CORTE DI APPELLO DI SALERNO

- Manuale di sicurezza per gli utenti -

PREMESSA

La Direzione Generale per i Sistemi Informativi Automatizzati (DGSIA) ha racchiuso la normativa in materia di sicurezza di trasmissione, interscambio, accesso e conservazione dei documenti informatici nel **PSS** (Piano strategico di sicurezza), trasmesso a tutte le articolazioni Ministeriali ed Uffici Giudiziari; questi sono tenuti a realizzare le misure proattive e reattive previste, per ridurre i rischi nel campo della sicurezza informatica e reagire agli eventuali incidenti.

I documenti informatici[1] trattati dall'Amministrazione Giudiziaria sono comunque inerenti a un'attività fondamentale della Stato che deve essere preservata da intromissioni esterne; devono essere trattati al fine di garantirne integrità e provenienza, disponibilità e confidenzialità (secretazione) e devono essere tutelati nell'ambito di specifici flussi di lavoro, considerandone la struttura e le specifiche tecniche di conservazione fisica, oltre che la tipologia giuridica.

Il trattamento[2] dei dati personali, svolto da questo ufficio nell'ambito esclusivo delle sue finalità istituzionali[3], con o senza ausilio degli strumenti elettronici, deve avvenire nel rispetto dei principi fissati dall'articolo 5 del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali (*GDPR, General Data Protection Regulation)*:

- liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
- limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati: i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione di quelli che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: è necessario provvedere alla conservazione dei dati per il tempo strettamente necessario agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Per una corretta applicazione dei principi esposti, e quindi a garanzia di un'adeguata tutela dei diritti degli interessati, è importante che i dipendenti rispettino le seguenti indicazioni, tenuto conto che l'accesso alle Banche Dati avviene per mezzo di sistemi informatici censiti dalla DGSIA, sulla base dei profili di autorizzazione definiti dalle mansioni assegnate[4]:

- ☐ garantire i diritti degli interessati e comunque osservare il principio di necessità, di esattezza e aggiornamento delle informazioni trattate, nonché il principio di pertinenza;

---

[1] Art.1 lettera p) del Codice dell'Amministrazione Digitale: *rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*

[2] Art.4 nr.2): *qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.*

[3] Art.6 let.e):*il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento*

[4] art.4 nr.10 GDPR e Art. 2-quaterdecies d.lgs.196/2003.

□ trattare i dati personali di cui vengono a conoscenza nello svolgimento delle proprie funzioni in modo lecito e secondo correttezza, essendone vietata la diffusione, la comunicazione e l'utilizzo oltre il dovuto;

□ effettuare la raccolta, l'elaborazione, la registrazione ecc.. di dati personali esclusivamente per gli scopi inerenti l'attività svolta e nei limiti strettamente necessari per adempiere ai compiti assegnati;

□ osservare scrupolosamente tutte le misure di sicurezza già in atto, o che verranno comunicate in seguito dal Titolare/Responsabile/Sub-Responsabile del trattamento;

□ assicurare la custodia dei dispositivi e la segretezza delle proprie credenziali di autenticazione (utilizzare password non facilmente ricostruibile dai propri dati personali), che non dovrà essere comunicata a terzi;

□ cambiare la password almeno ogni sei mesi se sono trattati dati personali e ogni tre mesi quando sono trattati dati sensibili o giudiziari (su espressa autorizzazione di legge che specifichi la finalità di rilevante interesse pubblico, la tipologia dei dati trattati e le operazioni di trattamento);

□ evitare di lasciare aperta una sessione di lavoro, dopo essersi identificati con il proprio login e la propria password, in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;

□ in caso di prolungata assenza o impedimento del dipendente che tratta dati personali, saranno impartite (dal direttore amministrativo responsabile dell'ufficio/cancelleria) idonee e preventive disposizioni scritte volte ad individuare le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici. In tal caso, la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della custodia delle copie i quali informeranno tempestivamente il dipendente dopo ogni intervento effettuato con le sue credenziali;

