COMUNE DI
SCICLI

Comune di SCICLI

Via Francesco Mormina Penna, 2
97018 Scicli (RG)
Tel. 0932 839111
PEC protocollo@pec.comune.scicli.rg.it
P.Iva 00080070881

PIANO PER LA SICUREZZA INFORMATICA

Nome Struttura:

Comune di SCICLI

All'interno del documento sono indicate tutte le procedure e le metodologie adottate per la gestione, automatizzata e manuale, del sistema informatico della struttura.

Tali procedure nascono dalle indicazioni tecniche fornite nell'ambito delle linee guida per la certificazione ISO/IEC 27001:2013 e le linee guida definite all'interno del Codice dell'Amministrazione Digitale (D.Lgs. 82 del 2005).

Tale piano si pone l'obiettivo di garantire, monitorare e controllare la sicurezza dei sistemi informativi della struttura e, minimizzando il rischio residuo, assicurando la continuità del business e il soddisfacimento dei requisiti relativi alla privacy e alla protezione dei dati trattati dall'organizzazione.

Come è noto, il "**Piano per la sicurezza informatica**" è parte integrante del Manuale di Gestione documentale, per la quota parte di competenza, nel rispetto delle:

- misure di sicurezza predisposte dall'AgID e dagli altri organismi preposti;
- delle disposizioni in materia di protezione dei dati personali in linea con l'analisi del rischio;
- indicazioni in materia di continuità operativa dei sistemi informatici predisposti dall'AGID.

COMUNE DI
SCICLI

Comune di SCICLI

Via Francesco Mormina Penna, 2 - 97018 Scicli (RG)
Tel. 0932 839111
PEC protocollo@pec.comune.scicli.rg.it
P.Iva 00080070881

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	23/12/2024	Maria Sgarlata	Rtd
Verifica	23/12/2024	Francesco Petino	Responsabile Protezione dei Dati
Approvazione		Nadia Gruttadauria	Segretario Generale - Esercente Funzione di Titolarità

REGISTRO DELLE VERSIONI E RELATIVE DISTRIBUZIONI

N°Ver/Rev/Bozza	Data emissione	Osservazioni
1	23/12/2024	
2		
3		

Via Francesco Mormina Penna, 2 - 97018 Scicli (RG)
Tel. 0932 839111
PEC protocollo@pec.comune.scicli.rg.it
P.Iva 00080070881

PREMESSA - RIFERIMENTI ED ALLEGATI

Il presente Piano della Sicurezza (PdS) descrive l'implementazione del Sistema di Gestione della Sicurezza Informatica (SGSI) dell'organizzazione:

Comune di Scicli

Ogni indicazione contenuta nel PdS è da intendersi riferita, ove altrimenti non indicata, esclusivamente alla gestione del sistema informativo utilizzato.

Il PdS fa riferimento ad una serie di documenti e procedure che sono utilizzate all'interno della organizzazione stessa. Nel seguito, si fa riferimento agli aspetti della norma ISO/IEC 27001:2013, alle norme ISO/IEC 27002 e lo ETSI TS 101 533-01. Si considerano inoltre, a puro titolo di esempio, aspetti contemplati nella norma ISO 9001:2008, oltre che ad altre eventuali norme e/o dispositivi legislativi.

TERMINOLOGIA (GLOSSARIO, ACRONIMI)

Glossario dei termini - definizioni	
Sistema	Applicazione/Servizio che deve essere disponibile agli aventi diritto in termini di esercizio e disponibilità dell'informazione.
Disponibilità richiesta	Tempo in cui il sistema deve essere utilizzabile in conformità alle funzionalità previste, esclusi i tempi programmati per la manutenzione, rispetto alle ore concordate per l'esercizio.
Periodo criticità servizio	Data/periodo in cui il dato o il servizio deve essere tassativamente erogato per esigenze specifiche del business, quali scadenze o presentazione dei dati.
RBAC	Role Based Access Control - Sistema di controllo accessi basato sui ruoli in cui le entità del sistema che sono identificate e controllate rappresentano posizioni funzionali in una organizzazione o processi.
Tempo ripristino richiesto (Recovery Time Objective)	Tempo entro il quale un processo informatico ovvero il Sistema Informativo primario deve essere ripristinato dopo un disastro o una condizione di emergenza (o interruzione), al fine di evitare conseguenze inaccettabili.
Obiettivo temporale di recupero (Recovery Point Objective)	Indica la perdita dati tollerata: rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di un evento imprevisto.

