



GIUFFRÈ EDITORE

DOTT. A. GIUFFRÈ EDITORE S.p.A.

Manuale Operativo PdA – Vers. 1.3

Manuale Operativo del Punto di Accesso al Processo Telematico e alle consultazioni Polisweb

SOMMARIO

STORIA DELLE MODIFICHE APPORTATE, DEFINIZIONI E ACRONIMI, RIFERIMENTI	3
1 PREMESSA	4
2 DATI IDENTIFICATIVI	4
2.1 PUNTO DI ACCESSO	4
2.2 GESTORE	4
2.3 VERSIONE DEL MANUALE OPERATIVO	5
2.4 RESPONSABILE DEL MANUALE OPERATIVO E REFERENTI TECNICI	5
3 DEFINIZIONE DEGLI OBBLIGHI DEL TITOLARE DEL PUNTO DI ACCESSO E DI COLORO CHE VI ACCEDONO PER	5
3.1 OBBLIGHI DEL TITOLARE	5
3.2 OBBLIGHI DEGLI UTENTI	7
4 DEFINIZIONE DELLE RESPONSABILITÀ E LIMITAZIONI AGLI INDENNIZZI	10
4.1 CONOSCENZA DEL MANUALE OPERATIVO	10
4.2 LIMITAZIONI DI RESPONSABILITÀ	11
4.3 DECADENZA	11
4.4 MANLEVA	11
5 TARIFFE E CONDIZIONI	11
5.1 TARIFFE	11
5.2 CONDIZIONI D'USO	11
6 MODALITÀ DI AUTENTICAZIONE, REGISTRAZIONE E GESTIONE DEGLI UTENTI	11
6.1 AUTENTICAZIONE DEGLI UTENTI	11
6.2 GESTIONE DEGLI UTENTI	12
6.2.1 REGISTRAZIONE E ATTIVAZIONE	12
6.2.2 MODIFICA DEI RECAPITI E DEL CERTIFICATO DI CIFRATURA	13
6.2.3 CANCELLAZIONE	13
6.2.4 DISABILITAZIONE	13
6.2.5 VARIAZIONE DELLO STATUS DIFENSORE	14
6.3 GESTIONE DELLE ABILITAZIONI	14
6.4 GESTIONE DELLE DELEGHE	14
7 INDIRIZZI ELETTRONICI	15
7.1 MODALITÀ DI ATTIVAZIONE E GESTIONE DEGLI INDIRIZZI ELETTRONICI	15
7.2 MODALITÀ DI ATTIVAZIONE E GESTIONE DELLE CASELLE DI POSTA ELETTRONICA CERTIFICATA	15
7.3 MODALITÀ DI GESTIONE DEL REGISTRO DEGLI INDIRIZZI ELETTRONICI	15
7.4 MODALITÀ DI ACCESSO AL REGISTRO DEGLI INDIRIZZI ELETTRONICI	15
8 POLITICHE E PROCEDURE DI SICUREZZA	15
9 PROCEDURE DI GESTIONE DELLE ANOMALIE RELATIVE AI FLUSSI DI INTERFACCIA CON IL GESTORE CENTRALE	16

STORIA DELLE MODIFICHE APPORTATE

VERS.	DATA EMISS.	DESCRIZIONE
1.0	23/02/2010	Prima emissione.
1.1	16/04/2010	Revisione in base alle indicazioni della DGSIA.
1.2	10/05/2010	Modifica della ubicazione dell'hardware su cui è installato il PdA
1.3	07/10/2011	Aggiunta gestione abilitazione "segretarie" e deleghe

DEFINIZIONI E ACRONIMI

DEFINIZIONI	
Utente utilizzatore	Soggetto iscritto al PdA allo scopo di usufruirne dei servizi.
Titolare del Punto di Accesso	Dott. A. Giuffrè Editore S.p.A.

ACRONIMI	
CA	Certification Authority, ovvero, Autorità di Certificazione
CdO	Consiglio dell'Ordine
CNS	Carta Nazionale dei Servizi
GC	Gestore Centrale
Giuffrè	Dott. A. Giuffrè Editore S.p.A.
MO	Manuale Operativo
PCT	Processo Civile Telematico
PdA	Punto di Accesso al Processo Telematico e alle consultazioni Polisweb
Re.G.Ind.E.	Registro Generale degli Indirizzi Elettronici
Re.L.Ind.E.	Registro Locale degli Indirizzi Elettronici
SICI	Sistema Informatico Civile
SIECIC	Sistema Informatico Esecuzioni Civili Individuali e Concorsuali

RIFERIMENTI

RIFERIMENTO	DESCRIZIONE
[RT]	Ministero della Giustizia – Decreto 17 luglio 2008 – Regole Tecnico-Operative per l'uso di strumenti informatici e telematici nel processo civile
[SI]	DGSIA. – Specifiche di Interfaccia tra Punto di Accesso e Gestore Centrale, vers. 3.0
[PV]	DGSIA. – Piano delle Verifiche per il rilascio dell'autorizzazione ai punti di accesso, vers. 2.2
[PSD]	DGSIA. – Procedura di segnalazione disservizi invio/ricezione PdA, vers. 1.1
[SIA]	DGSIA. – Specifiche per l'invio, variazioni e cancellazione di tutto o parte dell'albo Avvocati, vers. 1.4
[WS]	DGSIA. – Specifiche tecniche per l'esposizione dei servizi di consultazione, vers. 2.0
[PW-ST]	DGSIA. – Polisweb – Specifiche tecniche, vers. 4.1
[PW-IT]	DGSIA. – Polisweb – Indicazioni tecnico-pratiche, vers. 1.1
[PW-PV]	DGSIA. – Polisweb – Piano delle Verifiche per il rilascio dell'autorizzazione ai punti di accesso limitati a Polisweb, vers. 1.0
[PC]	CNIPA - Regole Tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata

1. PREMESSA

Il presente *Manuale Operativo* (d'ora in poi *MO*) ha lo scopo di illustrare, ai sensi dell'articolo 33 delle Regole Tecnico-Operative ([RT]) e successive specifiche della DGSIA. ([SI],[PV]), come attualmente pubblicate sul sito ufficiale del Processo Civile Telematico, le procedure adottate dalla società Dott. A. Giuffrè Editore S.p.A. (d'ora in poi *Giuffrè*) per l'erogazione del servizio denominato "*Punto di Accesso al Processo Telematico e alle consultazioni Polisweb*" (d'ora in poi *PdA*).