□ garantire i diritti degli interessati e comunque osservare il principio di necessità., di esattezza e aggiornamento delle informazioni trattate, nonché il principio di pertinenza;

□ effettuare la raccolta, l'elaborazione, la registrazione ecc.. di dati personali esclusivamente per gli scopi inerenti l'attività svolta e nei limiti strettamente necessari per adempiere ai compiti assegnati a ciascuno;

□ mantenere aggiornate tutte le banche dati cui hanno accesso e non eccedere le finalità per le quali sono stati raccolti, elaborati e registrati;

□ evitare di creare banche dati nuove senza espressa autorizzazione;

□ conservare negli spazi e con i metodi indicati dal titolare/responsabile, tutti i documenti contenenti dati sensibili, evitando di trattenerli per un tempo superiore a quello minimo necessario per l'espletamento dei propri compiti ed in caso di interruzione anche temporanea del lavoro verificare che i dati non siano accessibili a terzi;

□ con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate;

□ evitare di asportare supporti informatici o cartacei contenenti dati personali di terzi, senza la previa autorizzazione del titolare/responsabile;

□ in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al dirigente dell'ufficio responsabile per la successiva comunicazione al titolare/responsabile del trattamento.

Di seguito i principali suggerimenti e le istruzioni per aumentare la sicurezza globale del sistema:

TRATTAMENTO DATI CON STRUMENTI ELETTRONICI
CAUTELE GENERALI

Spegnere il computer se ci si assenta per un periodo di tempo lungo

Un computer acceso è in linea di principio maggiormente attaccabile perché raggiungibile tramite la rete o direttamente sulla postazione di lavoro; più lungo è il periodo di assenza, inoltre, maggiore è la probabilità che un'interruzione dell'energia elettrica possa portare un danno.

Non lasciare lavori incompiuti sullo schermo ed evitare di lasciare aperta una sessione di lavoro dopo essersi identificati

Chiudete le applicazioni con cui state lavorando quando vi allontanate dal posto di lavoro: potreste rimanere lontani più del previsto, e una postazione aperta è vulnerabile a trattamenti non autorizzati.

Salvaschermo

Ogni postazione di lavoro deve avere il salvaschermo attivato, con richiesta di password per poter riprendere il controllo della postazione.

Non riutilizzare supporti rimovibili (CD, pen-drive ecc..) per affidare a terzi i vostri dati

Quando un file viene cancellato da un supporto magnetico, i dati non vengono effettivamente eliminati dal disco ma soltanto marcati come non utilizzati e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei dati dai dischi. Solo l'uso di un apposito programma di cancellazione sicura garantisce che sul dischetto non resti traccia dei dati precedenti. Se ciò non è possibile, essi devono essere distrutti e comunque è sempre meglio usare un dischetto nuovo.

Prestare particolare attenzione all'utilizzo dei computer portatili

I PC portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile, proteggetelo con una password sul BIOS, fate installare un programma di cifratura del disco rigido (per impedire la lettura dei dati in caso di furto) ed **effettuate periodicamente il backup**. Per garantire la sicurezza dei sistemi e lo sfruttamento delle funzionalità, i PC portatili aziendali devono essere collegati regolarmente (almeno ogni 30 gg.) alla rete RUG per gli aggiornamenti periodici. Questo processo è essenziale per garantire che i dispositivi siano costantemente allineati agli standard di sicurezza e alle più recenti migliorie tecnologiche.

Fare attenzione a non essere spiati mentre si digita una password o qualunque codice di accesso

Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate una password questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura. Chiedete agli astanti di guardare da un'altra parte quando introducete una password o controllate che nessuno stia guardando.

Proteggere il proprio computer con una password. Abilitare ove possibile l'accesso tramite password

La maggior parte dei computer offre la possibilità di impostare una password all'accensione. Anche alcuni applicativi permettono di proteggere i propri dati tramite password. Imparate a utilizzare queste caratteristiche che offrono un buon livello di riservatezza.