Via Francesco Mormina Penna, 2 - 97018 Scicli (RG)
Tel. 0932 839111
PEC protocollo@pec.comune.scicli.rg.it
P.Iva 00080070881

Acronimi (suggerimento)	
CA	Certification Authority
CAD	Codice dell'Amministrazione Digitale; il testo vigente è costituito dal DLgs 82/2005, e successive modifiche.
DLgs	Decreto Legislativo
DM	Decreto Ministeriale
DPCM	Decreto del Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica

NORMATIVA E STANDARD DI RIFERIMENTO

Normativa di riferimento :

Il Regolamento eIDAS (electronic IDentification Authentication and Signature) - Regolamento UE n° 910/2014 sull'identità digitale - ha l'obiettivo di fornire una base normativa a livello comunitario per i servizi fiduciari e i mezzi di identificazione elettronica degli stati membri.

La normativa di riferimento per la gestione dei documenti informatici all'interno della pubblica amministrazione è rappresentata da: Codice dei Beni Culturali e del paesaggio: decreto legislativo 22 gennaio 2004, n. 42

Le misure minime di sicurezza ICT emanate da AgID, sono un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle amministrazioni, al fine di contrastare le minacce informatiche più frequenti: https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

Standard di riferimento

Nella definizione del contesto normativo il legislatore ha provveduto ad identificare un set di standard tecnologici di valenza internazionale a cui riferirsi, sia al fine di recepire le ricerche e gli studi effettuati a livello internazionale sull'argomento:

ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;

- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V 1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

Via Francesco Mormina Penna, 2 - 97018 Scicli (RG)
Tel. 0932 839111
PEC protocollo@pec.comune.scicli.rg.it
P.Iva 00080070881

- ETSI TR 101 533-2 V 1.3.1 (2012-04) Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The *Dublin Core* metadata element set, Sistema di metadata del *Dublin Core*.

ORGANIZZAZIONE DEL SISTEMA DI CONSERVAZIONE

Ruoli e responsabilità del sistema di conservazione

Lo svolgimento delle attività di conservatore richiede la presenza di più attori coinvolti nel progetto, ognuno dei quali ha la responsabilità di specifiche attività da svolgere.

Questi ruoli si inseriscono nell'organigramma generale dell'organizzazione arricchendo i ruoli e le procedure già previste per la gestione dei processi interni.

Per ogni figura prevista nel processo di gestione del sistema di conservazione sono richiesti specifici requisiti di onorabilità e di esperienza minima nel ruolo. Peraltro, così com'è previsto che alcune attività possano essere svolte dal medesimo soggetto è, altresì, previsto che alcune funzioni possano essere delegate ad altri soggetti, fermo restando i predetti vincoli di onorabilità e di requisiti di esperienza del delegato.

Nome del Responsabile della conservazione:

Sgarlata Maria

Azienda o organismo incaricato del servizio di conservazione:

Maggioli SpA

Le attività relative al servizio di conservazione coinvolgono vari settori dell'organizzazione, che interagiscono tra loro al fine di garantire la gestione di tutte le esigenze del produttore dei documenti.

Specificamente le attività impattano sulle seguenti struttura organizzative:

- *Organismo apicale o funzione omologa* richiede la formalizzazione delle procedure interne per la gestione dei rischi dell'organizzazione.
- *Responsabile dei Sistemi Informativi e/o RTD (ove designato)*
- *Responsabile del Servizio di Conservazione* per la definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione.
- *Responsabile della Funzione Archivistica di Conservazione*, per la definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato.

Per ulteriori informazioni si fa riferimento ad eventuali allegati a questo documento.

Comune di SCICLI

Via Francesco Mormina Penna, 2 - 97018 Scicli (RG)
Tel. 0932 839111
PEC protocollo@pec.comune.scicli.rg.it
P.Iva 00080070881

Incaricato alla sicurezza informatica del sistema

Il *Responsabile della Sicurezza* è identificato dall'organizzazione:

Nome	Cognome	Ruolo all'interno dell' organizzazione	Interno/Esterno	Contatto
Giombattista	Miceli	Responsabile del Servizio Sistemi Informativi e Transizione Digitale – Amministratore di Sistema	interno	0932839230
Mario	Ferro	Coadiutore dell'Amministratore di Sistema	interno	0932839235

Procedure di produzione, gestione della documentazione

La produzione e la gestione della documentazione avviene attraverso le seguenti procedure software garantite da accordo di Data processor con accordo secondo quanto previsto dall'Art. 28 dell (ue) 679/2016.