In particolare, il presente documento descrive le procedure operative, gli obblighi, le garanzie, le responsabilità e le misure di sicurezza adottate dalla Giuffrè nel ruolo di Gestore del Punto di Accesso. Inoltre illustra gli obblighi, le modalità di autenticazione, registrazione e gestione degli utenti, le modalità di attivazione e gestione degli indirizzi elettronici e le modalità di accesso e gestione del registro degli indirizzi elettronici. La Giuffrè si riserva di apportare variazioni al presente documento per esigenze tecniche o per modifiche alle procedure intervenute sia a causa di norme di legge o regolamenti, sia per ottimizzazioni del ciclo lavorativo. Ogni nuova versione pubblicata del manuale, annulla e sostituisce le precedenti versioni.

2. DATI IDENTIFICATIVI

2.1 Punto di Accesso

Codice identificativo	PDAGIUFFRE
Descrizione PdA	Punto di Accesso attivato e gestito da Dott. A. Giuffrè Editore S.p.A.
Sedi operative	Dott. A. Giuffrè Editore S.p.A. Via Busto Arsizio, 40 - 20151 Milano Tel. 02 38089 456 - Fax 02 38089 454 Giuffrè Informatica srl Via Ceccaroni n. 53 - 62100 Macerata Tel. 0733 230561 - Fax 0733 233155
Ubicazione hardware	Presso il Datacenter di Seeweb S.r.l., Corso Lazio 9/a - Frosinone
Nome secondo lo standard X.500	http://pda.giuffre.it/
Indirizzo web	https://pda.giuffre.it/
Casella di posta elettronica di sistema	pdagiuffre@pda.giuffre.it
Dominio della posta elettronica ordinaria	pda.giuffre.it
Dominio della posta elettronica certificata	pec-pt.giuffre.it

2.2 Gestore

Denominazione	Dott. A. Giuffrè Editore S.p.A.
Partita Iva	00829840156
Sede legale	Via Busto Arsizio, 40 - 20151 Milano
Telefono	02 – 38089 456
Fax	02 – 38089 454
E-mail	giuffre@giuffre.it
Indirizzo internet	http://www.giuffre.it
Rappresentante legale	Ing. Antonio Giuffrè - In qualità di Direttore Generale con deleghe

2.3 Versione del Manuale Operativo

Il presente MO è di proprietà della Giuffrè. Questo documento è la versione 1.1 del Manuale Operativo, è individuato da codice interno **PdA_Giuffre_MO_v1.1** ed è consultabile per via telematica al seguente URL: http://pda.giuffre.it/doc/PDAGIUFFRE_MO_v1.1.pdf.

2.4 Responsabile del Manuale Operativo e referenti tecnici

Il responsabile del presente MO, nonché referente per la DGSIA è:

Paolo Della Costanza
 Tel. 0733 - 230561; cell. 335 - 732 4552
 E-mail: paolo.dellacostanza@giuffre.it

I referenti tecnici per la DGSIA, i CISIA locali e le sedi distrettuali competenti sono:

ing. Andrea Paternesi
 Tel. 0733 - 230561; cell. 335 - 1028 375
 E-mail: andrea.paternesi@giuffre.it

dott. Andrea Mariottini
 Tel. 0733 - 230561; cell. 335 - 732 4553
 E-mail: andrea.mariottini@giuffre.it

ing. Marcello De Geronimo (consulente)
 Tel. 095 - 2939 117
 PEC: marcello.degeronimo@ingpec.eu

Servizi Informatici di Diego Zanga (consulente)
 Tel. 335 - 5890 692
 E-mail: admin@edp-si.it

3. DEFINIZIONE DEGLI OBBLIGHI DEL TITOLARE DEL PUNTO DI ACCESSO E DI COLORO CHE VI ACCEDONO PER L'UTILIZZO DEI SERVIZI

3.1 Obblighi del Titolare

Nello svolgimento della sua attività, il Titolare del Punto di Accesso, in base a quanto indicato in [RT] artt. 28, 29, 30 e 32, e successive modificazioni ([SI] e [PV]):

1. afferma di possedere i requisiti richiesti dall'art.6, comma 6, lettere a) e b) delle Regole Tecnico-Operative [RT];
2. fornisce ai soggetti abilitati esterni i servizi di consultazione del SICI e di trasmissione telematica degli atti e garantisce il rilascio dei biglietti cancelleria al mittente del singolo atto;
3. garantisce la verifica dei titoli dell'utente ad accedere al servizio attraverso la ricezione da parte dello stesso della necessaria documentazione comprovante la propria iscrizione all'ordine territoriale di competenza. Fornisce il servizio di autenticazione dei soggetti abilitati, per l'accesso al SICI, come previsto dall'art. 8 delle Regole Tecnico-Operative [RT];
4. mantiene un *registro degli indirizzi elettronici* contenente l'elenco di detti indirizzi emessi, revocati o sospesi dal *Punto di Accesso* e ne rende disponibile una *copia operativa*, secondo quanto specificato negli artt. 16, 18 e 19 delle Regole Tecnico-Operative [RT];

5. garantisce che la comunicazione tra la postazione informatica del soggetto abilitato esterno e il *Punto di Accesso* avvenga mediante canale sicuro;
6. implementa l'invio di documenti informatici secondo i flussi previsti dalle Regole Tecnico-Operative [RT] e successive specifiche della DGSIA. ([SI],[PV]);
7. fornisce il servizio di ricezione, inviando, in risposta ad ogni documento informatico ricevuto dal Gestore Centrale o da un altro Punto di Accesso, una ricevuta breve di avvenuta consegna;
8. verifica l'assenza di virus informatici in ogni messaggio in arrivo e in partenza;
9. garantisce, per un periodo non inferiore a cinque anni, la conservazione di tutti i messaggi inviati e ricevuti;
10. mette a disposizione degli utenti i servizi di consultazione esposti dal gestore locale a beneficio dei soggetti abilitati esterni;
11. garantisce che l'autenticazione dei soggetti abilitati esterni avvenga secondo le specifiche previste dalle Regole Tecnico-Operative [RT] e successive specifiche della DGSIA. ([SI],[PV]);
12. stabilisce le connessioni con il Gestore Centrale e i gestori locali esclusivamente secondo le modalità indicate dal DGSIA.;
13. garantisce l'accesso alla consultazione dei dati secondo le regole tecniche stabilite dal Ministero della Giustizia;
14. documenta dettagliatamente le procedure per la fornitura dei servizi attuate sul manuale operativo, previsto dall'art. 33 delle Regole Tecnico-Operative [RT];
15. documenta dettagliatamente nel piano per la sicurezza, previsto dall'art. 34 delle Regole Tecnico-Operative [RT] tutte le azioni e le procedure di sicurezza attivate;
16. garantisce il salvataggio dei dati utili con frequenza almeno giornaliera;
17. registra gli eventi significativi nel funzionamento del *Punto di Accesso* sul *Giornale di Controllo*, di cui all'art. 35 delle Regole Tecnico-Operative [RT];
18. garantisce l'uso di canali di autenticazione in SSL versione 3, con chiave a 1024 bit, ove richiesto dalle Regole Tecnico-Operative [RT] e dal DGSIA.;
19. esegue la sua attività in seguito all'iscrizione come previsto dall'art. 32 delle Regole Tecnico-Operative [RT].

