ISTITUTO NAZIONALE DI GEOFISICA E VULCANOLOGIA

il Direttore

Gestione WEB

Ai Direttori dei Dipartimenti
Ai Direttori delle Sezioni
Al Direttore della Direzione Centrale Affari Generali e Bilancio
Al Centro Servizi per il coordinamento delle attività a supporto della Ricerca
Al Centro Servizi Informativi
Alle OO.SS.
Al CUG

Oggetto: Pubblicità atti

Si notifica in copia l'allegato Decreto del Presidente n. 12 del 29/01/2019 concernente: Emanazione Regolamento Informatico.

Tullio PEPE

DIREZIONE CENTRALE
AFFARI AMMINISTRATIVI
E DEL PERSONALE

Via di Vigna Murata, 605 | 00143 Roma| Italia | Tel.: +39 39.0651860803 | Fax: +39.0651860576
direzione.centrale1@ingv.it | aoo.roma@pec.ingv.it | www.ingv.it

Decreto n. 12
OGGETTO: emanazione Regolamento Informatico.

IL PRESIDENTE

- Visto il Decreto legislativo 29 settembre 1999, n. 381, costitutivo dell'Istituto Nazionale di Geofisica e Vulcanologia (INGV);
- visto il Decreto legislativo 25 novembre 2016, n. 218, recante "Semplificazione delle attività degli Enti Pubblici di Ricerca ai sensi dell'art. 13 della Legge 7 agosto 2015, n. 124";
- visto lo Statuto dell'INGV, approvato con Delibera del Consiglio di Amministrazione n. 372/2017 del 9 giugno 2017, come modificata con Delibera del Consiglio di Amministrazione n. 424/2017 del 15 settembre 2017, e pubblicato sul Sito WEB istituzionale (Avviso di emanazione pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana - Serie generale - n. 27 del 2 febbraio 2018);
- visto il Regolamento di Organizzazione e Funzionamento dell'INGV, emanato con Decreto del Presidente n. 45/2018 del 21/2/2018, pubblicato sul Sito WEB istituzionale;
- visto il Decreto del Ministro dell'Istruzione, Università e Ricerca n. 286/2016 del 27/4/2016, con il quale il Prof. Carlo DOGLIONI è stato nominato Presidente dell'INGV;
- in relazione alla necessità di munire l'INGV di un regolamento informatico che, recependo le novelle normative intervenute negli ultimi anni a disciplinare la materia, sostituisca tutte le direttive attualmente vigenti nel settore;
- visto l'art. 15 della Costituzione Repubblica Italiana, il quale sancisce che *"La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge"*;
- vista la Legge 20 maggio 1970, n. 300 *"Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento"* (Statuto dei Lavoratori);
- visto il Decreto Legislativo n. 518/92, concernente la Normativa in materia di protezione del software introdotta, quale "Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratori", che ha provveduto ad aggiungere l'art. 171-bis, avente ad oggetto la tutela di programmi per elaboratori, all'art. 171 della Legge n. 633/1941;

- visto il Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";
- visto il Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati - GDPR) e recepito con Decreto Legislativo 101/2018;
- vista la Circolare Agenzia per l'Italia Digitale 18 aprile 2017, n. 2/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015)" e ss.mm.ii;
- visto il Codice dell'Amministrazione Digitale D.Lgs. n. 82/2005 - CAD e successive modificazioni ed integrazioni D.lgs. 13 dicembre 2017, n. 217;
- vista la Delibera del Consiglio di Amministrazione n. 745/2018 del 20/12/2018, con la quale è stato approvato lo schema di nuovo regolamento informatico dell'Istituto,

DECRETA

È emanato il Regolamento Informatico dell'INGV allegato al Presente decreto del quale costituisce parte integrante e sostanziale.

Il Regolamento entrerà in vigore il giorno successivo a quello della sua pubblicazione sul Sito WEB istituzionale.

Roma, 29 GEN. 2019

Prof. Carlo DOGLIONI

1. INTRODUZIONE

L'Istituto Nazionale di Geofisica e Vulcanologia, di seguito INGV, mette a disposizione del proprio personale e di eventuali collaboratori esterni i seguenti strumenti di lavoro, in funzione del loro ruolo e delle esigenze lavorative:

1. Strumenti di informatica individuale, quali personal computer e relativi accessori.
2. Apparati e servizi condivisi, quali ad esempio, posta elettronica, internet, stampanti di rete, file server ecc.
3. Programmi di produttività individuale, programmi specialistici e procedure gestionali.
4. Sistemi di calcolo.
5. Sistemi di calcolo per i servizi amministrativi, come Protocollo Informatico, Workflow, ecc.

Tali risorse costituiscono strumenti di lavoro e devono essere utilizzati, di norma, per il perseguimento di fini strettamente connessi agli incarichi lavorativi secondo criteri di massima correttezza e professionalità, coerentemente al tipo di attività svolta ed in linea con le disposizioni normative vigenti. Il documento illustra le norme generali di utilizzo di tali risorse che il personale e i collaboratori devono rispettare al fine di mitigare i rischi che un uso improprio degli stessi può determinare alla sicurezza del patrimonio informativo e all'immagine dell'Ente nonché l'ambito di eventuali verifiche effettuate dal personale addetto riguardo alla funzionalità e sicurezza dei sistemi informatici in dotazione. In particolare si evidenzia come l'utilizzo delle risorse informatiche per scopi non inerenti all'attività lavorativa possa contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza delle infrastrutture dell'ente.
L'INGV, aderendo all'associazione Consortium GARR - Rete italiana dell'Università e della Ricerca, garantisce l'osservanza delle regole dettate dal Consortium GARR, ACCEPTABLE USE POLICY - AUP.
Nella definizione delle norme comportamentali da osservare si è tenuto conto di quanto previsto dalla normativa vigente in materia, dal decreto legislativo 13 dicembre 2017 n. 217 e ss.mm.ii. (CAD) e, in particolare, dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR) e dal Decreto Legislativo 10 agosto 2018, n. 101 che aggiorna al GDPR il precedente "Codice in materia di protezione dei dati personali" del 30 giugno 2003, n. 196 e dai provvedimenti emessi dall'Autorità Garante per la protezione dei dati personali. Tra questi rientrano le "Linee guida del Garante per posta elettronica e internet" emesse in data 1 marzo 2007.