N.O.	Nome Procedura	Software House	Contatto	Pec
01	Maggioli Sicraweb (Protocollo, Pratiche SUE, Pratiche SUAP, Contabilità e Ragioneria, Economato, Gestione Patrimonio, Gestione Economica, Notifiche Multe e Verbali, Gestione Personale, Procedimenti Disciplinari, Organi Istituzionali, Contratti, Imposta di Soggiorno)	Maggioli SpA	Tel. 0541 628380 Portale assistenza (https://assistenza.maggioli.it/)	segreteria@maggioli.legalmail.it
02	Tributi Minori e Maggiori	Sikuel Srl	Tel. 0932 667555	sikuel@ecert.it
03	Demografici (Anagrafe, Stato Civile, Elettorale, Leva)	Golem Net srl	Tel. 06 95995160 Email assistenza@golemnet.it	golemnet@pec.golemnet.it
04	Software di produttività individuale (LibreOffice, Office, ecc.)	Software house diverse	Assistenza interna (Servizio Sistemi Informativi e Transizione Digitale): Tel. 0932 839235 Email ced@comune.scicli.rg.it Assistenza esterna (Ricca IT srl): Tel. 0932 668082 Email assistenza@ricca-it.com	//
05	Pagamenti PagoPA	Eremind srl	Tel. 0342 1831135 Email info@pmpayment.com	eremindsrl@legalmail.it
06	CMS "FlexCMP" (gestione del sito istituzionale)	Deda Digital srl	Tel. 051 780630	dedadigital@legalmail.it

			Portale assistenza (https://support.deda.digital/login)	
07	Sistema F Platinum Top (gestionale Farmacia Comunale)	CSF Sistemi srl	Assistenza di zona Eurosistemi snc: Tel 0932 654242 Email assistenza.software@eurosistemi.rg.it	eurosistemi@pec.it

Gestione dati e documenti

Procedura di **cancellazione** delle informazioni all'interno del sistema informativo.

Per tutti gli asset (PC, NAS, Dispositivi di memorizzazione) è prevista un'attività di cancellazione dei dati permanente. A seguito dell'operazione, dovrà essere compilato un modulo di descrizione della procedura effettuata da inviare al responsabile alla sicurezza informatica.

La relazione dovrà contenere almeno:

- data
- nome del dispositivo
- procedura utilizzata
- verifica effettuata
- nome dell'operatore che ha eseguito l'attività

La procedura di **distruzione e triturazione** dei supporti non riscrivibili utilizzati per la memorizzazione delle informazioni sarà eseguita utilizzando le apparecchiature a corredo dell'organizzazione preposte a tale scopo.

Piano di formazione del personale

All'interno del programma formativo annuale dei dipendenti dovrà essere prevista almeno una giornata di formazione dedicata ad istruzioni ed obblighi al fine della tutela dei dati e documenti utilizzati dall'organizzazione.

Via Francesco Mormina Penna, 2 - 97018 Scicli (RG)
Tel. 0932 839111
PEC protocollo@pec.comune.scicli.rg.it
P.Iva 00080070881

Continuità operativa

Misure adottate a garantire la continuità operativa quali ad esempio il disaster recovery e il backup delle informazioni.

N.O.	Elenco Procedure	Backup (Si/No)	Cloud (Si/No)	Ridondanza
01	Maggioli Sicraweb (Protocollo, Pratiche SUE, Pratiche SUAP, Contabilità e Ragioneria, Economato, Gestione Patrimonio, Gestione Economica, Notifiche Multe e Verbali, Gestione Personale, Procedimenti Disciplinari, Organi Istituzionali, Contratti, Imposta di Soggiorno)	si	si	si
02	Tributi Minori e Maggiori	si	no	no
03	Demografici (Anagrafe, Stato Civile, Elettorale, Leva)	si	no	no
04	Software di produttività individuale (LibreOffice, Office)	si	no	no
05	Pagamenti PagoPA	si	si	si
06	Sito web CMS “FlexCMP”	si	si	si
07	Sistema F Platinum Top (gestionale Farmacia Comunale)	si	si	si