Inoltre il Titolare del Punto di Accesso si impegna a non divulgare i dati personali dell'utente a terzi e ad usarli unicamente per l'erogazione del servizio, nel rispetto della normativa vigente sulla Privacy (Decreto Lgs. 196/03).

Il Titolare del Punto di Accesso garantisce il supporto necessario agli utenti attraverso un servizio di help desk secondo le modalità descritte nell'apposita pagina del PdA, <https://pda.giuffre.it/supporto>.
Le modalità di supporto possono essere riviste a seconda delle effettive esigenze degli utenti rilevate durante l'attività di esercizio.

3.2 Obblighi degli utenti

Gli utenti, nell'usufruire dei servizi offerti dal Punto di Accesso, in base a quanto indicato in [RT] art. 36, [SI] e [PV] devono usare postazioni di lavoro adeguate. In particolare la postazione di lavoro dei soggetti abilitati esterni deve:

1) Avere l'insieme delle risorse hardware, software e di rete adeguate per la formazione dei documenti informatici, per l'inoltro e la ricezione dei messaggi e per la consultazione del SICI.

2) Essere dotata dell'hardware e del software necessario alla gestione della firma digitale su smart card, e all'autenticazione nei confronti del *Punto di Accesso*, conformemente alle Regole Tecnico-Operative [RT] e successive specifiche della DGSIA.

Per quanto riguarda l'autenticazione, sono considerati attendibili i certificati firmati dalle seguenti autorità emittenti:

CN=ArubaPEC S.p.A. NG CA1, O=ArubaPEC S.p.A., chiave pubblica:

```
b2:bb:6e:3a:cc:22:f2:9d:90:c7:01:f1:9f:6d:
e8:35:5b:1c:5b:fb:21:27:7c:eb:db:f3:27:18:e9:
db:e0:f3:62:9e:b5:d9:19:cb:87:86:60:b8:b9:be:
98:ea:96:89:10:02:87:20:30:5d:62:c8:f7:1e:6d:
48:13:38:d2:1e:3f:a2:f0:96:12:25:41:85:f6:16:
c7:f7:a5:f0:cb:ac:29:0d:b6:d6:b5:df:af:db:55:
91:95:f3:11:a5:ae:fb:80:42:dc:0a:63:1f:80:1f:
f2:54:6e:23:9d:73:46:2d:a4:68:92:6e:3c:98:62:
ab:af:de:78:44:62:3c:94:1d:88:35:c2:2c:27:87:
c5:17:7e:b4:f8:58:53:55:70:13:a8:6e:bd:76:b8:
a8:05:5d:fd:ab:58:33:ff:56:2e:c4:2e:f9:15:36:
87:f2:ad:21:de:ba:f1:21:4b:3a:6c:c0:c4:0f:1d:
5b:80:84:e5:df:ad:22:49:da:31:e3:3b:fa:be:75:
7e:4d:13:fc:7f:47:6d:a9:a0:99:75:bc:36:f7:8e:
e0:78:83:06:be:b2:9a:2d:da:8b:15:e8:55:86:77:
d9:dd:be:ad:fb:d6:de:a1:92:b2:00:41:da:a0:03:
68:b4:e7:56:d4:1f:2a:0f:bc:01:8f:f7:6b:1c:2e:
68:f3
```

CN=Consiglio Nazionale Forense - Autenticazione, O=Consiglio Nazionale Forense, chiave pubblica:

```
ba:14:77:4f:21:80:8e:50:0c:52:96:60:48:4d:
17:a9:0a:6a:72:80:67:b0:39:59:f5:85:dd:fc:34:
f5:c7:dd:e9:98:c2:66:d6:5e:69:81:5f:08:16:94:
2e:87:f7:75:cb:1d:55:e7:c0:13:94:25:2b:59:1c:
95:12:07:bd:04:52:cf:e3:d3:7a:c3:d3:16:b0:5d:
8f:6f:4a:50:3b:19:6e:ef:b6:ec:66:83:22:bc:17:
a6:63:51:04:51:a7:e0:aa:90:7d:ce:37:98:c4:8c:
46:09:b4:56:65:7f:61:08:40:0c:2a:ab:8f:2b:9d:
e5:a3:24:c5:73:76:68:d2:6e:83:b5:0c:4e:cb:03:
3f:eb:38:5e:a0:3b:e9:1d:bf:db:81:c2:5f:9f:cc:
7c:ae:e2:50:35:b8:a0:76:91:34:ed:88:95:0d:ee:
31:b4:08:8c:42:6f:c9:df:46:1b:d2:4a:fb:36:3e:
d1:2a:19:34:c2:b2:3e:98:57:34:23:82:b4:81:2e:
28:e1:8c:36:89:9f:68:0a:fe:03:18:62:b0:58:1e:
ac:27:66:b9:22:d6:95:fe:cc:ed:99:19:36:e9:4c:
56:65:b0:0c:fe:dc:7d:4b:7a:00:00:67:7d:b4:0f:
0d:b6:9a:36:0f:2e:f3:1a:63:af:36:39:9c:61:6a:
4e:69
```

CN=InfoCamere Servizi di Certificazione, O=InfoCamere SCpA, chiave pubblica:

```
c4:92:e2:73:94:ba:a9:7f:2a:80:1a:98:4e:9b:
```