Non permettere l'uso del proprio computer o del proprio account da personale esterno, a meno di non essere sicuri della loro identità. Personale esterno può avere bisogno di installare del nuovo software/hardware nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro PC.

Non utilizzare apparecchiature non autorizzate o per cui non si è autorizzati

L'utilizzo di modem su postazioni di lavoro collegate alla rete di ufficio offre una porta d'accesso dall'esterno non solo al vostro computer ma a tutta la rete di cui fate parte. *E' quindi **vietato** l'uso di modem all'interno della rete locale.* Nel caso che ciò sia strettamente necessario, disconnettere fisicamente la postazione di lavoro dalla rete locale prima di effettuare il collegamento via modem. Per l'uso di altre apparecchiature, chiedere consiglio al Presidio CISIA competente.

Non installare programmi non autorizzati
Oltre alla possibilità di trasferire involontariamente un virus o di introdurre un cosiddetto "cavallo di troia", va ricordato che la maggior parte dei programmi sono protetti da copyright, per cui la loro installazione può essere illegale.

Diffidare dei dati o dei programmi la cui provenienza non è certa
Per proteggersi di virus ed altri agenti attivi di attacco, anche se la fonte appare affidabile o il contenuto molto interessante; molti sistemi di attacco inviano dati che sembrano provenire da un utente noto al destinatario per vincerne la naturale diffidenza nei confronti degli estranei.

Applicare con cura le linee guida per la prevenzione da infezioni da virus
La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore rispetto alla correzione degli effetti di un virus. Inoltre, se non avete attivato adeguate misure anti-virus potreste incorrere in una perdita irreparabile di dati o in un blocco anche molto prolungato della vostra postazione di lavoro.

Proteggere attentamente i dati
Bisogna prestare particolare attenzione ai dati di cui si è personalmente responsabili. Come minimo bisogna posizionarli in un'area protetta da password e non dare di default a nessun altro utente il permesso di lettura o modifica. Ai dati da condividere applicare i permessi opportuni solo per il tempo strettamente necessario all'interazione con gli altri utenti.
L'utilizzo dei dati personali deve avvenire in base al principio del *"need to Know":* non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento). I dati non devono essere comunicati all'esterno dell'Ufficio Giudiziario e comunque a soggetti terzi se non previa autorizzazione.

Usare, se possibile, il salvataggio automatico dei dati. Non dimenticare i salvataggi volontari
Molti applicativi, ad esempio quelli di videoscrittura, salvano automaticamente il lavoro a intervalli fissi, in modo da minimizzare il rischio di perdita accidentale dei dati. Imparate comunque a salvare manualmente il vostro lavoro con una certa frequenza, in modo da prendere l'abitudine di gestire voi stessi i dati e non fare esclusivo affidamento sul sistema.
La regola generale è quella di procedere al ***backup periodico dei dati*** *su supporti o su cartelle ospitate sui server, misure di sicurezza che devono essere eseguite da ogni utente, anche per evitare che la rottura o il malfunzionamento dell'hard disk comprometta il lavoro e causi la perdita dei dati.*

Utilizzo del PC
L'utente deve attenersi scrupolosamente all'utilizzo del PC solo ed esclusivamente per attività di Ufficio, ed è fatto divieto, salvo operazioni semplici (p.e., sostituzione di mouse, di tastiera) che non possano compromettere la funzionalità del PC, assumere iniziative personali per porre rimedio ad eventuali problemi tecnici, in particolar modo di tipo hardware; in tale caso è consigliabile rivolgersi al proprio ufficio che curerà la pratica di assistenza (Ufficio per l'Innovazione del Distretto o Ufficio Economato/Beni Patrimoniali) e in caso di urgenza contattare il Presidio CISIA.
I dati personali conservati sui PC devono essere cancellati in modo sicuro (chiamare l'assistenza sistemistica per formattare i dischi) prima di destinare i PC ad usi diversi.

