



è un marchio Maggioli Spa

Santarcangelo di Romagna, 11/12/2017

DICHIARAZIONE DI CONFORMITÀ SERVIZI CLOUD MAGGIOLI IN TEMA DI MISURE MINIME DI SICUREZZA (Circ. Agid 2/2017)

Gentile Cliente,

con la presente si informa che i servizi Cloud di Maggioli S.p.a. erogati dai propri Datacenter sono conformi alle indicazioni della Circolare Agid n.2/2017 del 18 aprile 2017 in relazione alle «*Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)*». I nostri servizi Cloud Hosting/IaaS/PaaS sono sottoposti a specifiche e rigorose certificazioni e controlli inerenti la sicurezza dei dati quali ISO27001 (di cui riportiamo il certificato) e ne rispettano le direttive Agid sino a permettere a Maggioli Spa lo status di conservatore accreditato Agid (<http://www.agid.gov.it/agenda-digitale/pubblica-amministrazione/conservazione/elenco-conservatori-attivi>) Poiché per precisione la circolare n.2/2017 riporta punti di diversa competenza e dominio (postazioni e/o risorse locali, dominio di tipo applicativo ecc..) elenchiamo di seguito quelli correlati a servizi Cloud Hosting/IaaS/PaaS oggetto della presente dichiarazione di conformità.

Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	ABSC 1.1.1
Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	ABSC 1.1.3
Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	ABSC 1.3.1
Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	ABSC 2.3.1
Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	ABSC 2.3.3
Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	ABSC 3.1.1
Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	ABSC 3.2.1

Maggioli Informatica
via Bornaccino, 101
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 621153
informatica@maggioli.it
www.maggioli.it



Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	ABSC 3.2.2
Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	ABSC 3.4.1
Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	ABSC 4.1.1
Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	ABSC 4.4.1
Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	ABSC 4.5.1
Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio	ABSC 4.7.1
Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	ABSC 4.7.2
Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	ABSC 4.8.1
Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	ABSC 4.8.2
Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	ABSC 5.1.1
Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	ABSC 5.1.2
Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	ABSC 5.2.1
Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	ABSC 5.5.1
Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	ABSC 5.7.3
Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	ABSC 5.7.3
Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le	ABSC 5.10.3

situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	
Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	ABSC 5.11.1
Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	ABSC 8.1.3
Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	ABSC 10.1.1
Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	ABSC 10.1.2
Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	ABSC 10.1.3
Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	ABSC 10.2.1
Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	ABSC 10.3.1
Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	ABSC 10.4.1

Cordiali Saluti

Maggioli Informatica
Responsabile Sistemi
Oscar Bevoni



Maggioli Informatica
via Bornaccino, 101
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 621153
informatica@maggioli.it
www.maggioli.it



Italia

CERTIFICATO

Nr 50 100 9442 - Rev. 06

Si attesta che / This is to certify that

IL SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI DI
THE INFORMATION SECURITY MANAGEMENT SYSTEM OF

MAGGIOLI S.p.A.

SEDE LEGALE E OPERATIVA: / REGISTERED OFFICE AND OPERATIONAL SITE:

VIA DEL CARPINO 8 I-47822 SANTARCANGELO DI ROMAGNA (RN)

ALTRE SEDI OPERATIVE: VEDI ALLEGATO 1
OTHER OPERATIONAL SITES: SEE ANNEX 1

È CONFORME AI REQUISITI DELLA NORMA
HAS BEEN FOUND TO COMPLY WITH THE REQUIREMENTS OF

UNI CEI ISO/IEC 27001:2014

QUESTO CERTIFICATO È VALIDO PER IL SEGUENTE CAMPO DI APPLICAZIONE
THIS CERTIFICATE IS VALID FOR THE FOLLOWING SCOPE

Erogazione di: servizi di inserimento dati, anche presso la sede del cliente, degli atti elevati dalla Polizia Municipale o altri uffici della Pubblica Amministrazione; servizi di stampa, rendicontazione, postalizzazione e riscossione connessi alla gestione delle sanzioni amministrative. Progettazione, sviluppo, analisi e manutenzione di sistemi informativi socio-sanitari sia legati a prodotti sviluppati dal Gruppo, sia orientati alla system integration di prodotti di mercato. Erogazione di servizi di data center: housing, hosting, cloud computing, disaster recovery. Erogazione di servizi di conservazione digitale di documenti informatici. Progettazione, sviluppo, analisi, manutenzione, assistenza e delivery di piattaforme di e-procurement (IAF 33, 35)

Provision of data entry, even at the customer site, services of acts by the municipal police or other offices of public administration, printing, reporting, mailing and collection services related to administrative penalties management. Design, analysis, realization maintenance of social and health information systems products both developed by the "Gruppo Maggioli" and integration of market products. Provision of data center services: housing, hosting, cloud computing, disaster recovery. Provision of conservation of electronic documents. Design, analysis, realization, maintenance, support and delivery of e-procurement platforms (IAF 33, 35)

Dichiarazione di applicabilità: Rev.2.0 del 20/09/2016