22:64:de:89:fa:c2:77:31:74:98:64:b2:57:bb:90:
1c:7c:2a:dc:68:e4:f4:7e:26:e7:61:71:d9:6d:18:
22:41:f1:e7:ee:d4:4e:aa:1f:64:9e:f3:ab:62:96:
32:c1:1a:b9:8f:f9:e7:e4:b5:06:d3:ff:ce:84:8c:
cc:c2:e2:0e:06:c6:57:33:dd:96:40:36:9b:50:22:
4d:0f:82:51:bf:b2:50:97:02:64:5e:e0:0f:92:f1:
06:c4:5e:44:c1:07:2b:54:9e:ce:7b:87:18:bc:5a:
16:7b:14:ce:fc:9f:84:56:43:51:60:94:4c:e3:a4:
0d:e0:e3:f5:99:30:a1:4f:9d:36:a4:84:22:5e:de:
ed:cc:44:18:7e:b9:16:f7:30:b9:28:9c:08:82:99:
32:d5:02:ca:07:c2:c8:2c:b1:a2:b7:db:b7:16:24:
5b:f9:77:44:6d:c0:2c:31:de:3a:27:e1:72:09:2e:
ce:ef:30:3d:81:48:15:30:06:37:4a:ca:76:80:8d:
f2:a2:ae:96:29:fa:c4:28:4b:79:bc:f0:6d:75:18:
7c:fa:cc:67:d9:00:cc:14:c5:39:da:56:86:9d:ca:
25:9b:15:f5:34:4b:dc:b7:a0:fc:21:9c:bf:50:2e:
fb:99

CN=InfoCamere Servizi di Certificazione 2, O=InfoCamere SCpA, chiave pubblica:

fd:36:b5:48:9c:c0:2f:a6:ce:ca:ec:7f:14:c8:
23:45:63:96:46:77:4a:0b:4d:c9:ce:29:1d:6f:dc:
a7:90:c0:43:97:72:ad:da:cb:87:cc:a9:ef:7c:bc:
ec:29:b5:d2:e0:55:f8:7b:db:1d:c2:71:b7:9a:0e:
06:94:02:d0:2a:9a:8c:40:42:84:e3:1b:bd:99:b9:
61:77:71:ca:d8:8e:98:76:98:19:3b:75:d3:02:2f:
4b:38:63:be:9a:66:84:e4:3e:13:f0:20:83:fc:03:
8f:9f:aa:20:45:1f:54:80:a8:77:5d:5e:67:9d:fe:
34:0d:a7:3b:4c:ac:18:10:5f:c4:87:f8:cb:aa:a4:
9a:d8:1c:13:96:c5:ae:bf:dd:b8:d2:53:12:bc:96:
03:e9:15:57:bd:23:6e:04:ce:83:0a:fc:82:db:26:
b4:82:62:bc:19:84:e2:1f:2b:a9:d8:e0:a5:2a:d0:
a0:dc:c5:94:d6:d6:66:04:89:ca:59:d9:4d:bc:c4:
ed:10:4d:29:f5:0b:2f:33:26:2b:54:8d:7e:96:02:
b3:de:ba:29:ce:83:f0:d6:3a:b0:5d:7d:9c:0a:19:
ec:46:af:c4:17:5a:6c:6e:8a:79:99:08:89:29:c5:
c4:cc:36:39:83:5b:b4:ac:d8:db:c7:20:90:d6:46:
08:fd

CN=InfoCert Servizi di Certificazione, O=INFOCERT SPA, chiave pubblica:

ce:aa:75:eb:4c:bd:7c:2f:87:38:03:82:0b:d7:
99:be:72:45:d9:5d:d0:65:47:48:79:1b:2c:8c:4d:
01:d6:18:24:d9:85:07:6f:74:f9:05:69:b3:12:53:
d3:fc:f1:c0:5a:7e:0b:a8:03:45:a0:0a:30:9d:b8:
25:a5:bc:ca:d3:79:ee:55:e0:76:51:c8:b6:08:4b:
8d:36:f0:ae:b6:ca:cd:c6:91:ed:6f:06:58:67:60:
bd:ae:1e:e1:d7:dd:32:c4:dd:7a:32:0b:2c:fe:62:
6f:7f:20:3f:99:9c:0d:c8:ff:a4:fb:90:26:4d:88:
cd:77:86:b8:30:75:ec:b3:f0:8a:69:e2:f5:73:37:
e7:45:0a:35:6d:06:bd:bd:8f:95:a9:eb:14:ae:cf:
c8:a0:a2:3b:a6:07:71:12:e5:19:bf:e7:d0:0d:89:
42:63:34:72:6a:d5:a7:f8:e7:6c:4a:24:02:9b:4a:
bc:a0:f3:7a:1f:11:46:3e:4c:87:0d:8c:a3:02:78:
57:a5:de:37:24:b9:e9:67:c5:8b:65:3f:0b:18:60:
0a:99:fb:a9:c7:5f:49:b6:3f:76:df:27:0c:4a:fc:
fc:cd:06:1b:25:83:a6:ad:5a:b0:69:20:b1:64:78:
21:2b:07:c5:33:7e:72:28:6d:0e:83:94:66:16:07:
b6:69

CN=Postecom CA1, O=Postecom s.p.a., chiave pubblica:
e5:63:3b:f7:3a:bf:a8:d1:1f:da:41:da:c2:6d:
be:45:b0:af:ee:5c:47:2f:65:93:4f:59:34:78:a1:
eb:04:60:4d:db:f8:cb:10:32:d8:ba:40:90:7d:f4:
37:6a:28:e9:e6:6c:66:fe:c6:d2:26:f1:0c:e2:da:
e1:4c:21:da:fc:26:af:1b:eb:da:29:8a:ab:97:96:
11:ab:43:c2:64:00:ba:72:3d:87:16:c5:76:ef:4c:
8e:c8:d7:83:a7:9c:bd:68:15:ec:b7:03:fa:48:da:
6a:95:1a:be:98:84:e3:af:e0:67:6c:2c:95:f7:b0:
12:68:f6:ae:c2:8e:d6:e6:7a:b6:18:fb:04:9f:10:
d6:db:52:10:9b:87:76:24:d5:c7:ce:15:45:88:e7:
62:03:4a:c4:2c:37:5c:0f:d6:50:2a:88:11:01:43:
ba:e5:f5:11:6a:ff:5a:b1:b6:63:e8:e9:c1:de:cb:
3c:d4:5a:04:c0:95:69:45:9b:ea:e3:94:01:50:4f:
e2:7e:6f:c4:ad:aa:1e:bd:76:ea:25:ce:2c:07:8b:
d8:cb:7d:5d:63:ae:49:7c:cd:d4:6e:1d:4d:5a:b8:
25:f7:07:64:81:56:8c:70:ae:da:d9:c6:63:f5:18:
ee:3f:89:8c:07:4c:bf:93:5d:35:39:60:2c:f7:2a:
93:89