Annotazioni:
Per quanto riguarda le **connettività** sia **internet** che **intranet** delle 12 sedi comunali sono gestite dalla ditta Blunova Srl con i seguenti contatti : Telefono: 0932/1838938 e 0932/667666 dal lunedì al venerdì, dalle ore 9:00 alle ore 13:00 e dalle ore 14:30 alle ore 18:30; 0932/1838915 per ricevere assistenza nelle altre fasce orarie Email: assistenza@novaquadri.it - info@novaquadri.it

Piano Audit del sistema informativo

L’audit è previsto con cadenza annuale e può essere anticipato qualora il sistema precede un profondo cambiamento logico o tecnico. L’audit viene organizzato e pianificato dal responsabile della sicurezza e/o dal Responsabile protezione dei dati se nominato.

COMUNE DI
SCICLI

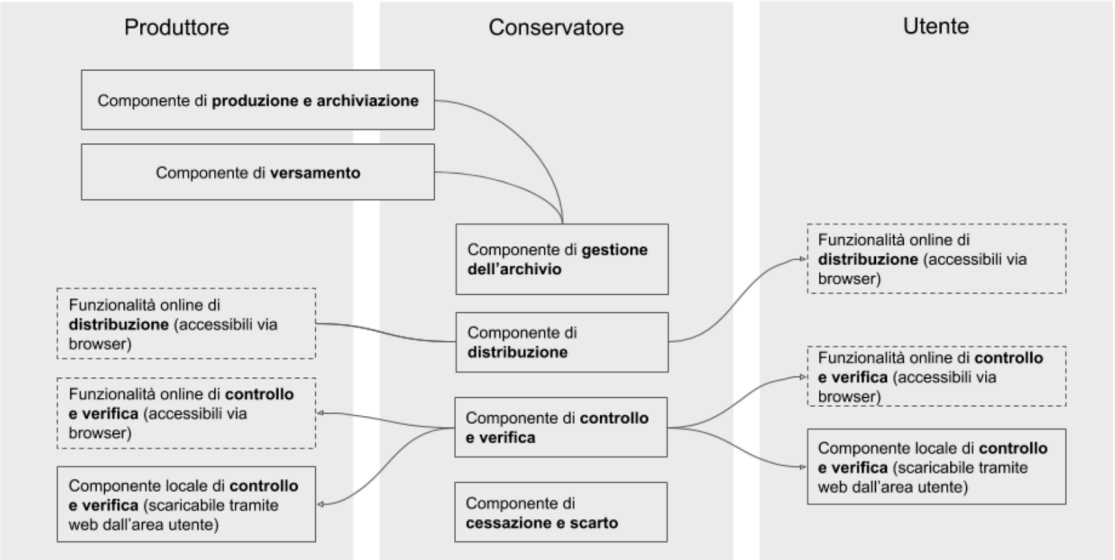
Comune di SCICLI

Via Francesco Mormina Penna, 2 - 97018 Scicli (RG)
Tel. 0932 839111
PEC protocollo@pec.comune.scicli.rg.it
P.Iva 00080070881

PERIMETRO DEL SISTEMA DI CONSERVAZIONE

Descrizione del Sistema di Conservazione. Analisi e implementazione di continuità operativa e disaster recovery dati e documenti.

Schema topologico



Componenti fisiche (censimento) del sistema informativo

SW=switch o hub, PC=Postazioni di lavoro fisse e mobili, SV=SERVER, AP=Access point, TL=Telecamere IP, FW=Firewall, NS= Nas, PN=Stampanti di rete, RP=Rilevatori delle presenze

Dopo un rilevamento pressoché preciso nelle sedi comunali (considerando non in elenco componenti in disuso o non funzionanti) si contano:

Componenti	**SW**	**PC**	**SV**	**AP**	**TL**	**FW**	**NS**	**PN**	**RP**
Numero totale	**26**	**154**	**8**	**4**	**//**	**2**	**3**	**75**	**11**

Piani di manutenzione delle infrastrutture

La manutenzione non è programmata per tutti gli apparati fisici facenti parte del Sistema.

Componenti	SW	PC	SV	AP	TL	FW	PN	RP
Manutenzione Programmata (Si/No)	No	Si	Si	No	//	No	No	No

Presenza e manutenzione delle Infrastrutture di supporto al fine di assicurare la continua disponibilità e integrità.