L'INGV non effettua registrazioni per il controllo dell'attività lavorativa dei dipendenti, ma solo registrazioni volte a salvaguardare la sicurezza ed il mantenimento dell'efficienza dei sistemi. I dati registrati automaticamente a tale scopo non vengono utilizzati in alcun modo per il controllo a distanza dei lavoratori, se non è preventivamente richiesto dal datore di lavoro, e le tecnologie utilizzate a tal fine sono compatibili con quanto disposto dalla normativa vigente in materia come modificata dal Jobs Act (Decreto Legislativo n. 151 del 14 settembre 2015, recante «Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014 n. 183».) e secondo il principio che sono legittimi quei controlli diretti ad accertare comportamenti illeciti del lavoratore e lesivi del patrimonio aziendale (Cfr. Cass. n. 3122/2015 e Cass. n. 2722/2012). Il trattamento dei dati raccolti in relazione all'uso delle risorse di calcolo e dei servizi di rete avviene solo per finalità determinate, esplicite e legittime, nel rispetto dei principi di necessità, pertinenza, correttezza e non eccedenza. I sistemi informativi e i programmi informatici sono pertanto configurati in modo da ridurre al minimo l'utilizzo dei dati personali e identificativi, come gli istanti temporali di login, mac address, ip address utilizzati per accedere alle risorse di rete. In ogni caso, come previsto

dalla normativa europea in materia di trattamento dei dati personali e privacy, è disponibile il Registro del Trattamento dei Dati personali, che conterrà:

1. Il nome e i dati di contatto del titolare del trattamento e, se presente, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
2. Le finalità del trattamento;
3. La descrizione delle categorie di interessati e delle categorie di dati personali;
4. Le categorie di destinatari a cui i dati personali siano stati o saranno comunicati, compresi i destinatari di paesi terzi;
5. Se presenti, i trasferimenti di dati personali verso paesi terzi e la loro identificazione;
6. I termini ultimi previsti per la cancellazione delle diverse categorie di dati;
7. Una descrizione generale delle misure di sicurezza tecniche e organizzative.

2. CAMPO DI APPLICAZIONE

Il presente Regolamento si applica a tutti coloro cui sia stato consentito l'accesso alle risorse di calcolo ed ai servizi di rete e più in generale all'infrastruttura informatica dell'INGV.

3. GLOSSARIO E FIGURE PROFESSIONALI

1. **"Utente"**: Qualsiasi soggetto che sia stato autorizzato ad utilizzare le risorse informatiche e di rete dell'INGV in relazione alle funzioni ed attività che svolge.
2. **"Amministratore di sistema"**: Ogni figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente regolamento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi. Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati, come richiesto da Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008:
    a. La figura fu definita inizialmente dal Codice del 2003 come "soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione" (art. 1, comma 1, lett. c) d.P.R. 318/1999) successivamente nel Provvedimento del Garante del 27 novembre 2008 come "una figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali". La figura è completata nel GDPR, come un addetto/incaricato al trattamento ex art. 29, e contribuisce, secondo l'art. 32 par. 1, a che il Titolare del trattamento

ST QV

possa mettere in atto misure tecniche e organizzative per "garantire un livello di sicurezza adeguato al rischio" ed è conscio delle prescrizioni poste dal garante della privacy con "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".

3. "**Amministratore di Rete**": Dipendente INGV incaricato di gestire specifici apparati di rete (LAN e/o WAN) o sottosistemi di interconnessione fra risorse informatiche dell'INGV. L'Amministratore di Rete si impegna a mettere in atto le azioni necessarie all'osservanza del presente regolamento e della normativa vigente in materia di dati personali; inoltre, di concerto con il Centro Servizi Informativi, definisce, implementa e verifica le politiche di accesso alle strutture di rete da lui gestite.
4. **"Centro Servizi Informativi (CSI)"**: Nell'ambito del presente Regolamento è la Struttura posta alle dirette dipendenze del Direttore Generale ed incaricata di coordinare ed organizzare le attività informatiche dell'INGV, ottimizzare l'uso e la disponibilità delle risorse e garantire adeguati livelli di sicurezza. Il CSI gestisce in modo diretto le attività delle sezioni romane e le loro sedi collegate e coordina la gestione delle risorse informatiche delle sezioni esterne attraverso i referenti appositamente designati dai Direttori di Sezione (uno per ciascuna sezione), che si riuniranno in "assemblea CSI".
5. **"Delegati"**: Dipendenti o altra tipologia di personale (Consulenti, fornitori ecc.) che possono essere delegati dai Centro Servizi Informativi per specifiche attività, compiti o per la gestione di determinate risorse, spesso rientrano nella definizione di amministratore di sistema.
6. **"Responsabile della protezione dei dati (DPO)"**: il DPO è un supervisore indipendente, designato obbligatoriamente da soggetti apicali di tutte le pubbliche amministrazioni, con gli obiettivi di informare e fornire consulenza a titolare e al responsabile del trattamento nonché ai dipendenti degli obblighi derivanti dal regolamento, sorvegliare l'osservanza del regolamento, nonché delle altre disposizioni europee o di diritto interno in materia di protezione dati, sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e attività di controllo, fornire pareri e sorvegliare alla redazione della Data protection impact assessment (c.d. Dpia), fungere da punto di contatto e collaborare con l'Autorità Garante per la protezione dei dati personali, controllare che le violazioni dei dati personali siano documentate, notificate e comunicate (c.d. Data Breach Notification Management).