Amministrare correttamente le password
Con l'arruolamento delle postazioni di lavoro sul sistema nazionale ADN vengono utilizzate dei criteri e policy di sicurezza più rigidi. In particolare se l'utente inserisce erroneamente per tre volte consecutive le proprie credenziali l'account viene bloccato per un certo lasso di tempo ed inoltre la password ha una durata 90 gg. Per quanto riguarda la composizione della password si indica il link del GPDP (Garante per la Protezione dei dati personali) dove è possibile trovare i consigli di base per impostare

pw sicure e gestirle in modo accorto https://www.gpdp.it/temi/cybersecurity/password . Per la configurazione e per adeguare la sicurezza del software di base valgono le Linee Guida **AGID 2020:**

- devono essere composte da almeno otto caratteri in funzione delle criticità delle informazioni da difendere (es. 15 caratteri per utenze amministrative);
- devono contenere almeno tre tipi diversi di caratteri inclusi tra quelli maiuscoli, minuscoli, cifre e simboli di interpunzione;
- non devono essere parole presenti in dizionari delle lingue più diffuse;
- non devono essere basate su parole dialettali o gergali;
- non devono essere basate su informazioni personali come data di nascita, numeri di telefono, indirizzi;
- non devono essere basate su informazioni personali di familiari, amici, colleghi, attori, personaggi famosi, ecc.;
- non devono essere termini tecnici o informatici, comandi, siti, società. ecc.;
- non devono essere del tipo aaabbb, 123456, fedcba, o simili;
- non devono essere password dei tipi elencati in precedenza scritte al contrario;
- non devono essere basate su password analoghe alle precedenti con l'aggiunta di cifre prima o dopo.

Tutti gli utenti, infine, debbono attenersi scrupolosamente alle seguenti prescrizioni:

- non rivelare le password a nessuno, inclusi amici e familiari;
- non condividere le password con altri colleghi o assistenti, salvo quanto disposto a proposito dell'utilizzo del programma "SCRIPT@";
- non inviare le password tramite e-mail o altri metodi di comunicazione elettronica, né tramite telefono;
- non mostrare a video le password (ma neanche PIN, passphrase, ecc.., in generale: chiavi segrete) quando viene inserita e non dare indicazioni sulla sua lunghezza;
- cambiare obbligatoriamente al primo log-on la password temporanea;
- non scrivere le password su carta o biglietti e non memorizzare le password su file o altri sistemi (palmari o agende elettroniche) senza cifratura;
- non scrivere la propria password su questionari o presunti moduli di sicurezza;
- non parlare della propria password o rivelare indizi su essa;
- non utilizzare sistemi informatici che permettono di memorizzare le password o gestire un database di password;
- non riutilizzare in nessun caso le password già utilizzate in precedenza.

Non violare le leggi in materia di sicurezza informatica.

Ricordatevi che anche solo un tentativo di ingresso non autorizzato in un sistema costituisce un reato. Se siete interessati a studiare la sicurezza della vostra postazione di lavoro o della rete di cui fate parte, chiedete preventivamente l'autorizzazione al Referente locale della sicurezza del singolo Ufficio. Non utilizzate senza autorizzazione software che possa creare problemi di sicurezza o danneggiare la rete, come port scanner, security scanner, network monitor, network flooder, fabbriche di virus o di worm.

Segnalare tempestivamente qualsiasi variazione del comportamento della propria postazione di lavoro

Può essere il sintomo di un attacco in corso.

Segnalare comportamenti che possano far pensare a tentativi di ridurre la sicurezza del sistema informativo

Ad esempio segnalate al Responsabile della sicurezza dell'Ufficio se un altro utente insiste per avere accesso ai vostri dati o per conoscere la vostra password o per poter lavorare sulla vostra postazione di lavoro. Analogamente non fidatevi e segnalate telefonate o messaggi che sembrano provenire da

un sistema e vi chiedono di fare operazioni strane sul vostro computer (ad esempio, cambiare subito la password con una datavi al telefono o nel corpo del messaggio).
Si fa presente che per ogni ulteriore informazione sulle modalità di comportamento da tenere sul luogo di lavoro è necessario far riferimento al responsabile o al titolare del trattamento dei dati.