Riepilogo (previsto/non previsto) si/no

Antifurto	Antintrusione	Antiallagamento	Continuità Elettrica	Antincendio
no	si	no	si	si

Descrizione dettagliata e/o motivazione delle infrastrutture di supporto di cui sopra

Antintrusione
La stanza della sede Municipio dove sono presenti i server e i firewall è chiusa con una porta dotata di serratura.

Antifurto
//

Antiallagamento
//

Continuità Elettrica
Tutti i server e i firewall e la maggior parte delle postazioni di lavoro sono protetti da gruppo di continuità

Antincendio
In diversi punti delle sedi degli uffici comunali sono presenti gli estintori

Strutture organizzative preposte alla gestione dello stato di emergenza

CDC - Comitato di Crisi

Relativamente alle situazioni che possono portare alla condizione di stato di emergenza sul sistema informatico, il **Comitato di Crisi** oltre ad avere un ruolo fondamentale nella gestione dell'emergenza ICT, è impegnato in tutte le attività necessarie che devono essere svolte.

- Raccoglie tutte le informazioni necessarie alle decisioni;
- Coordinare i team operativi per la gestione dell'emergenza e per il processo di ritorno alla normalità;
- in caso di conclusione dell'emergenza cura tutte le operazioni di ritorno alla normalità.

Descrizione delle modalità operative del **Comitato di Crisi**

1. fase di reazione all'emergenza;
2. fase di gestione dell'emergenza;
3. fase di riattivazione dei servizi;
4. fase di ritorno alla normalità.

Il Comitato di Crisi è l'organismo di vertice a cui spettano le principali decisioni e la supervisione delle attività delle risorse coinvolte; è l'organo di direzione strategica dell'intera struttura in occasione dell'apertura dello stato di emergenza informatica, organo di responsabilità di garanzia e controllo sulla continuità operativa di un'organizzazione.

Le figure minime necessarie per la costituzione del Comitato di Crisi sono rappresentate da:

- **ORGANO APICALE DI VERTICE**

  Sgarlata Maria
  (ruolo di vertice con poteri decisionali e di indirizzo in materia organizzativa ed economica, ovvero il responsabile dell'Ufficio Unico Dirigenziale ex art. 17 del CAD)

- **RESPONSABILE INFORMATICO E/O/ RESPONSABILE DISASTER RECOVERY E CONTINUITA' OPERATIVA**

  Miceli Giombattista
  (colui conosce in modo approfondito il sistema informatico dell'organizzazione)

- **RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)**

  Francesco Petino (società Marco La Diega srl)
  (Il Data Protection Officer 2016/679 GDPR, sia esso soggetto interno o esterno con competenze giuridiche, informatiche, di risk management e di analisi dei processi)

- **RESPONSABILE DELLA SICUREZZA AI SENSI d.lgs 81/2008**

  Nicola Quinci (società Ergon Ambiente e Lavoro srl)
  (D.Lgs. 81/08: il datore di lavoro nomini il Responsabile del Servizio di Prevenzione e Protezione - RSPP in quanto figura che, in possesso di capacità e requisiti professionali, coordina il servizio di prevenzione e protezione dai rischi)

In condizioni ordinarie il Comitato si riunisce con periodicità almeno annuale, allo scopo di valutare lo stato della soluzione di continuità ICT, verificare le criticità, attuare e pianificare le iniziative per il miglioramento continuo dei processi che garantiscono la continuità operativa.

I principali compiti del Comitato di Crisi in condizioni ordinarie sono: definizione ed approvazione del piano di sicurezza informatico e approvazione degli aggiornamenti. Coordinamento delle attività di formazione e sensibilizzazione sul tema della sicurezza informatica.

Via Francesco Mormina Penna, 2 - 97018 Scicli (RG)
Tel. 0932 839111
PEC protocollo@pec.comune.scicli.rg.it
P.Iva 00080070881

Continuità operativa e disaster recovery

La continuità operativa nel contesto ICT è la capacità di una organizzazione di adottare - per ciascun processo critico e per ciascun servizio critico erogato in modalità ICT, attraverso accorgimenti, procedure e soluzioni tecnico-organizzative - misure di reazione e contenimento ad eventi imprevisti che possono compromettere, anche parzialmente, all'interno o all'esterno dell'organizzazione, il normale funzionamento dei servizi e delle funzioni dell'organizzazione.