4. NORMATIVA DI RIFERIMENTO

Il presente Disciplinare Interno è redatto in conformità alla normativa vigente, di seguito riportata per riferimento:

1. Costituzione della Repubblica Italiana, art. 15 sancisce che "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro

limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge".

2. Legge 20 maggio 1970, n. 300 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento" (Statuto dei Lavoratori).
3. Normativa in materia di diritto d'autore e di altri diritti connessi al suo esercizio introdotta con la Legge n.633/41 per la protezione delle opere dell'ingegno di carattere creativo qualunque ne sia il modo o la forma di espressione.
4. Normativa in materia di protezione del software introdotta con il D.lgs. n.518/92 "Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratori"; tale provvedimento normativo ha infatti aggiunto l'art. 171-bis, avente ad oggetto la tutela di programmi per elaboratori, all'art.171 della Legge n° 633/1941. L'art. 171-bis, il cui testo è stato ultimamente modificato dalla L. n°248/2000 "Nuove norme di tutela del diritto d'autore", prevede sanzioni penali a carico di coloro che duplicano, detengono, distribuiscono o vendono programmi per elaboratore oggetto di copyright; pertanto la norma pone il divieto assoluto di fare copie illegali di materiale protetto da leggi a tutela del diritto d'autore e di rendere tale materiale disponibile a terzi per effettuare delle copie.
5. Codice Penale art. 616 - Violazione, sottrazione e soppressione di corrispondenza – "Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prendere o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da lire sessantamila a un milione. Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni. Il delitto è punibile a querela della persona offesa. Agli effetti delle disposizioni di questa sezione, per «corrispondenza» si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza.
6. Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati - GDPR).
7. Decreto Legislativo 30 giugno 2003, n°. 196 "Codice in materia di protezione dei dati personali", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali e della dignità dei soggetti a cui si riferiscono i dati, imponendo l'adozione di misure di sicurezza che riducono il rischio informatico e consentano un efficace controllo sull'utilizzo e la conservazione dei dati. Il decreto prevede un livello minimo di sicurezza per i dati personali definendo le misure fisiche, logiche e organizzative che devono essere adottate al fine di: evitare possibili distruzioni, perdite, alterazioni di dati; garantire che l'accesso ai dati sia effettuato dalle

sole persone incaricate al trattamento e quindi autorizzate; garantire che il trattamento avvenga per le finalità e nelle modalità consentite.

8. Circolare Agenzia per l'Italia Digitale 18 aprile 2017, n.2/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)" e ss.mm.ii.
9. Le misure di sicurezza sono applicate garantendo il rispetto di quanto disposto dalle "Linee guida del Garante per posta elettronica e internet" emesse dall'Autorità Garante per la protezione dei dati personali il 1 marzo 2007 e suoi interventi successivi.
10. Codice dell'Amministrazione Digitale d.l.vo n. 82/2005 – CAD e successive modificazioni ed integrazioni d.l.vo 13 dicembre 2017 n. 217.
11. Per quanto non presente si rimanda alla normativa di riferimento.

5. UTILIZZO DELLE POSTAZIONI DI LAVORO

Le risorse informatiche, in quanto essenziali per l'INGV, sono rese disponibili esclusivamente per il conseguimento delle finalità istituzionali dell'Ente.
Gli utenti sono tenuti a servirsi delle risorse informatiche dell'Ente prestando il proprio contributo affinché ne sia preservata l'integrità e garantito il buon funzionamento.

Sono pertanto vietate:

1. Attività contrarie alla legge nazionale, comunitaria e internazionale o proibite dai regolamenti e dalle consuetudini d'uso delle reti e dei servizi acceduti.
2. Attività commerciali, o comunque lucrative, non autorizzate, nonché la trasmissione di materiale commerciale e/o pubblicitario non richiesto (spamming) o l'uso delle proprie risorse da parte di terzi per tali attività.
3. Attività comunque idonee a danneggiare, distruggere, compromettere la sicurezza delle risorse informatiche dell'Ente o dirette a violare la riservatezza e/o cagionare danno a terzi, ivi inclusa la creazione, trasmissione e conservazione di immagini, dati o altro materiale offensivo, diffamatorio, osceno, indecente o che attenti alla dignità umana, specialmente se riguardante il sesso, la razza, la religione, le opinioni politiche o la condizione personale o sociale.
4. Utilizzo di software o file, coperti da copyright, senza licenza alcuna.
5. Attività comunque non conformi ai fini istituzionali dell'Ente.

6. REGOLE DI UTILIZZO DELLE RISORSE INFORMATICHE

I calcolatori elettronici in uso presso l'INGV possono essere distinti in apparecchiature per prevalente uso tecnico-scientifico (categoria TS) ed apparecchiature dedicate prevalentemente ad uso amministrativo e ai servizi di sorveglianza (categoria AS). Le postazioni di lavoro, normalmente, sono connesse alla rete interna della sede con lo scopo di usufruire dei servizi dell'Ente, accedere alle applicazioni software gestite da Centro Servizi Informativi, condividere informazioni, fruire i contenuti della Intranet e di Internet.

Al fine di garantire la sicurezza delle risorse di calcolo e dei servizi di rete è vietato:

1. Connettere risorse di calcolo alla rete locale o ad altri servizi che includono la connettività di rete senza l'autorizzazione del CSI.