PRESCRIZIONI PARTICOLARMENTE IMPORTANTI
VIRUS E MISURE ANTIVIRUS

Gli utenti devono:

- usare soltanto programmi provenienti da fonti fidate perché copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato;
- assicurarsi di non far partire accidentalmente il computer da supporto esterno e, se possibile, impostare il BIOS in modo da avere come *primary boot device* il disco rigido e proteggere l'accesso al BIOS tramite password. Se il supporto fosse infetto, il virus potrebbe trasferirsi nella memoria RAM ed infettare altri file;
- proteggere i supporti da scrittura quando possibile. È il più efficace mezzo di prevenzione, infatti i virus non possono rimuovere la protezione meccanica;
- salvare o sottoporre a backup i dati importanti per evitare di perderli in caso di infezione.

Gli utenti non devono:

- aprire mail di provenienza sospetta e, in generale, non aprire nessun allegato senza una preventiva scansione anti-virus;
- visitare siti illegali, usati come specchietto per le allodole per attirare visitatori su cui condurre attacchi;
- modificare le configurazioni del software antivirus.

POSTA ELETTRONICA

Gli utenti devono:

- Prestare la massima attenzione nella apertura dei file allegati a messaggi di posta elettronica certificata, ivi compresi quelli ricevuti mediante il protocollo documentale, perché potrebbero contenere allegati malevoli;
- usare solo il software di posta approvato dal Ministero della Giustizia;
- effettuare la scansione con programmi di controllo antivirus approvati dal Ministero dei messaggi in ingresso per evitare virus o contenuti maligni;
- impedire ad altre persone di utilizzare il proprio account per inviare posta elettronica;
- trasmettere dati confidenziali solo se adeguatamente cifrati (standard S/MIME);
- trasmettere di preferenza messaggi con firma digitale (standard S/MIME con firma di tipo deatched), per garantire al destinatario l'origine del messaggio; si noti che questa tecnica, pur basandosi sui medesimi principi della firma digitale usata per la sottoscrizione di documenti elettronici con valore legale, è fondamentalmente diversa e viene usata nello standard S/MIME per garantire l'autenticità dei messaggi di posta elettronica ed evitare quindi la generazione di messaggi falsi ("fake mail") che potrebbero indurre in errore utenti inesperti;

gli utenti non devono:

- utilizzare la posta elettronica per scopi in conflitto con il piano di sicurezza ed in ogni caso non utilizzarla eccessivamente per scopi personali;
- partecipare alle cosiddette "Catene di Sant'Antonio" o, in generale, non utilizzare la posta elettronica per spamming;
- inviare mai informazioni confidenziali tramite posta elettronica non cifrata;
- aprire posta elettronica di provenienza dubbia, accertarsi sempre della provenienza dei messaggi di posta elettronica contenente allegati, nel caso che il mittente dia origine a dubbi, cancellare direttamente il messaggio senza aprire gli allegati. Per una corretta ed approfondita analisi della presunta e-mail malevola, inoltrare il messaggio all'indirizzo antispam.dgsia@giustizia.it

INTERNET

- Evitare l'accesso a siti in contrasto con il profilo etico specifico della nostra organizzazione o che possono costituire motivo di distrazione nell'espletamento dell'attività lavorativa;
- Salvaguardare la rete geografica da un uso eccessivo e non legato ad esigenze lavorative del servizio di navigazione Internet.

TRATTAMENTO DATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

CAUTELE GENERALI

Chiudere a chiave armadi/cassetti ed uffici

Il primo livello di protezione di qualunque sistema è quello fisico. E' certamente vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania o visibili su uno schermo. Pertanto, chiudete a chiave il vostro ufficio alla fine della giornata ed ogni volta che vi assentate. Inoltre chiudete i documenti a chiave nei cassetti ogni volta che potete. I documenti contenenti dati personali non devono in alcun modo rimanere incustoditi e a fine giornata devono essere riposti in armadi /cassetti chiusi a chiave in modo da non essere accessibili a persone non autorizzate.

