Euro Informatica Sistemi S.r.l.

SEDE
Via Principe di Napoli, 126
00062 Bracciano (Roma)
Tel. 06.99.80.31.31 – Fax 06.99.80.3027

FILIALE
Via Fiume 55/a/b
00055 Ladispoli (Roma)
Tel. 06.99.22.2012 – Fax 06.99.22.6763
www.euroinf.it
info@euroinf.it
info@pec.euroinf.it

GDPR AUDIT
CHECK LIST TECNICA

Ver 1.8 del 26/04/2018

CONSULENTE: _____ *DATA VISITA:*_____
RAGIONE SOCIALE OPPURE NOME E COGNOME_____
INDIRIZZO SEDE LEGALE CAP CITTA' PROVINCIA_____
TELEFONO FAX PARTITA IVA_____
E-MAIL E/O WEB SITE REFERENTE_____
CHECK LIST PER LA SEDE DI : INDICARE IL NUMERO DI SEDI OLTRE QUESTA:

- *(Compilare check list per ogni sede del cliente)*

1. Struttura informatica cliente

Descrivere, brevemente, la struttura del cliente :

_____
_____
_____

- *(Es. Gli uffici sono su vari piani, ogni ufficio ha una sala CED al piano, ogni armadio rack ha un firewall, etc)*

1.1 Numero computer presenti in azienda: _____
Quanti pc sono collegati alla rete aziendale? _____
Indicare il numero dei pc e relative versioni del sistema operativo :

n° ____ win _____ mac _____ linux/unix _____altro _____
n° ____ win _____ mac _____ linux/unix _____altro _____
n° ____ win _____ mac _____ linux/unix _____altro _____
n° ____ win _____ mac _____ linux/unix _____altro _____
n° ____ win _____ mac _____ linux/unix _____altro _____
n° ____ win _____ mac _____ linux/unix _____altro _____

- *NOTE IMPORTANTI : WINDOWS XP NON E' A NORMA IN QUANTO MICROSOFT NON RILASCIA PIU' AGGIORNAMENTI, E' NECESSARIO IMPOSTARE AGG.AUTOMATICI DEL S.O., PER RENDERE PIU' EFFICACI LE PROTEZIONI*

1.2 Su questi computer viene effettuata Teleassistenza in remoto?

☐ Si ☐ No

Se SI, indicare l'azienda che effettua la manutenzione e il software di accesso remoto:

_____

· *(SUGGERIMENTO: Accertarsi di aver autorizzato l'azienda esterna all'accesso alla rete aziendale e all'elaboratore elettronico).*

1.3 Esiste un elenco dei dispositivi presenti in azienda? ☐ Si ☐ No

· *(SUGGERIMENTO: dispositivi da tracciare nella rete sono: Computer, stampanti, altri device. La lista dei dispositivi deve essere conservata insieme al resto della documentazione predisposta per il GDPR come da allegato "Misure tecniche – Elenco dipositivi.xlsx")*

1.4 Viene utilizzato un software per il rilevamento dei dispositivi nella rete?

☐ Si ☐ No

1.5 I dispositivi come sono identificati nella rete?

☐ Indirizzo dinamico DHCP ☐ Indirizzo Statico IP ☐ Indirizzo MAC

1.6 I computer sono protetti all'accesso con password? ☐ Si ☐ No

· *(N.B. Ogni utente deve avere la password)*

Le password vengono modificate/aggiornate? ☐ Si ☐ No

Se "SI", con quale frequenza? ☐ 60gg ☐ 90gg ☐ 120gg ☐ altro _____

· *NOTE IMPORTANTI: L'agenzia per l'Italia Digitale suggerisce un cambio password almeno trimestrale*

1.7 E' presente almeno un'utenza "amministratore" sui singoli computer?

☐ Si ☐ No

· *(Se presenti più amministratori di sistema diversificare le password di accesso)*

1.8 Gli utenti hanno profili limitati sui singoli computer?

☐ Si ☐ No

1.9 Sono presenti utenti "Ospiti" o "Guest" sui singoli computer?

☐ Si ☐ No

· *(SUGGERIMENTO: E' consigliabile avere un profilo "Guest" su alcuni computer in modo da avere delle utenze disponibili per soggetti esterni)*