CN=Postecom CA2, O=Postecom S.p.A., chiave pubblica:
ae:92:18:c5:8f:ba:64:8d:20:cc:bb:2b:96:d7:
5d:47:af:9c:50:a7:9d:f5:e6:50:cf:26:39:c5:64:
be:ee:99:79:ed:1e:b4:9c:3a:c9:a2:23:3a:12:34:
6c:7a:da:df:3e:0f:89:92:a2:46:9a:d6:61:8e:ef:
3a:62:31:dc:4a:48:d7:1e:f5:cc:3b:f7:5a:27:64:
b3:f5:42:6e:22:16:95:cd:7a:94:74:35:0c:fd:37:
bc:08:11:7e:e8:c0:58:5a:aa:cd:50:b9:4f:9c:d9:
27:82:bc:a6:b4:c5:8f:10:88:5e:09:c4:de:35:cc:
ac:73:5a:f1:f7:1b:d4:d2:8b:86:b1:18:19:96:e8:
6f:75:6a:b7:2b:70:2a:7e:0f:86:f6:e3:f5:96:17:
03:93:81:a4:37:ec:10:f2:ab:da:91:71:68:11:d2:
17:95:0e:89:63:fb:3d:9d:8d:5c:ad:3f:a4:28:b8:
62:74:1f:2b:ad:9a:2b:80:24:16:9b:04:43:41:c9:
07:b3:b3:9c:9a:b2:08:33:ee:a9:a6:6f:4a:8d:6a:
6b:d1:f0:38:be:70:fb:df:13:7d:c1:8f:4d:56:61:
5a:71:1e:b3:40:21:12:5c:c0:fd:2c:27:84:a9:12:
96:f1:36:6b:b2:f1:7a:df:73:59:86:1a:ad:40:34:
16:99

Inoltre, per certificati di autenticazione emessi in data successiva al 31 dicembre 2008, si richiede che il dispositivo di autenticazione rispetti le specifiche previste per la Carta Nazionale dei Servizi (CNS), conformemente alle indicazioni del Ministero di Giustizia.

Il PdA è tecnicamente predisposto per configurare altre autorità emittenti accreditate. La configurazione può avvenire in seguito alla segnalazione da parte di un utente al Titolare del Punto di Accesso o per iniziativa del Gestore del PdA stesso, previa comunicazione al DGSIA.

Indicazioni aggiornate sui dispositivi crittografici utilizzabili sono disponibili nell'apposita area del sito all'indirizzo <http://pda.giuffre.it/smartcard>.

3) Essere dotata di software idoneo a verificare l'assenza di virus informatici in ogni messaggio in arrivo e in partenza.

Per le problematiche inerenti l'installazione e la configurazione dei dispositivi di autenticazione e firma digitale, gli utenti devono fare riferimento al proprio fornitore.

Ogni utente è tenuto a:

1. Informare tempestivamente il Gestore del Punto di Accesso in caso di:
 - perdita del possesso del dispositivo di autenticazione (smarrimento, furto, ecc.);
 - guasto o cattivo funzionamento del dispositivo di autenticazione;
 - compromissione della segretezza della chiave privata;
 - cessata attività o altre cause analoghe;
 utilizzando i recapiti telefonici e/o l'e-mail indicati nel presente manuale - in modo da consentire al Gestore del Punto di Accesso la disattivazione dell'utente stesso; il Gestore del Punto di Accesso provvederà alla disattivazione dopo opportune verifiche.
2. Prendere atto di essere l'unico responsabile della protezione della propria chiave privata da danni, perdite o sottrazioni, divulgazioni, modifiche o usi non autorizzati della stessa o del dispositivo che la contiene.
3. Richiedere, in caso di smarrimento o sottrazione del dispositivo di autenticazione, la sospensione immediata del certificato, contattando il certificatore, provvedere alla disabilitazione del certificato smarrito o del proprio account, usando l'apposito comando disponibile sulla pagina <https://pda.giuffre.it/profilo> o chiedendo supporto al Gestore del Punto di Accesso per la disabilitazione, e sporgere denuncia alle autorità competenti. Confermato il caso di furto o smarrimento deve inoltrare richiesta di revoca al certificatore allegando copia della relativa denuncia.
4. Comunicare la variazione dei dati presentati al momento della registrazione (par. 6.2.1) attraverso l'apposita funzione resa disponibile dal PdA (<https://pda.giuffre.it/profilo>).

Indicativamente i requisiti minimi relativi al software di sistema per accedere al servizio, e salvo ulteriori adeguamenti a seguito di test, sono i seguenti:

- Sistemi operativi: Windows 98, Windows 2000, Windows XP e Windows Vista, MacOS (varie versioni), Linux.
- *Browser*: MS Internet Explorer, versione 6.0 o successiva; Mozilla Firefox, Safari.

4. DEFINIZIONE DELLE RESPONSABILITÀ E LIMITAZIONI AGLI INDENNIZZI.

4.1 Conoscenza del Manuale Operativo

Gli utenti sono tenuti a consultare preventivamente ed a conoscere il presente Manuale Operativo e i successivi aggiornamenti che verranno pubblicati nel sito all'indirizzo: <http://pda.giuffre.it/doc/>.

4.2 Limitazioni di responsabilità

La Dott. A. Giuffrè Editore S.p.a., in qualità di soggetto privato abilitato all'attivazione e gestione del Punto di Accesso ai sensi dell'art. 6, comma 6, lett. a) del D.M.17/7/2008, non è responsabile in relazione a impossibilità (totale o parziale) dell'utente di accedere ai servizi derivante da:

- inosservanza delle previsioni contenute nel presente Manuale Operativo;
- non conformità del certificato di autenticazione alla normativa sul PCT e alle specifiche ministeriali;
- fatto di terzi di cui a titolo esemplificativo e non esaustivo: uso illegittimo dei dispositivi di autenticazione; errori dell'Ente Certificatore che rilascia i certificati al singolo utente; indisponibilità, malfunzionamento, mancata o errata manutenzione dei sistemi hardware e/o software e/o delle basi dei dati in capo al Gestore Locale e/o al Gestore Centrale;
- caso fortuito, forza maggiore, atti della Pubblica Autorità.

La responsabilità della Dott. A. giuffrè Editore S.p.A. quale gestore del PdA è in ogni caso limitata al solo dolo o colpa grave.

In particolare la Dott. A. Giuffrè S.p.A. in qualità di Gestore del Punto di Accesso non presta alcuna garanzia per danni di qualsiasi natura, diretti od indiretti, derivanti da cause non imputabili alla stessa, se non nei casi di proprio dolo o colpa grave.