Conservare supporti di memoria e stampe in luoghi sicuri

Alla conservazione dei supporti di memoria (CD, pen-drive....) si applicano gli stessi criteri di protezione dei documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. A meno che non siate sicuri che contengano solo informazioni non sensibili, riponeteli sotto chiave non appena avete finito di usarli.

Maneggiare e custodire con cura le stampe di materiale riservato

Non lasciate accedere alle stampe persone non autorizzate. Se la stampante non si trova sulla vostra scrivania recatevi il più in fretta possibile a ritirare le stampe. Per stampe riservate cercate di usare una stampante non condivisa oppure usate la modalità di stampa ritardata impostando un tempo sufficiente a permettervi di raggiungere la stampante prima dell'inizio della stampa. Distruggete personalmente le stampe quando non servono più.

Non gettare nel cestino le stampe di documenti che possono contenere informazioni confidenziali.

Se trattate dati di particolare riservatezza, considerate la possibilità di dotarvi di una distruggi-documenti (shredder); in ogni caso non gettate mai documenti cartacei senza averli prima sminuzzati in modo da non essere ricomponibili.

Sanzioni per inosservanza delle norme

Le presenti istruzioni integrano elementi di valutazione della condotta del lavoratore.
La violazione delle prescrizioni contenute può generare, oltre che responsabilità penali e civili, l'irrogazione di sanzioni disciplinari, in considerazione della gravità della condotta.

Il Dirigente Amministrativo
- dott.ssa Francesca Del Grosso -

La Presidente f.f.
- dott.ssa Ornella Crespi -

NUMERI DI ASSISTENZA AGLI APPLICATIVI MINISTERIALI

(sw nazionali approvati dal Responsabile dei Sistemi Informativi Automatizzati, ai sensi dell'art. 12 dell'allegato al D.M. 27 aprile 2009):

Servizio di Help Desk per la Conduzione dei Sistemi ed uniche modalità di contatto per il servizio di Assistenza Applicativa dal 2 aprile 2024

Per ogni problematica (guasti hardware, alla rete locale e rete geografica, per attività di system management e per applicativi area penale, civile e TIME MANAGEMENT, per servizi di Interoperabilità (posta elettronica, posta elettronica certificata ed Internet) è possibile aprire in autonomia un ticket al numero verde 800749049, comunicando nominativo e PIN attribuito al momento della registrazione in ADN, o collegandosi con le proprie credenziali ADN al portale web https://helpdesk.giustizia.it/. In caso di smarrimento, è possibile recuperare il PIN rivolgendosi al referente GSI/IAA/MultiUX dell'Ufficio.

Il nuovo portale https://helpdesk.giustizia.it consente di segnalare la problematica in completa autonomia, anche al di fuori dell'orario di servizio dell'Help Desk.
Principali funzionalità utili

- **monitoraggio in tempo reale dello stato di avanzamento di tutti i ticket associati all'utente, a prescindere dal canale di apertura;**
- **una sezione di Knowledge Base in continua crescita, che si arricchirà di contenuti informativi sempre a disposizione dell'utente per facilitare la risoluzione in autonomia delle problematiche più comuni;**
- **catalogo dei servizi per facilitare le richieste all'Help Desk;**
- **possibilità di scambiare messaggi con l'operatore dal portale;**
- **possibilità di valutare il servizio ricevuto e fornire suggerimenti per il continuo miglioramento del servizio stesso.**

Oltre al portale, si rammenta che per l'apertura dei ticket è disponibile anche il numero verde 800.749.049 disponibile dalle ore 08:00 alle ore 18:00 dal lunedì al venerdì e dalle ore 08:00 alle ore 13:00 del sabato.

Se si chiama da un numero telefonico dell'Amministrazione, dopo aver selezionato il tasto 1 l'utente sarà automaticamente messo in contatto con il primo operatore libero all'utente associato.