout	gruppi di continuità	tre volte l'anno, distribuite uniformemente	responsabile settore ove incardinato il servizio manutenzioni
firewall (porte)	• controllare le porte aperte	impedire l'accesso dall'esterno	firewall	una volta l'anno	amministratore di sistema
firewall (contratto)	• controllare la scadenza del contratto per la fornitura del firewall	garantire il monitoraggio e la sicurezza del traffico di rete		una volta l'anno	responsabile settore ove incardinato il servizio ced
backup area documentale	• controllare il corretto funzionamento del sistema di backup locale	garantire la disponibilità di copie di sicurezza	server locale e nas	una volta al mese	amministratore di sistema
utenze con credenziali amministrative	• controllare se le utenze con credenziali amministrative attive siano assegnate a utenti che effettivamente ne devono avere la titolarità	impedire l'accesso ai dati a soggetti non aventi titolo	server	due volte l'anno	amministratore di sistema
diritti e profili utenze gestionali	• controllare la validità dei profili associati ai vari utenti • disattivare i profili dei soggetti che non hanno diritto ad accedere alle procedure	impedire l'accesso , la modifica o l'alterazione dei dati a soggetti non aventi titolo	• gestionali Halley Informatica • gestionale Tributi • gestionale GPE • intranet sito web • DPM Data Protection Manager • X-Desk	due volte l'anno e, in ogni caso, tempestivamente al variare di mansioni, nuove assunzioni, cessazioni	amministratore di sistema
diritti e profili area documentale	• controllare la validità dei profili associati ai vari utenti • disattivare i profili dei soggetti che non hanno diritto ad accedere alle varie aree documentali	impedire l'accesso ai dati, la modifica o l'alterazione dei dati, a soggetti non aventi titolo	area documentale server	due volte l'anno	amministratore di sistema
documenti area documentale	• controllare la presenza nelle cartelle condivise per il deposito delle scansioni la presenza di files vecchi di oltre 7 giorni	impedire l'accesso ai dati a soggetti non aventi titolo	server	una volta al mese	responsabile settore ove incardinato il servizio ced
dominio internet	• controllare la scadenza del contratto per la registrazione del dominio e fornitura delle caselle di posta elettronica	garantire la disponibilità delle informazioni sul sito e negli account di posta elettronica	nessun sistema	una volta l'anno	responsabile settore ove incardinato il servizio ced
posta elettronica	• controllare l'assegnazione delle caselle di posta elettronica ai vari utenti, compresi eventuali redirect • disattivare le caselle assegnate a soggetti che non hanno più diritto ad utilizzare una casella istituzionale	impedire l'accesso ai dati a soggetti non aventi titolo	portale di gestione delle caselle di posta	tre volte l'anno distribuite uniformemente e, in ogni caso, tempestivamente al variare di mansioni o cessazioni	responsabile settore ove incardinato il servizio ced
posta elettronica	• controllare le impostazioni della casella pec istituzionale per accertare l'assenza di regole o altre impostazioni che possono presumere	impedire l'accesso ai dati a soggetti non aventi titolo	portale di gestione delle caselle di posta	tre volte l'anno distribuite uniformemente	responsabile settore ove incardinato il servizio protocollo

	la compromissione delle credenziali di accesso				
conservazione sostitutiva	• controllare la scadenza del contratto per la fornitura del servizio di conservazione sostitutiva	garantire la disponibilità dei documenti inviati in conservazione oltre a permettere l'invio di ulteriore documentazione	nessun sistema	una volta l'anno	responsabile settore ove incardinato il servizio ced
conservazione sostitutiva	• controllare (a campione) il regolare invio dei documenti in conservazione	garantire l'integrità e la disponibilità dei documenti inviati in conservazione	X-Desk	una volta al mese	responsabile della conservazione
vpn	• verifica vpn attive	impedire l'accesso ai dati a soggetti non aventi titolo	firewall	tre volte l'anno distribuite uniformemente	responsabile settore ove incardinato il servizio ced
registro delle attività di trattamento	• controllo periodico finalizzato all'aggiornamento del registro	ricognizione e valutazione dei trattamenti svolti finalizzata anche all'analisi del rischio (obbligo di legge)	DPM Data Protection Manager	due volte l'anno (tempestivo in caso di change)	responsabili di tutte le aree
piano di sicurezza	• controllare se il piano necessita di un aggiornamento	formalizzare in un documento ufficiale la strategia che il Comune adotta per poter soddisfare i requisiti di sicurezza	nessun sistema	una volta l'anno	responsabile settore ove incardinato il servizio ced
videosorveglianza	• controllare la scadenza del contratto di manutenzione dell'impianto	garantire il corretto funzionamento dell'impianto nonché assicurare la manutenzione programmata dello stesso	impianto di videosorveglianza	una volta l'anno	responsabile settore ove incardinato il servizio di polizia locale
procedura whistleblowing	• controllare la corretta assegnazione delle credenziali di accesso alla procedura di segnalazione al Responsabile Anticorruzione • controllare che l'indirizzo e-mail utilizzato sia consultabile dal Responsabile Anticorruzione in carica	assicurare che l'accesso alle comunicazioni che transitano attraverso la procedura per la segnalazione di illeciti sia riservata al Responsabile Anticorruzione	• portale per la gestione della procedura whistleblowing • portale di gestione delle caselle di posta	tempestivamente ad ogni sostituzione del Responsabile Anticorruzione	responsabile settore ove incardinato il servizio ced