2. Cablare, collegare o modificare apparati di rete (access point, router, print server, modem, etc.) senza l'autorizzazione del CSI.
3. Utilizzare indirizzi di rete e nomi non espressamente assegnati.
4. Installare sistemi, hardware o software, che consentano accesso alle risorse informatiche senza l'autorizzazione del CSI.
5. Fornire accesso alle risorse informatiche a soggetti non espressamente autorizzati.
6. Divulgare informazioni sulla struttura e configurazione delle risorse informatiche, con particolare riferimento a quelle che consentono accesso da remoto.
7. Accedere senza autorizzazione ai locali dei CED, nonché ai locali ed alle aree riservate alle apparecchiature di rete.
8. Intraprendere ogni altra azione diretta a degradare le risorse del sistema, impedire ai soggetti autorizzati l'accesso alle risorse, ottenere risorse superiori a quelle autorizzate o accedere alle risorse di calcolo violando le misure di sicurezza.

Gli Utenti inoltre:

1. Sono tenuti ad agire in conformità alla legge e nel rispetto delle indicazioni del Servizio di Calcolo e Reti in materia di sicurezza, garantendo la riservatezza nel trattamento dei dati personali, anche mediante la puntuale osservanza delle norme dettate dall'INGV in materia e accessibili presso la seguente pagina web: www.ingv.it.
2. Nella scelta e nell'acquisto degli strumenti informatici di cui si servono, devono tenere in opportuna considerazione le indicazioni del CSI, in particolare per quanto riguarda le caratteristiche relative alla sicurezza, privilegiando i sistemi e le procedure che offrono i livelli più elevati di protezione.
3. Sono responsabili dei dati e del software installato sui computer loro affidati: procedono ad una loro attenta valutazione preliminare e non installano software privi delle regolari licenze;
4. Sono tenuti a proteggere da accessi non autorizzati i dati utilizzati e/o memorizzati nei propri computer e nei sistemi cui hanno accesso.
5. Valutano attentamente l'affidabilità dei servizi esterni eventualmente utilizzati, ivi inclusi quelli di tipo cloud, in termini di sicurezza, conservazione e confidenzialità dei dati.
6. Sono tenuti a seguire le indicazioni del CSI per il salvataggio periodico dei dati e programmi utilizzati.
7. Il salvataggio (backup) dei dati necessari all'attività lavorativa per le postazioni che non memorizzano i propri dati su un file server centrale è di esclusiva responsabilità dell'utente.
8. Sono tenuti a proteggere il proprio account mediante password non banali e, qualora siano presenti più sistemi di autenticazione, differenti per ogni sistema, adottando, ove possibile, sistemi di autenticazione in più fattori.
9. Non devono diffondere né comunicare la propria password, ovvero concedere ad altri l'uso del proprio account privilegiando metodo di archiviazione sicuri.
10. Sono tenuti a segnalare immediatamente al proprio Dirigente e al CSI incidenti, sospetti abusi e violazioni della sicurezza.
11. Per i sistemi operativi che lo prevedono, devono utilizzare programmi antivirus aggiornati, avendo cura di sottoporre a scansione antivirus file e programmi scambiati via rete e i supporti rimovibili utilizzati.
12. Non devono mantenere connessioni remote non utilizzate né lasciare la postazione di lavoro con connessioni aperte non protette, soprattutto in caso di accesso in VPN.

Per le postazioni di lavoro in categoria TS il ricercatore/tecnologo a cui la postazione è assegnata e limitatamente a tale postazione è considerato amministratore di sistema.

Tutti coloro che trattano dati "sensibili", in quanto RUP di gare, gestori di procedure concorsuali, ecc. in caso di necessità di archiviazione di documenti contenenti dati sensibili su supporti rimovibili o su servizi di rete non gestiti dall'INGV (ad esempio servizi cloud) sono tenuti ad adottare adeguate misure di protezione con sistemi di crittografia.
Per le postazioni di lavoro in categoria AS la modifica delle configurazioni software impostate sulla propria o altrui postazione di lavoro, è consentita esclusivamente al personale CSI e agli Amministratori di Sistema: l'utente può eventualmente procedere ad eventuali modifiche solo dopo aver avuto esplicita autorizzazione a farlo.
In caso di smarrimento o furto di dispositivi informatici, oltre a sporgere regolare denuncia all'autorità competente, informare tempestivamente i Centro Servizi Informativi comunicando quali dati erano contenuti all'interno.

Infine:

1. Al termine del lavoro deve essere correttamente chiusa la sessione e devono essere spenti i computer, video ed accessori non utilizzati, fatto salvo i casi in cui i calcolatori siano impegnati in elaborazioni.
2. Costituisce buona prassi effettuare con cadenza periodica (almeno ogni sei mesi) la pulizia degli archivi presenti sulla propria postazione e nelle cartelle di rete di propria competenza, con cancellazione dei file inutili o obsoleti. Si deve porre particolare attenzione ad evitare un'archiviazione ridondante con duplicazione dei dati.
3. La tutela della gestione locale dei dati presenti sulle stazioni di lavoro personali (personal computer) è demandata all'utente finale che dovrà effettuare, con frequenza opportuna, salvataggio su supporti di rete o sistemi di archiviazione esterna.
4. Nel caso in cui esista la necessità di elaborare banche dati in locale, ad esempio su fogli di calcolo o database personali, è necessario adottare le misure di sicurezza idonee a garantire il rispetto della normativa in materia di tutela dei dati personali, concordando con CSI tecniche e modalità.
5. L'utente è responsabile delle attrezzature che gli sono affidate in uso e pertanto deve provvedere a mantenerle in completa efficienza, anche della manutenzione hardware nel caso di rottura di componenti, gestendo la garanzia della sua macchina, segnalando tempestivamente ai Centro Servizi Informativi ogni eventuale problema tecnico e, in caso di dubbio, sulla sicurezza della postazione di lavoro. Le suddette norme comportamentali devono essere osservate anche nei casi di utilizzo di risorse informatiche non fornite direttamente dai Centro Servizi Informativi, ma acquisite a vario titolo nel corso del tempo.
6. Per scopi organizzativi o di progetto alcuni utenti possono ricevere l'incarico di amministratore di sistema di server o servizi specifici, questi utenti sono delegati dal CSI a compiere le normali attività di amministrazione e manutenzione sulla risorsa. L'utente nominato amministratore di sistema diventa responsabile della risorsa informatica e si impegna a rispettare con particolare attenzione le misure minime di sicurezza, i regolamenti e seguire i manuali operativi di sicurezza e gestione delle risorse emanati dal CSI adoperandosi per mantenere gli standard di qualità della risorsa informatica. L'amministratore di sistema in particolar modo presta attenzione alle attività di aggiornamento del sistema operativo e dei programmi in presenza di problemi di sicurezza, collaborando durante i periodici audit di sicurezza e vulnerabilità con il CSI e i suoi delegati.
7. Ai soli fini di prestare assistenza tecnica informatica ai lavoratori, l'Ente può utilizzare alcuni software che permettono all'amministratore di sistema di vedere in tempo reale le attività svolte dal lavoratore all'interno della propria sessione di lavoro ed eventualmente di intervenire attivamente. L'attivazione di tale funzionalità può essere richiesta solamente da parte degli

amministratori di sistema e solo quando strettamente necessario per poter svolgere l'attività di assistenza tecnica informatica e deve essere sottoposta ad un preventivo e contestuale consenso da parte del lavoratore.

7. COMPITI DEL CENTRO SERVIZI INFORMATIVI

Il Centro Servizi Informativi, oltre ai compiti indicati nei decreti e regolamenti di Istituto, ad esclusione dei servizi di Help Desk per le singole utenze, al fine di mantenere il più elevato livello di sicurezza all'interno delle reti locali, in relazione all'evoluzione tecnologica del settore:

1. Rilascia le credenziali per l'accesso alle risorse informatiche di Istituto, provvedendo alla rigenerazione delle credenziali scadute o dimenticate, alla disattivazione delle credenziali relative ad utenze cessate, ecc.
2. Controlla che gli accessi remoti alle risorse locali avvengano esclusivamente mediante l'uso di protocolli che prevedano l'autenticazione e la cifratura dei dati trasmessi, ad esempio VPN client-to-site.
3. Limita l'uso interno di servizi e programmi che trasmettono in chiaro le password.
4. Sulle macchine gestite, provvede a disattivare i servizi non essenziali ed a limitare il numero degli utenti privilegiati a quello strettamente necessario per le attività di coordinamento, controllo e monitoraggio della rete e dei servizi ad essa afferenti.
5. Effettua la revisione, almeno annuale, degli account.
6. Effettua il monitoraggio dei sistemi gestiti, registrando gli accessi privilegiati, eventuali modifiche ai file di sistema e l'uso non autorizzato dei servizi di rete.
7. Realizza i sistemi di filtraggio e logging sugli apparati perimetrali della rete.
8. Fornisce supporto per conservare e incrementare la sicurezza delle risorse affidate agli utenti.

Le credenziali identificano l'utente in modo univoco e sono strettamente personali. L'utente è tenuto a conservarle garantendone la segretezza, ed a comunicare immediatamente al Centro Servizi Informativi ogni circostanza che possa anche solo potenzialmente compromettere la sicurezza.

8. USO DELLA POSTA ELETTRONICA

Principi generali

L'Istituto Nazionale di Geofisica e Vulcanologia fornisce un servizio di posta elettronica, mettendo a disposizione indirizzi con estensione @ingv.it. Gli indirizzi possono essere individuali ovvero di gruppo. Gli indirizzi individuali sono in uso ad una singola persona, mentre gli indirizzi di gruppo sono destinati allo svolgimento di attività o servizi istituzionali e sono condivisi fra tutto il personale coinvolto nelle attività connesse, individuando uno o più utenti con il ruolo di "gestore" del gruppo, al fine di gestire le afferenze alla lista ed i ruoli.

Hanno diritto ad un indirizzo di posta elettronica individuale i dipendenti ed i titolari di assegni di ricerca, purché diretti dipendenti dell'Istituto. Negli altri casi si adotta la politica di creare

alias che puntino ad indirizzi di posta elettronica "personali" o della realtà lavorativa di provenienza.

Il servizio di posta elettronica è uno strumento di lavoro e deve essere utilizzato per lo svolgimento di attività connesse agli incarichi lavorativi e/o istituzionali.

Il servizio di posta elettronica può essere tecnicamente realizzato direttamente dall'INGV tramite la propria infrastruttura informatica ovvero può essere gestito da fornitori commerciali di servizi, alle condizioni d'uso sottoscritte. In questo secondo caso, l'utilizzo del servizio di posta elettronica è soggetto, oltre alle disposizioni contenute nel presente regolamento, alle condizioni d'uso e alle norme sulla protezione dei dati personali soggette alla normativa vigente in materia di privacy, nazionale ed europea. L'utente è tenuto a prendere visione ed a rispettare tali condizioni d'uso. Il Centro Servizi Informativi ed il Responsabile per la Protezione dei Dati sono a disposizione per fornire agli utenti tutte le i chiarimenti necessari.

Alla cessazione dell'attività lavorativa presso l'Istituto valgono le regole del successivo articolo 12.

Non utilizzare la posta elettronica per l'invio di materiale riservato o contenente dati sensibili senza adottare opportune protezioni crittografiche.