Per quel che riguarda il sistema informativo, è necessario dettagliare i livelli di servizio erogati, i periodi di criticità e presidio, con i relativi tempi di ripristino e gli obiettivi temporali di backup come riportato in tabella.

Sistema	**Previsto Si/No**	**Tempo ripristino richiesto (RTO)**	**Obiettivo temporale di recupero (RPO)**
SISTEMA INFORMATIVO INTERNO	si	24/48	24/48
PORTALE WEB	si	24/48	24/48
SISTEMA DI VIDEOSORVEGLIANZA (N.B. NON E' PRESENTE UN SISTEMA DI VIDEOSORVEGLIANZA INTERNO ALLE SEDI DI UFFICI COMUNALI)	//	//	//
Maggioli Sicraweb (Protocollo, Pratiche SUE, Pratiche SUAP, Contabilità e Ragioneria, Economato, Gestione Patrimonio, Gestione Economica, Notifiche Multe e Verbali, Gestione Personale, Procedimenti Disciplinari, Organi Istituzionali, Contratti, Imposta di Soggiorno)	si	24/48	24/48
Sistema F Platinum Top (gestionale Farmacia Comunale)	si	24/48	24/48

Comune di SCICLI

Via Francesco Mormina Penna, 2 - 97018 Scicli (RG)
Tel. 0932 839111
PEC protocollo@pec.comune.scicli.rg.it
P.Iva 00080070881

Infrastruttura di rete

Descrizione della infrastruttura di rete

Location	N. punti rete WAN	N. punti rete LAN
01 – Municipio	1	100
02 – Palazzo Mormino (Delegazione Donnalucata)	1	2
03 – Protezione Civile (c.da Zagarone)	1	3
04 – Ufficio Cimiteriale	1	4
05 – Palazzo Spadaro	1	1
06 – Sede C.so Mazzini – Via Lume	1	18
07 – Biblioteca Comunale	1	7
08 – Centro Polifunzionale (c.da Zagarone)	1	17
09 – Mercato c.da Spinello	1	1
10 – Polizia Municipale	1	27
11 – Farmacia Comunale	1	6
12 – Via Tagliamento	1	40

VERIFICA DELLA CONFORMITÀ E MIGLIORAMENTO DELLA SICUREZZA DEI DATI

Per una corretta gestione del rischio è necessario identificare un insieme di attività critiche o operative dell'organizzazione, quali, a esempio, le seguenti :

Identificazione dei rischi (Area rischio)

- Risorse di rete e tecniche (hardware e software);
- Processi / procedure relativi all'operazione di trattamento dei dati;
- Diverse parti e persone coinvolte nell'operazione di trattamento;
- Settore di operatività e scala del trattamento.

Analisi e valutazione

Il processo di analisi e valutazione del rischio relativo alla protezione dati (della sicurezza delle informazioni), tenendo conto della norma UNI CEI EN ISO/IEC 270011, viene eseguito in modo che:

a) stabilisca e mantenga i criteri di rischio relativo alla sicurezza delle informazioni che includano:

- i criteri per l'accettazione del rischio;
- i criteri per effettuare valutazioni del rischio relativo alla sicurezza delle informazioni;

b) assicuri che ripetute valutazioni del rischio relativo alla sicurezza delle informazioni producano risultati coerenti, validi e confrontabili tra loro;

c) identifichi i rischi relativi alla sicurezza delle informazioni:

- applicando il processo di valutazione del rischio relativo alla sicurezza delle informazioni per identificare i rischi associati alla perdita di riservatezza, di integrità e di disponibilità delle informazioni incluse nel campo di applicazione del sistema di gestione per la sicurezza delle informazioni;
- identificando i responsabili dei rischi;

d) analizzi i rischi relativi alla sicurezza delle informazioni:

- valutando le possibili conseguenze che risulterebbero se i rischi identificati si concretizzassero;
- valutando la verosimiglianza realistica del concretizzarsi dei rischi identificati;
- determinando i livelli di rischio;

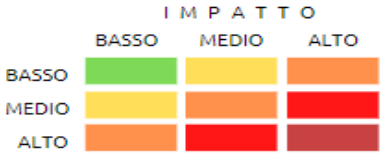
e) ponderi i rischi relativi alla sicurezza delle informazioni:

- comparando i risultati dell'analisi del rischio con i criteri di rischio prestabiliti;
- stabilendo le priorità dei rischi analizzati per il trattamento del rischio.