4.3 Decadenza

Il danneggiato decade dal diritto al risarcimento del danno imputabile al PdA qualora non invii entro 5 giorni dal verificarsi dell'evento dannoso, ovvero dalla sua scoperta, lettera raccomandata R.R. contenente le motivazioni a fondamento della eventuale pretesa presso la sede legale della Dott. A. Giuffrè Editore S.p.A. sita in via Busto Arsizio n. 40 – 20151 Milano.

4.4 Manleva

L'utente dichiara di manlevare e tenere indenne la società Dott. A. Giuffrè Editore S.p.a. in qualità di Titolare e gestore del Punto di Accesso, da qualsiasi responsabilità, spesa, pregiudizio o danno, diretto o indiretto, derivante da pretese o azioni giudiziarie da parte di terzi di cui essa sia chiamata a rispondere per fatto imputabile all'utente, ivi espressamente incluse, a titolo esemplificativo e non esaustivo, le responsabilità e i danni derivanti dalla eventuale erroneità o non attualità delle informazioni o dei dati rilasciati al Punto di Accesso.

5 TARIFFE E CONDIZIONI D'USO

5.1 Tariffe

Gli utenti che intendono usufruire del servizio di accesso al PdA hanno l'onere al momento della loro iscrizione, di versare un canone annuo il cui importo è pubblicato sul sito <http://pda.giuffre.it>. Il pagamento del suddetto canone permette all'utente di usufruire del servizio per un periodo di 12 mesi esatti. Qualora allo scadere dei 12 mesi l'utente non provveda a rinnovare il pagamento della quota per ulteriori 12 mesi, il servizio viene immediatamente sospeso, lasciando all'utente la possibilità di cancellarsi e di consultare la propria CPECPT.

5.2 Condizioni d'uso

Verificati requisiti di accesso ai servizi, ricevuta la documentazione cartacea prevista al successivo punto 6.2.1, verificato l'avvenuto pagamento, la Dott. A. Giuffrè Editore S.p.A. consentirà al richiedente di accedere ai servizi del PCT, entro un tempo minimo necessario per l'espletamento degli aspetti burocratici connessi e comunque non prima dell'allineamento dei registri una volta inviata la richiesta di abilitazione al GC.

La Dott. A. Giuffrè Editore S.p.A in qualità di Gestore del servizio Punto di Accesso, si riserva il diritto di apportare modifiche al servizio, alle condizioni contrattuali, alle tariffe, alle specifiche tecniche del servizio (per sopravvenute esigenze tecniche, legislative e gestionali) ed alle previsioni del Manuale Operativo. Tali modifiche saranno comunque apportate in ottemperanza a quanto stabilito dalle Regole Tecnico-Operative ([RT]) e successive specifiche della DGSIA. ([SI],[PV]).

6 MODALITÀ DI AUTENTICAZIONE, REGISTRAZIONE E GESTIONE DEGLI UTENTI

L'autenticazione, la registrazione e la gestione degli utenti avvengono secondo quanto stabilito dalle Regole Tecnico-Operative ([RT]) e successive specifiche della DGSIA. ([SI],[PV]).

6.1 Autenticazione degli utenti

L'autenticazione di un utente avviene soltanto se sono rispettate le seguenti condizioni:

- l'utente si connette via *browser* con il PdA autenticandosi tramite un dispositivo crittografico conforme alle Regole Tecnico-Operative ([RT]) e successive specifiche della DGSIA. ([SI],[PV]), presentando un certificato valido;
- l'utente risulta iscritto al PdA;

- l'utente non è stato temporaneamente disabilitato.

Agli utenti con status *non attivo* viene consentita comunque l'autenticazione, come richiesto dalla DGSIA., tenendo presente che lo status dell'utente "viaggia" con gli atti depositati, per cui la gestione, presso la cancelleria, degli atti depositati in base allo status *radiato* o *sospeso* del difensore può avvenire come accade normalmente nell'ambito dei depositi "cartacei".

Per quanto riguarda il dispositivo di autenticazione, sono considerate attendibili le *Autorità di Certificazione* (CA) accreditate dal CNIPA di cui al precedente punto 3.2. Inoltre, per certificati di autenticazione emessi in data successiva al 31 dicembre 2008, si richiede che il dispositivo di autenticazione rispetti le specifiche previste per la *Carta Nazionale dei Servizi* (CNS), conformemente alle indicazioni del Ministero di Giustizia.

Indicazioni aggiornate sui dispositivi crittografici utilizzabili per l'autenticazione sono disponibili nell'apposita area del nostro sito internet all'indirizzo: <http://pda.giuffre.it/smartcard>.

L'avvenuta autenticazione implica l'instaurarsi di un canale sicuro fra il browser dell'utente e il PdA utilizzando SSL v.3 e chiavi lunghe 1024 bit.

Anche per l'*Interfaccia Amministrativa* del PdA la comunicazione avviene su canale sicuro utilizzando SSL v.3 e chiavi lunghe 1024 bit, ma l'autenticazione non avviene verificando, oltre alla firma da parte della CA emittente, il solo codice fiscale dell'utente. Piuttosto viene verificata la corrispondenza dell'intero certificato abilitato. Ovvero l'utente non può accedere presentando altri certificati digitali registrati a suo nome. Inoltre l'interfaccia amministrativa è accessibile solo dagli IP stabiliti dal Titolare del PdA.

6.2 Gestione degli utenti

6.2.1 Registrazione e attivazione

Premesso che il PdA fornisce il servizio unicamente ai soggetti abilitati esterni come descritti nelle Regole Tecnico-Operative ([RT]) e successive specifiche della DGSIA. ([SI],[PV]), la registrazione, come disposto dall'art. 14 delle Regole Tecnico-Operative [RT], prevede che l'utente compili una richiesta scritta, che il Titolare del PdA conserva per almeno dieci anni, contenente i seguenti dati:

- nome e cognome;
- luogo e data di nascita;
- codice fiscale;
- indirizzo della residenza anagrafica;
- indirizzo del domicilio legale;
- certificato digitale, relativo alla chiave pubblica, per la cifratura;
- consiglio dell'ordine di appartenenza.

Come previsto per i punti di accesso privati, verrà inoltre richiesto di allegare alla domanda in originale:

- a. per gli avvocati un certificato, rilasciato in data non anteriore a venti giorni, in cui il consiglio dell'ordine attesta l'iscrizione all'albo, all'albo speciale, al registro dei praticanti abilitati oppure la qualifica che legittima all'esercizio della difesa e l'assenza di cause ostative allo svolgimento dell'attività difensiva;
- b. per i consulenti tecnici il certificato di iscrizione all'albo dei consulenti tecnici o copia della nomina da parte del giudice dalla quale risulta che l'incarico non è esaurito;

La procedura di iscrizione viene espletata da parte dell'utente accedendo, tramite smart card, alla pagina <https://pda.giuffre.it/iscrizione>, che consente di impostare il certificato di cifratura e di stampare la domanda d'iscrizione in modo semplice ed intuitivo. L'utente, quindi, è tenuto a inviare la domanda firmata con firma autografa al Gestore del PdA.