9. USO DEI SISTEMI DI VIDEOCONFERENZA

Principi generali

L'ente mette a disposizione un servizio di videoconferenza e streaming web che deve essere utilizzato per le attività istituzionali e lavorative, il suo uso viene incentivato soprattutto per le attività, es. riunioni, che comporterebbe lo spostamento del personale tra le sedi nazionali.

Regole di utilizzo

Per l'uso dei servizi di videoconferenza, valgono le seguenti norme comportamentali:

1. Dato il consumo di banda internet sono sconsigliate le videoconferenze tra utenti presenti nella stessa sede.
2. Nel caso di videoconferenze e streaming web di eventi come convegni e conferenze il personale presente nella sede dove si tiene l'evento è invitato a partecipare di persona per lasciare ai colleghi esterni la possibilità di accesso al sistema.
3. È vietato instaurare videoconferenze in locali e ambienti allo scopo di monitorare le attività che lì si svolgono.
4. L'attività di una videoconferenza in corso deve essere opportunamente segnalata ai presenti.
5. Le sale riunioni e le sale conferenza sono dotate di sistemi dedicati, è fatto divieto di modificare le configurazioni di detti sistemi senza la preventiva autorizzazione del CSI.
6. I CSI predispongono procedure di richiesta e guide d'uso per il servizio videoconferenza e streaming.
7. Gli utenti sono tenuti a conoscere il funzionamento della video conferenza, documentandosi tramite gli howto messi a disposizione allo scopo dal CSI.

ST QV

10. USO DELLA RETE LOCALE, INTERNET E RISORSE CONDIVISE

Principi generali

Di norma ogni postazione di lavoro è connessa alla rete locale della propria sede ed agli utenti sono fornite le credenziali per l'accesso alla intranet, ad internet ed alle risorse di rete condivise funzionali all'attività lavorativa. Tali accessi devono avvenire esclusivamente per finalità istituzionali, strettamente connesse agli incarichi lavorativi svolti e sempre nel rispetto delle regole elencate in questo documento o nei manuali operativi di dettaglio.

Regole di utilizzo

Per l'uso dei servizi connessi ad internet, alla rete locale ed alle risorse di rete condivise, valgono le seguenti norme comportamentali:

1. Non trasferire sulla propria postazione di lavoro, mediante download, file o programmi da siti sconosciuti che potrebbero compromettere il funzionamento del computer.
2. Non scaricare e/o scambiare materiale protetto da diritti di proprietà intellettuale senza averne titolo e comunque sempre e solo per attività connesse alle esigenze lavorative.
3. Non è consentito l'uso di programmi peer to peer per lo scambio di file in ambito privato.
4. Non pubblicare testi, immagini o video a contenuto blasfemo, osceno o diffamatorio.
5. È vietata ogni forma di registrazione a nome dell'Istituto o fornendo i dati relativi ad indirizzi e-mail lavorativi a siti i cui contenuti non siano legati all'attività lavorativa.
6. Cercare di limitare, ogni volta che sia possibile, le stampe in modo da risparmiare preziose risorse e non intralciare il lavoro altrui.
7. Ad ogni utente e ad ogni ufficio che ne faccia richiesta, viene assegnato, compatibilmente alle disponibilità, uno spazio sui file server centrali.
8. Le cartelle presenti nel server sono aree di salvataggio e/o condivisione di informazioni strettamente professionali: non possono in alcun modo essere utilizzate per scopi diversi.
9. Il materiale non pertinente all'attività lavorativa non può essere dislocato, nemmeno temporaneamente, sulle cartelle di rete condivise. Il personale dei Centri Servizi Informativi può procedere in ogni momento alla rimozione di materiale ritenuto non pertinente o potenzialmente pericoloso senza preavviso.
10. Sulle unità di rete condivise vanno svolte regolari attività di controllo, amministrazione e back up da parte dei Centro Servizi Informativi, nel caso in cui si rientri in unità condivise di servizi comuni, da parte dell'amministratore di sistema o del singolo utente che gestisce l'unità condivisa, per evitare la perdita dei dati.
11. Lo spazio disco messo a disposizione ha dei costi notevoli sia in termini economici che di tempo dedicato alla manutenzione, pertanto ogni utente periodicamente provvede alla cancellazione dei file obsoleti o inutili; Al superamento del limite individuale impostato per la quantità di informazioni, per validi e giustificati motivi, è possibile per

il responsabile del servizio richiedere ai Centro Servizi Informativi un ampliamento dello spazio a disposizione.

11. USO E ACCESSO AI CENTRI ELABORAZIONE DATI (CED)

Principi generali

Ogni Sede dell'INGV è dotato di uno o più locali CED adeguati all'attività ad accesso controllato sotto la supervisione del CSI locale. Questi locali sono destinati ad ospitare l'infrastruttura server, storage e di rete della sede fornendo un adeguato sistema di alimentazione, raffreddamento, sicurezza e controllo accessi. Al loro interno trovano collocazione principalmente i servizi informatici di uso generale, i sistemi perimetrali di connettività e sicurezza, i sistemi che gestiscono in modo centralizzato i dati amministrativo-contabili, sensibili e personali; se i locali lo consentono e senza ridurre il livello di sicurezza dei servizi generali è possibile collocare all'interno anche infrastrutture server e storage dedicati alle attività dell'ente, al "supercalcolo" e ai progetti scientifici.