2. PROTEZIONE DELLO STRUMENTO

2.1 Indicare le protezioni in uso, (SI/NO):

2.2 Indicare le misure adottate per "Rete" (indicare nome prodotto):

Antivirus _____

Antimalware _____

Firewall _____ ☐ Hardware ☐ Software

Altro _____

· *(completa le informazioni di sicurezza firewall al punto dal 2.5-2.8)*

2.3 Indicare le misure adottate per "Computer" (indicare nome prodotto):

Antivirus _____

Antimalware _____

Firewall _____ ☐ Hardware ☐ Software

Altro _____

2.4 Indicare le misure adottate per "Server" (indicare nome prodotto):

Antivirus _____

Antimalware _____

Firewall _____ ☐ Hardware ☐ Software

Altro _____

- *NOTE IMPORTANTI: Gli Antivirus gratuiti non garantiscono una sicurezza adeguata. Nel caso di una struttura con almeno 5 PC consigliamo di installare un Antivirus di Rete. (se di rete compilare punto "7.")*

2.5 In azienda viene utilizzato il FIREWALL? ☐ Si ☐ No

- *(Dispositivo per la sicurezza della rete che permette di monitorare il traffico in entrata e in uscita nella rete e che utilizza*

Protezione Rete Computer server

Antivirus ☐ Si ☐ No ☐ Si ☐ No ☐ Si ☐ No

- Eseguite aggiornamenti? ☐ Si ☐ No ☐ Si ☐ No ☐ Si ☐ No

Antimalware ☐ Si ☐ No ☐ Si ☐ No ☐ Si ☐ No

- Eseguite aggiornamenti? ☐ Si ☐ No ☐ Si ☐ No ☐ Si ☐ No

Firewall ☐ Si ☐ No ☐ Si ☐ No ☐ Si ☐ No

- Eseguite aggiornamenti? ☐ Si ☐ No ☐ Si ☐ No ☐ Si ☐ No

Altro ☐ Si ☐ No ☐ Si ☐ No ☐ Si ☐ No

- Eseguite aggiornamenti? ☐ Si ☐ No ☐ Si ☐ No ☐ Si ☐ No

una serie predefinita di regole di sicurezza per consentire o bloccare gli eventi.

Se Si, che tipo di Firewall? ☐ Software ☐ Hardware

Se Software indicare il nome: _____

- *(NB. di solito utilizzato da utenti poco esperti, facilmente vulnerabile)*

Se Hardware indicare il Mod.: _____

Indicare il tipo di protezione:

☐ HTTPS ☐ SSL ☐ TLS ☐ Altro _____

Vengono eseguiti gli aggiornamenti del firmware o delle patch?

☐ Si ☐ No

Indicare il nome del referente informatico che si occupa della manutenzione:

_____ della società _____

2.6 Si fa utilizzo di Proxy sul browser di navigazione web?

☐ Si ☐ No

Se Si indicare il nome del software: _____

- *(Non Anonymous proxy (NOA), Anonymous Proxy Server, High Anonymous Proxy, proxy http)*

3. COPIE DI SICUREZZA – UTENTE CLIENT

3.1 Si effettuano periodicamente le copie di sicurezza dei dati dei PC Client?

☐ Si ☐ No

- *(SUGGERIMENTO: Se le copie di sicurezza vengono effettuate dai server compilare i campi al punto 5 "SERVER")*

Se SI su quale supporto viene effettuata la copia di sicurezza?

☐ RAID ☐ HD EST. ☐ NAS ☐ DVD ☐ USB ☐ CLOUD ☐ ALTRO _____

- *(SUGGERIMENTO: Se la copia è effettuata sul Cloud, accertarsi che la trasmissione avvenga in modo protetto)*