La documentazione richiesta comprensiva della domanda firmata ed in originale, deve essere inoltrata per posta, usando i recapiti indicati nella pagina del supporto <https://pda.giuffre.it/supporto>, oppure può essere consegnata dall'utente stesso *brevi manu* al personale dell'Agenzia della Dott. A. Giuffrè Editore S.p.A. della sua zona. La lista delle Agenzie Giuffrè è consultabile via web all'indirizzo <http://pda.giuffre.it>.

La pagina d'iscrizione consente anche di impostare l'inoltro di una copia di ogni comunicazione pervenuta sul PdA verso caselle e-mail ordinarie.

Il Gestore del PdA, una volta ricevuta la richiesta scritta, dopo le dovute verifiche evade la domanda in sospeso ed inoltra la richiesta al GC attraverso l'*Interfaccia Amministrativa del PdA*. Tale procedura avviene secondo le modalità stabilite dalle Regole Tecnico-Operative ([RT]) e successive specifiche della DGSIA. ([SI],[PV]).

La generazione dell'indirizzo elettronico dell'utente avviene al momento dell'accesso alla pagina d'iscrizione mentre l'inizializzazione della relativa CPEPPT avviene automaticamente al momento della ricezione della *Comunicazione Indirizzi PdA* di iscrizione dal GC. Infine, l'effettiva attivazione dell'account avviene solo in seguito all'iscrizione dell'utente nel *Registro Generale degli Indirizzi Elettronici* (d'ora in poi *Re.G.Ind.E.*).

Al momento dell'accesso alla pagina d'iscrizione viene anche generato un certificato di cifratura per l'utente della durata di dieci anni, con CA firmataria identica a quella del certificato usato per firmare le buste S/MIME dei depositi.

Tale certificato viene proposto come quello predefinito per l'iscrizione, fermo restando che l'utente può facilmente impostarne uno diverso.

Il PdA esegue ogni notte la ricerca degli utenti con iscrizione in sospeso all'interno del *Re.G.Ind.E.*, allo scopo di attivarli e allineare il *Re.L.Ind.E.*.

La verifica e l'eventuale allineamento del *Re.L.Ind.E.* avvengono anche ad ogni tentativo di accesso, da parte di un utente in attesa di attivazione (limitatamente all'utente stesso).

6.2.2 Modifica dei recapiti e del certificato di cifratura

La modifica dei recapiti e/o del certificato di cifratura di un utente deve essere sottoposta dall'utente stesso tramite l'apposita pagina del PdA, <https://pda.giuffre.it/profilo>.

Una volta avvenuto l'inoltro, il PdA gestisce la richiesta come prescritto dalle Regole Tecnico-Operative ([RT]) e successive specifiche della DGSIA. ([SI],[PV]).

La modifica del *Re.L.Ind.E.* avviene in seguito alla ricezione, dal GC, della *Comunicazione Indirizzi PdA* di tipo M (Modifica). Una volta inoltrata la richiesta di modifica, l'utente non potrà inoltrarne altre fino al completamento del flusso, che si conclude con l'allineamento del *Re.L.Ind.E.*.

Attraverso la pagina del profilo, l'utente può anche eseguire la sospensione del certificato di cifratura fornitogli dal PdA.

6.2.3 Cancellazione

Un utente può inoltrare la richiesta di cancellazione per un qualunque motivo dallo stesso ritenuto valido ed in qualsiasi momento.

La richiesta di cancellazione deve essere inoltrata usando l'apposito pulsante disponibile sulla pagina <https://pda.giuffre.it/profilo>.

La cancellazione dal *Re.L.Ind.E.* avviene in seguito alla ricezione, dal GC, della *Comunicazione Indirizzi PdA* di tipo C (Cancellazione). Tuttavia l'accesso al PdA viene già inibito al momento dell'inoltro della richiesta di cancellazione. Come previsto dalle regole tecniche, in seguito alla cancellazione, l'utente potrà continuare ad usufruire dei servizi di consultazione Polisweb per un periodo di 180 giorni.

6.2.4 Disabilitazione

Un utente può richiedere la disabilitazione del proprio *account* per un qualunque motivo dallo stesso ritenuto valido ed in qualsiasi momento.

La disabilitazione può essere eseguita usando l'apposito link disponibile sulla pagina <https://pda.giuffre.it/profilo> o rivolgendosi al Gestore del PdA.

Per l'abilitazione di un *account* disabilitato, l'utente interessato deve rivolgersi al Gestore del PdA, in quanto questa operazione può essere effettuata solo tramite l'interfaccia amministrativa del PdA.

La casella CPECPT e i flussi in ingresso relativi ad un utente disabilitato vengono mantenuti attivi e il Gestore del PdA si adopera per superare in tempi brevi i problemi che hanno portato alla decisione di disabilitare l'*account*.

6.2.5 Variazione dello status di un difensore

La variazione dello status di un difensore viene comunicata telematicamente dall'Ordine di appartenenza del difensore stesso, in seguito alla variazione dello status sull'albo.

Nel caso di radiazione dall'albo o se vengono rilevate cause ostative allo svolgimento dell'attività difensiva, lo status dell'utente sui registri elettronici viene cambiato in *non attivo*.

L'aggiornamento del Re.L.Ind.E. avviene in seguito alla ricezione, dal GC, della *Comunicazione Indirizzi* Gestore del PdA di tipo V (Variazione).

Lo scambio di messaggi tra PdA, GC e CdO avviene sempre per via telematica, e le comunicazioni sono strutturate in linguaggio XML, secondo i formati definiti nel relativo decreto ministeriale.

Di seguito una descrizione del flusso:

- Il Consiglio dell'Ordine che vuole variare lo stato di un difensore, crea un file XML contenente i dati dell'avvocato e il nuovo stato (attivo, sospeso, radiato, ecc.);
- Il file XML viene inviato al Gestore Centrale tramite la CPECPT del CdO;
- Il Gestore Centrale aggiorna il Re.G.Ind.E. con i dati del difensore;
- Il Gestore Centrale inoltra al PdA della Società il file XML ricevuto dal Consiglio dell'Ordine;
- Il PdA della Società aggiorna il Re.L.Ind.E.