Regole di utilizzo

Ogni CSI locale, in accordo con il presente regolamento e la normativa vigente, i servizi tecnici e il responsabile della sicurezza sul lavoro, predispone un manuale operativo di uso e accesso ai CED che in modo dettagliato regoli almeno i seguenti aspetti:

1. Politiche di accesso ai locali e loro politica di sicurezza;
2. Politiche di uso degli spazi e delle risorse;
3. Politiche di acquisto delle risorse e loro dismissione;
4. Politiche di gestione dell'infrastruttura;
5. Politiche d'uso da parte degli utenti e in particolare dei progetti scientifici;
6. Politiche di interazione e collaborazione con soggetti esterni all'ente.

12. CESSAZIONE DEL RAPPORTO DI LAVORO

Al momento della cessazione del rapporto di lavoro, ovvero di qualunque evento che comporti la modifica delle funzioni precedentemente espletate, l'utente deve mettere a disposizione dell'Ente tutte le risorse assegnate, sia in termini di attrezzature informatiche che di informazioni di interesse per i Servizi.
La fase di cessazione prevede le seguenti modalità operative:

1. Le credenziali fornite all'utente verranno disabilitate: è cura del responsabile del Servizio interessato e dell'ufficio del personale comunicare le cessazioni degli utenti ai Centro Servizi Informativi.
2. La casella di posta elettronica individuale verrà disattivata e successivamente cancellata: le attività necessarie per il passaggio delle consegne e la copia del materiale di interesse dell'Ufficio dovranno essere effettuati prima della disattivazione, a cura del responsabile del Servizio interessato. In particolare, dopo la cessazione, a vario titolo, l'account di posta istituzionale sarà mantenuto per 30 giorni e, se richiesto, per i successivi 30 giorni, sarà impostato un alias ad una casella di posta del cessando richiedente.
3. La procedura di rimozione/disattivazione può essere sospesa nel caso siano in corso attività di prolungamento dell'attività lavorativa per mezzo di associazioni, collaborazioni ecc. in via di definizione.
4. Le eventuali registrazioni su siti e sistemi esterni, effettuate per motivi di servizio e legate alla casella di posta elettronica del dipendente, dovranno essere portate a conoscenza del Direttore

in tempo utile per consentire una loro migrazione verso altri utenti, ovvero la loro disabilitazione.

5. Le informazioni e i documenti prodotti o entrati nella disponibilità dell'utente nell'esercizio dell'attività lavorativa a favore dell'Istituto Nazionale di Geofisica e Vulcanologia restano nella piena ed esclusiva disponibilità dell'Ente ad esclusione dei casi in cui la normativa di riferimento riconosca all'utente la proprietà intellettuale su tali prodotti.
6. L'utente non può formare, ottenere copia e/o cancellare documenti ed informazioni di interesse dell'Ente presenti sulle postazioni di lavoro o sulle risorse di rete, né farne alcun uso dopo la cessazione del rapporto di lavoro a meno di esplicita autorizzazione scritta preventiva da parte del responsabile della struttura di appartenenza.
7. Le informazioni eventualmente lasciate sulle postazioni di lavoro o sulle risorse di rete che non siano di interesse per l'Istituto verranno cancellate al termine del rapporto di lavoro senza alcuna responsabilità per l'Ente.
8. Il "cessando" è tenuto a fornire ai propri referenti qualunque dato di interesse collettivo, come ad esempio documenti sviluppati in gruppo tramite gli applicativi google, tempestivamente e comunque entro la data di cessazione dell'account, per evitare la perdita definitiva del materiale.

13. INTERVENTI DI ASSISTENZA E MANUTENZIONE

Il personale dei Centro Servizi Informativi ha tra i suoi compiti quello di garantire il funzionamento generale della infrastruttura (sicurezza informatica, backup, rete, server, progettazione informatica ecc.) e dedica le proprie risorse in via prioritaria allo svolgimento di tali attività.

Per le richieste di assistenza, valgono le seguenti norme comportamentali:

1. Le richieste vanno inoltrate esclusivamente attraverso l'apposita procedura presente in intranet o tramite altri strumenti similari resi disponibili presso le sezioni, indicando chiaramente il tipo di inconveniente riscontrato ed ogni tipo di informazione utile a diagnosticare il problema, evitando indicazioni generiche. Un messaggio di posta elettronica confermerà la presa in carico da parte del tecnico.
2. Le richieste vengono evase in ordine di ricezione, dando priorità agli interventi o che mettono a rischio la continuità dei servizi erogati ai cittadini o che coinvolgono più utenti.
3. Lo svolgimento di attività, che richiedono impegni finanziari per essere svolte, è soggetto a valutazioni di convenienza economica da parte dei Centro Servizi Informativi ed alla verifica della copertura finanziaria necessaria.

14. SVILUPPO

Il Servizio Informatico provvede allo sviluppo dell'infrastruttura informatica dell'Ente e ne cura la successiva manutenzione.
La gestione di progetti congiunti con altri Servizi e Direzioni è strutturata in modo tale per cui le attività aventi ricadute, anche indirette, sui Centro Servizi Informativi dell'Istituto Nazionale di Geofisica e Vulcanologia debbano prevedere il coinvolgimento dei Centro Servizi Informativi a partire dalla fase di progetto fino alla conclusione dei lavori, in modo da ottimizzare l'integrazione con l'infrastruttura esistente sia hardware che software con particolare riferimento alle attività legate a reti, cablaggi, procedure informatiche da ospitare

presso i CED o da alimentare con dati di pertinenza dell'Ente evitando costose duplicazioni e pericolose incompatibilità.

15. COORDINAMENTO DELLE ATTIVITÀ INFORMATICHE

Il Centro Servizi Informativi svolge un ruolo di coordinamento delle attività informatiche d'Istituto in particolar modo verso enti terzi quali AgID, GARR, CINECA, CASPUR, Bologna tecnopolo ecc., mantenendo costanti rapporti con questi enti e partecipando per conto dell'Istituto ai tavoli tecnici ed organizzativi per mezzo del suo personale o tramite delegati.