Via Francesco Mormina Penna, 2 - 97018 Scicli (RG)
Tel. 0932 839111
PEC protocollo@pec.comune.scicli.rg.it
P.Iva 00080070881

POSTAZIONI DI LAVORO COMPUTER

PROBABILITA' GENERALE DI MINACCIA



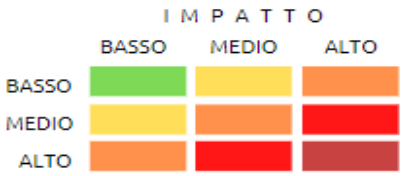
Elementi connotativi:

Non tutti i PC aggiornati ma protetti da antivirus

MEDIO-BASSO

INFRASTRUTTURA FISICA

PROBABILITA' GENERALE DI MINACCIA



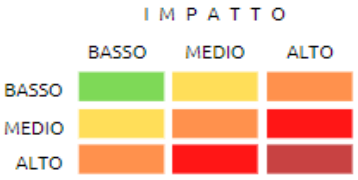
Elementi connotativi:

Server correttamente aggiornato e protetto

MEDIO-BASSO

DATI SERVER-STORAGE-CLOUD

PROBABILITA' GENERALE DI MINACCIA



Elementi connotativi:

Cloud per procedura e portale web fornito da Isp certificati

BASSO-MEDIO

L'organizzazione conserva valutazioni specifiche e documentate sul processo di valutazione del rischio relativo alla sicurezza delle informazioni. Per l'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza - i cui compiti, obiettivi ed aspetti organizzativi sono stati definiti dal Regolamento (UE) 2019/881 del 17 aprile 2019 - finalizzata ad applicarsi in ogni specifico contesto operativo e nei processi di un'organizzazione." In questo contesto, al fine di valutare il rischio concreto nell'ottica di adottare le misure tecniche e organizzative adeguate al rischio presentato, fondate sulla norma UNI EN ISO/IEC 27001, di cui sopra. Le Linee guida definiscono un approccio alla valutazione del rischio, che si basa su quattro fasi.

Il processo può essere così sintetizzato:

- Individuazione e registrazione dei pericoli;
- Valutazione dei pericoli per determinare il livello di rischio;
- Individuazione delle misure di prevenzione e protezione;
- Definizione del programma di miglioramento.

MONITORAGGIO E CONTROLLI

Descrizione delle procedure di monitoraggio e di controllo del funzionamento del sistema.

- Audit annuale programmato - Entro il mese di Marzo di ogni anno
- Audit straordinario - se il sistema presenta un aggiornamento o modifica importante
- Test di funzionamento e sopralluoghi per rilevamento denotativo e connotativo del sistema.
- Se necessario si prevede una procedura di penetration test.

Via Francesco Mormina Penna, 2 - 97018 Scicli (RG)
Tel. 0932 839111
PEC protocollo@pec.comune.scicli.rg.it
P.Iva 00080070881

Gestione dei log

N.O.	Nome Sistema/Procedura	Periodo minimo di archiviazione	Periodo massimo di archiviazione	Luogo di conservazione
01	Maggioli Sicraweb (Protocollo, Pratiche SUE, Pratiche SUAP, Contabilità e Ragioneria, Economato, Gestione Patrimonio, Gestione Economica, Notifiche Multe e Verbali, Gestione Personale, Procedimenti Disciplinari, Organi Istituzionali, Contratti, Imposta di Soggiorno)	6 mesi	6 mesi	Cloud
02	Tributi Minori e Maggiori	24 ore	24 ore	Sistema Informativo interno
03	Demografici (Anagrafe, Stato Civile, Elettorale, Leva)	n.d.	n.d.	Sistema Informativo interno
04	Software di produttività individuale (LibreOffice, Office)	3 mesi	3 mesi	Sistema Informativo interno
05	Pagamenti PagoPA	12 mesi	12 mesi	Cloud
06	Sito web CMS “FlexCMP”	12 mesi	12 mesi	Cloud
07	Sistema F Platinum Top (gestionale Farmacia Comunale)	n.d.	n.d.	Cloud

POLITICHE DI SICUREZZA

Politica di gestione della sicurezza dei sistemi (incluse le postazioni adibite a smart working)

La gestione in sicurezza delle infrastrutture informatiche ha l'obiettivo di garantire che i sistemi, le postazioni di lavoro, le applicazioni, i servizi di rete, i servizi elaborativi forniscono le prestazioni lavorative ai livelli e con i requisiti di sicurezza definiti.