6.3 Gestione delle abilitazioni

Il PdA consente ad ogni utente regolarmente iscritto di abilitare fino a due persone, tipicamente le segretarie dell'avvocato.

La richiesta deve essere confermata con l'invio di un Pdf firmato recante l'elenco delle persone da abilitare ed il loro codice fiscale.

Ogni soggetto abilitato ha la possibilità di accedere al PdA, mediante smartcard con certificato CNS con lo stesso livello di sicurezza degli utenti regolari, per consultare l'elenco la propria abilitazione e le deleghe ricevute, ma non ha altri diritti.

Tutte le abilitazioni vengono tracciate ed archiviate sul PdA, possono essere revocate in qualunque momento dall'utente che le ha sottoscritte. Ogni revoca viene tracciata sul PdA ed è costantemente verificabile. Le abilitazioni rimangono dunque valide solo se non sono revocate e solo se l'utente che ha richiesto le abilitazioni è regolarmente iscritto.

Una abilitazione non consente l'accesso al PdA, se l'utente che l'ha richiesta revoca la propria iscrizione al PdA o il relativo contratto scade.

6.4 Gestione delle deleghe

Il PdA consente ad ogni utente regolarmente iscritto di delegare le proprie funzioni ad altri utenti del PdA, siano questi utenti regolarmente iscritti o semplicemente abilitati. Questi previo accesso a mezzo smartcard con certificato CNS e livello di sicurezza già indicato nel manuale operativo, può effettuare delle ricerche con il codice fiscale e ruolo dell'utente delegante.

La richiesta di delega va confermata mediante l'invio di Pdf firmato, con la CNS del delegante, recante l'elenco delle persone delegate ed il loro codice fiscale, nonché elenco esatto delle funzioni delegate (al momento questa consultazione è a mezzo browser o consultazione a mezzo web service regolarmente esposti). La delega viene effettuata sotto la responsabilità diretta ed unica dell'utente delegante, indicata nel documento della delega stessa.

Tutte le deleghe vengono tracciate ed archiviate sul PdA, possono essere revocate in qualunque momento dall'utente che le ha sottoscritte. Ogni revoca viene tracciata sul PdA ed è costantemente verificabile. Le deleghe rimangono dunque valide solo se non sono revocate e solo se riguardano utenti regolarmente iscritti o abilitati.

Una delega non consente la consultazione dei dati per conto del delegante se questo perde i diritti di consultazione: cioè nel caso di sospensione del delegante o radiazione del delegante, o se il delegante revoca la propria iscrizione al PdA o il relativo contratto scade.

7. INDIRIZZI ELETTRONICI

Il PdA mantiene un *registro degli indirizzi elettronici* contenente l'elenco di detti indirizzi emessi, revocati o sospesi dal PdA stesso e ne rende disponibile una *copia operativa*, secondo quanto specificato negli artt. 16, 18 e 19 delle Regole Tecnico-Operative [RT].

7.1 Modalità di attivazione e gestione degli indirizzi elettronici

Il PdA attribuisce ad ogni utente un indirizzo elettronico univoco al momento dell'accesso alla pagina d'iscrizione, come descritto nel par. 6.2.

Gli indirizzi elettronici restano invariati, anche in seguito a una variazione dei dati o alla disabilitazione dell'utente.

7.2 Modalità di attivazione e gestione delle caselle di posta elettronica certificata

Ogni casella CPECPT viene inizializzata al momento della ricezione della *Comunicazione Indirizzi PdA* di iscrizione da parte del GC.

Attualmente il limite di capienza di ogni casella è illimitato ma in seguito, a fronte di specifiche esigenze di amministrazione del sistema e previo accordi con la DGSIA, potrebbe essere imposta una limitazione ragionevole alla dimensione delle caselle.

La casella di posta certificata è conforme a quanto previsto dalle regole tecniche del CNIPA [PC], salvo quanto previsto nelle Regole Tecnico-Operative [RT] e successive specifiche della DGSIA.

Come previsto dall'art. 12 delle Regole Tecnico-Operative [RT], dopo trenta giorni i messaggi vengono archiviati e sostituiti da un avviso, che resterà disponibile per sei mesi, contenente l'identificativo univoco del messaggio, il mittente e la data completa di ora e minuti.

7.3 Modalità di gestione del registro degli indirizzi elettronici

Le informazioni contenute nel suddetto registro vengono automaticamente aggiornate nell'ambito dei flussi descritti nel capitolo 6.

7.4 Modalità di accesso al registro degli indirizzi elettronici

La *copia operativa* del registro degli indirizzi elettronici è accessibile tramite protocollo *Ldap*, all'indirizzo ***ldap://ldap-pt.giuffre.it***, come richiesto dall'art. 19 delle Regole Tecnico-Operative [RT].

La copia operativa del registro è protetta da una password, che viene messa a disposizione degli iscritti purchè la richiesta sia adeguatamente motivata.

Successivamente verranno presi in considerazione, insieme alla DGSIA, meccanismi di protezione più adeguati.

8. POLITICHE E PROCEDURE DI SICUREZZA

La Dott. A. Giuffrè editore S.p.A. si impegna a fornire un'adeguata qualità dei servizi, dei processi informatici e dei relativi prodotti, idonea a garantire la sicurezza del sistema e a non comprometterne i livelli di servizio, nel rispetto dei requisiti tecnici.

Le politiche e le procedure di sicurezza adottate dal PdA sono riportate su un apposito documento, denominato "*Piano per la sicurezza*", secondo quanto specificato nell'art. 34 delle Regole Tecnico-Operative [RT].

9. PROCEDURE DI GESTIONE DELLE ANOMALIE RELATIVE AI FLUSSI DI INTERFACCIA CON IL GESTORE CENTRALE

La DGSIA. richiede espressamente che gli utenti evitino di rivolgersi al personale del CISIA e degli Uffici Giudiziari, per segnalazioni riguardanti le comunicazioni fra Punto di Accesso, Gestore Centrale e Uffici Giudiziari. Gli utenti sono tenuti a rivolgersi unicamente all'*help desk*, secondo le modalità descritte nell'apposita pagina del PdA, <https://pda.giuffre.it/supporto> (cfr. [PSD]).

Viceversa, le anomalie sui dati esposti dagli Uffici Giudiziari tramite i sistemi Polisweb non competono il gestore del Punto di Accesso. Piuttosto, occorre rivolgersi direttamente al personale delle Cancellerie (cfr. [PW-IT]).