3.2 Con quale frequenza viene effettuata la copia di sicurezza?

☐ Giornaliera ☐ Settimanale ☐ Mensile ☐ altro _____

3.3 In quale sede vengono conservate le copie di sicurezza

☐ All’interno della sede aziendale

☐ Luoghi diversi dalla sede aziendale _____

3.4 In quali luoghi vengono custodite le copie di sicurezza?

☐ Armadio ☐ Cassetto ☐ Cassaforte ☐ Caveau

☐ altro _____

3.5 In caso di trattamento di dati particolari, l'azienda effettua la cifratura della copia di sicurezza?

☐ Si ☐ No

3.6 Che tipo di cifratura viene utilizzata?

_____

_____

- *(crittografia, pki, controller di dominio, pseudonimizzazione)*

3.7 Chi è il soggetto che materialmente effettua le copie di sicurezza?

_____

4. TRATTAMENTO DATI PARTICOLARI - UTENTE

4.1 L'azienda effettua la pseudonimizzazione dei dati particolari?

☐ Si ☐ No

- *(SUGGERIMENTO: documentazione sanitaria dei dipendenti)*

4.2 Se SI, come viene effettuata? Descrivere il processo:

_____

_____

_____

4.3 L'azienda effettua la cifratura dei dati particolari memorizzati sui PC Client?

☐ Si ☐ No

4.4 Se SI, come viene effettuata? Descrivere il processo:

_____

_____

- *(Attenzione la cifratura del dato deve avvenire anche per comunicazioni email)*
- *(SUGGERIMENTI: Con la suite di Microsoft Office si proteggono singoli documenti, con le pen-drive USB crittografate della Kingstone il contenuto dell’unità, oppure Software e archiviazione in cloud protetto.)*

5. GESTIONE DEI SERVER/NAS

5.1 Di quanti server è dotata l’azienda? _____

Indicare n°, marca, sistema operativo, reparto(Es.Amm/Tecnico), funzione (Es. backup, gestionali)

N° __ Mod._____ S.O _____ Reparto _____ Funzione _____
N° __ Mod._____ S.O _____ Reparto _____ Funzione _____
N° __ Mod._____ S.O _____ Reparto _____ Funzione _____
N° __ Mod._____ S.O _____ Reparto _____ Funzione _____
N° __ Mod._____ S.O _____ Reparto _____ Funzione _____

5.2 Su questi server viene effettuata Teleassistenza in remoto?

☐ Si ☐ No

Se SI, indicare l’azienda che effettua la manutenzione e il software di accesso remoto:

_____

- *Accertarsi di aver autorizzato l'azienda esterna all'accesso alla rete aziendale e all'elaboratore elettronico.*

5.3 Descrivere la collocazione fisica dei server

☐ armadio rack ☐ Data center ☐ Caveau ☐ altro _____

5.4 Sono previste delle protezioni fisiche dei server?

☐ porte di accesso monitorate ☐ grate alle finestre

☐ sistema di condizionamento ☐ gruppo di continuità/elettrogeno

☐ pavimento flottante ☐ sistema di videosorveglianza interno

☐ accesso biometrico con riconoscimento facciale e iride

☐ altro_____

6. COPIE DI SICUREZZA – SERVER/NAS

6.1 Si effettuano periodicamente le copie di sicurezza dei dati dei SERVER?

☐ Si ☐ No

6.2 Se SI su quale supporto viene effettuata la copia di sicurezza?

☐ RAID ☐ HD EST. ☐ NAS ☐ DVD ☐ USB ☐ CLOUD ☐ ALTRO _____

- *(SUGGERIMENTO: Se la copia è effettuata sul Cloud, accertarsi che la trasmissione avvenga in modo protetto)*

6.3 Con quale frequenza viene effettuata la copia di sicurezza?

☐ Giornaliera ☐ Settimanale ☐ Mensile ☐ altro _____

6.4 In quale sede vengono conservate le copie di sicurezza

☐ All'interno della sede aziendale

☐ Luoghi diversi dalla sede aziendale _____

6.5 In quali luoghi vengono custodite le copie di sicurezza?

☐ Armadio ☐ Cassetto ☐ Cassaforte ☐ Caveau

☐ altro _____

6.6 Si effettuano copie ridondanti dei server? ☐ Si ☐ No

Se Si, indicare le modalità:

_____

_____

_____

6.7 L'azienda effettua la cifratura dei dati particolari memorizzati sui SERVER?

☐ Si ☐ No

Se Si, come viene effettuata?

_____

_____

6.8 In caso di trattamento di dati particolari, l'azienda effettua la cifratura della copia di sicurezza?

☐ Si ☐ No

Se Si, come viene effettuata?