Principi generali in base ai quali porre in essere la gestione sicura dei sistemi:

- deve essere gestito ed aggiornato un inventario degli asset hardware e software;
- devono essere applicate regole standard indicate dal produttore software/hardware per l'installazione e la configurazione dei sistemi;
- devono essere adottate procedure standard di configurazione dei sistemi che indirizzino:
    - disabilitazione o restrizione nell'utilizzo di alcuni particolari servizi;
    - restrizioni nell'accesso ad utilities di sistema particolarmente critiche ed a funzioni di setting di sistema;
    - utilizzo di funzioni di time-out;
    - le principali esigenze di aggiornamenti in termini di patch e di fix di sicurezza;
- le configurazioni dei sistemi devono essere archiviate ed aggiornate
- devono essere condotte regolarmente attività di monitoraggio sulle prestazioni dei sistemi al fine di gestire adeguatamente eventi, problemi e incidenti.

Gestione accessi alla documentazione informatica

Il Comune di Scicli accede alla documentazione informatica attraverso le piattaforme gestionali dedicate delle varie software house e attraverso le cartelle condivise sul sistema informativo interno.

Politica per il controllo degli accessi fisici

L'accesso fisico alla stanza dei server avviene utilizzando la chiave che è custodita presso l'Ufficio del Servizio Sistemi Informativi e Transizione Digitale ubicato nella sede Municipio.

Politica di gestione delle postazioni di lavoro

Gli elementi essenziali di questa politica sono:

- controllo delle postazioni di lavoro;
- installazione del software sulle postazioni di lavoro effettuata dal personale autorizzato;
- installazione degli aggiornamenti;
- smaltimento apparati mobili e supporti dati effettuato da personale autorizzato previa compilazione di un modulo contenente la dichiarazione di avvenuta distruzione dei dati;

GESTIONE DEGLI INCIDENTI

Si definisce "incidente di sicurezza" qualsiasi evento che comprometta o minacci di compromettere il corretto funzionamento dei sistemi e/o delle reti dell'organizzazione o l'integrità e/o la riservatezza delle informazioni in esse memorizzate od in transito, o che violi le politiche di sicurezza definite o le leggi in vigore (con particolare riferimento al d.lgs. 196/2003, alla L. 547/1993 ed alla L. 38/2006).
L'organizzazione deve classificare gli incidenti definendone la codifica preventiva e la gestione degli stessi (a esempio, seguendo le indicazioni della norma ISO 27035:2011 "*Information technology — Security techniques — Information security incident management*").

Il processo di gestione degli incidenti è articolato nelle seguenti fasi:

- rilevazione/identificazione/classificazione - vengono riconosciuti uno o più eventi di sicurezza come incidente e a ogni incidente ne viene assegnato un livello di gravità. Il rilevamento avviene a valle delle segnalazioni provenienti da strumenti automatici o ancora da segnalazioni del personale dell'amministrazione;

- contenimento - vengono attuate le prime contromisure, allo scopo di minimizzare i danni causati dall'incidente. In genere si tratta di azioni temporanee e veloci, di cui effettuare il roll-back dopo la successiva fase di eliminazione;
- eliminazione - vengono eliminate le cause che hanno portato al verificarsi dell'incidente;
- ripristino - vengono effettuate le operazioni necessarie per riparare i danni causati dall'incidente e si effettua il roll-back delle contromisure di contenimento;
- follow-up – viene verificata l'adeguatezza delle procedure di gestione degli incidenti e vengono identificati i possibili punti di miglioramento.

Per le procedure di gestione degli incidenti si rimanda al protocollo operativo GDPR.

Redazione	*Verifica*	*Approvazione*
SGARLATA MARIA 23.12.2024 12:43:08 GMT+01:00	firmato digitalmente da 2024.12.23 16:42:50 FRANCESCO PETINO	**Signed by:** GRUTTADAURIA NADIA **Issuer:** Namirial CA Firma Qualificata **Signing time:** 23-12-2024 17:08 UTC +01