_____

_____

6.9 Chi esegue le copie di sicurezza?

_____

7. RETI WIRELESS (WI-FI)

7.1 In azienda è presente una rete wi-fi/wi-max? ☐ Si ☐ No

7.2 Se SI, quali impostazioni di crittografia della password vengono usati?

☐ Wep 64/128 ☐ Wpa 802.1x ☐ Wpa2 AES ☐ Altro _____

7.3 Utilizzate password robuste ed efficaci? ☐ Si ☐ No

- *(Min. 8 caratteri, Maiuscole minuscole, numeri, caratteri speciali #)*

7.4 Limitate l'accesso alla rete ai dispositivi autorizzati? ☐ Si ☐ No

- *(Azione in uso sui router consentono la memorizzazione dei dispositivi)*

Se Si, hanno un accesso temporaneo con creazione di account dedicato?

☐ Si ☐ No

7.5 L'accesso è consentito anche ai dispositivi personali? ☐ Si ☐ No

Se Si, hanno un accesso limitato ☐ Si ☐ No

Se Si, hanno un accesso temporaneo con creazione di account dedicato?

☐ Si ☐ No

8. Periferiche di rete

8.1 Scanner/MFP/Stampanti di rete

L'accesso alla stampante/MFP/scanner di rete avviene con accesso protetto da password?

☐ Si ☐ No

Viene utilizzato lo spool di stampa per identificare il client da dove è partita la stampa?

☐ Si ☐ No

L'accesso ai file digitalizzati mediante scanner/Mfp di rete, avviene con strumenti di autenticazione? ☐ Si ☐ No

Questi dispositivi, memorizzano i dati in un archivio interno? ☐ Si ☐ No

Se Si, l'accesso alle informazioni è protetto da password? ☐ Si ☐ No

8.2 Plotter

L'accesso alla periferica grafica di rete avviene con accesso protetto da password?

☐ Si ☐ No

Viene utilizzato nelle impostazioni della periferica grafica un separatore che nello spool di stampa identifica il client da dove è partita la stampa?

☐ Si ☐ No

L'accesso ai file digitalizzati mediante la periferica grafica, avviene con strumenti di autenticazione? ☐ Si ☐ No

8.3 Kit Videoconferenza

Lo streaming dei filmati avviene con autenticazione sulle porte del router?

☐ Si ☐ No

8.4 Kit di Geolocalizzazione

Sono presenti strumenti di geolocalizzazione in azienda?

☐ Si ☐ No

Se Si indicare il tipo di strumento e lo scopo:

_____

Dove viene installato? ☐ Persone ☐ Mezzi ☐ Altro _____

9. Device

9.1 Smartphone

In caso di richiesta di accesso alla rete aziendale da parte di soggetti esterni avviene mediante la creazione di un account temporaneo dedicato?

☐ Si ☐ No

L'accesso alle periferiche di rete aziendali avviene con uno strumento di autenticazione?

☐ Si ☐ No

9.2 Tablet

In caso di richiesta di accesso alla rete aziendale da parte di soggetti esterni avviene mediante la creazione di un account temporaneo dedicato?

☐ Si ☐ No

L'accesso alle periferiche di rete aziendali avviene con uno strumento di autenticazione?

☐ Si ☐ No

9.3 Bring Your Own Device – Dispositivi personali

L'accesso alla rete aziendale avviene mediante la creazione di un account temporaneo dedicato? ☐ Si ☐ No

L'accesso alle periferiche di rete aziendali avviene con uno strumento di autenticazione?

☐ Si ☐ No

10. Business Continuity Disaster Recovery

10.1 Esiste un piano di Business Continuity/ Disaster recovery?

☐ Si ☐ No

Se Si selezionare l'area di appartenenza e indicare il soggetto responsabile interno:

☐ Infrastruttura di rete _____

☐ Infrastruttura software_____

☐ Altro _____ _____

Se Si selezionare l'area di appartenenza e indicare il soggetto responsabile esterno:

☐ Infrastruttura di rete _____

☐ Infrastruttura software_____

☐ Altro _____ _____

10.2 In quanto tempo è previsto il ripristino del sistema?

_____

Note:

_____
_____
_____
_____

Timbro e firma per accettazione

_____