16. CONTROLLI

L'INGV, utilizzando i Centro Servizi Informativi per esigenze produttive o organizzative (ad esempio per rilevare anomalie o per manutenzione), può avvalersi, nel rispetto dell'art. 4 comma 2 dello Statuto dei Lavoratori, di sistemi che permettano un controllo indiretto a distanza (controllo preterintenzionale) e determinano un trattamento di dati riferiti o riferibili ai lavoratori, nel rispetto delle "Linee guida del Garante per posta elettronica e internet" emesse dall'Autorità Garante per la protezione dei dati personali il 1 marzo 2007;
L'istituto non effettua, in alcun caso, trattamenti di dati personali mediante sistemi informatici che mirino al controllo a distanza dei lavoratori, grazie ai quali sia possibile ricostruire la loro attività e che vengano svolti con i seguenti mezzi:

1. Lettura e registrazione sistematica dei messaggi di posta elettronica, al di là di quanto tecnicamente necessario per fornire il servizio di posta stesso;
2. Memorizzazione ed eventuale riproduzione delle pagine web visitate dal dipendente;
3. Lettura e registrazione dei caratteri inseriti dai lavoratori mediante tastiera;
4. Analisi occulta di computer affidati in uso;

Le attività di controllo, legittimamente svolte dall'Istituto per tramite dei Centro Servizi Informativi ai sensi del presente regolamento si attengono in ogni caso ai seguenti principi fondamentali:

1. Necessità, pertinenza e non eccedenza: il CSI e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite, osservando altresì il principio di pertinenza e non eccedenza. L'Istituto raccoglie e tratta i dati nella misura meno invasiva possibile; le eventuali attività di controllo sono svolte solo da soggetti preposti e sono mirate sull'area individuata come "di rischio".
2. Finalità e correttezza: I trattamenti sono effettuati per finalità determinate, esplicite e legittime. Le finalità perseguite dall'INGV riguardano o possono riguardare, caso per caso:
    a. Sicurezza sul lavoro
    b. Sicurezza dei sistemi e relativa risoluzione di problemi tecnici
    c. Esigenze di organizzazione
    d. Esigenze di produzione
    e. Rispetto di obblighi legali
    f. Tutela dell'Ente

3. Le attività che comportano l'uso del servizio di accesso ad internet vengono automaticamente registrate in forma elettronica da un apparato informatico (proxy o firewall) e memorizzate su log di sistema con le sole finalità statistiche sull'utilizzo dell'infrastruttura; Il trattamento dei dati contenuti nei log predetti può avvenire esclusivamente in forma anonima, in modo da precludere l'identificazione degli utenti e delle loro attività.
4. I dati personali contenuti nei log possono essere trattati in forma non anonima solo in via eccezionale ed esclusivamente nelle ipotesi in cui si rilevano evidenze di un utilizzo improprio o illegale, ovvero sia necessario corrispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria.
5. I dati contenuti nei log sono conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza – comunque non superiore a sei mesi – e sono cancellati periodicamente ed automaticamente dal sistema.

I Centro Servizi Informativi predispongono un manuale delle procedure di sicurezza informatica che descrive in dettaglio le procedure seguite per le attività di monitoraggio, controllo e analisi dei sistemi e dei flussi dati.

17. AUDIT DI CYBER SECURITY E CYBER VULNERABILITY

Principi Generali

Il Centro Servizi Informativi utilizzando programmi automatizzati, personale interno e/o terze parti esegue un controllo periodico dei livelli di sicurezza e vulnerabilità dei servizi e delle risorse informatiche presenti sulla rete d'Istituto o esposti su internet.

Modalità

Le attività di controllo, legittimamente svolte dal Centro Servizi Informativi ai sensi del presente disciplinare, seguono le presenti modalità:

1. Il primo controllo non può essere fatto prima di sei (6) mesi dall'approvazione del presente regolamento.
2. I controlli di sicurezza devono essere svolti dal CSI con cadenza almeno semestrale per i servizi e i server esposti su internet e per quelli che trattano dati rilevanti per le normative sulla privacy, con cadenza almeno annuale per tutte le altre risorse informatiche.
3. Il CSI emana un avviso per mezzo di comunicato sulla intranet e tramite mail ai dipendenti coinvolti almeno un mese prima del controllo.
4. Gli amministratori di sistema sono tenuti a comunicare al CSI eventuali problemi di sicurezza o vulnerabilità conosciuti, segnalando se possono porvi rimedio nei tempi concessi ed eventualmente indicare in modo dettagliato i motivi che impediscono o hanno impedito fino a quel momento l'adozione del rimedio.

La responsabilità di eventuali danni derivanti dall'attività di audit riportati ai sistemi e ai dati per negligenza nell'adottare le misure minime di sicurezza, gli aggiornamenti rilasciati ed eventuali contromisure conosciute senza aver effettuato preventiva comunicazione al CSI sono imputabili all'amministratore di sistema.

18. SANZIONI

L'inosservanza delle norme comportamentali descritte nel presente documento saranno valutate dai dirigenti responsabili per eventuali azioni disciplinari eventualmente consentite. Il dipendente cui sono assegnati i dispositivi informatici essendo responsabile della relativa custodia risponde di possibili azioni tese al risarcimento di eventuali danni arrecati alle apparecchiature, al software ed alle configurazioni in uso.

19. AUDIT E VERIFICA

L'ente nomina le figure professionali richieste dalla normativa di riferimento, quali ad esempio CCO, DPO e CISO, e predispone una politica di audit, certificazione e verifica delle procedure anche tramite parti terze se necessario.

20. INFORMATIVA

Il presente Regolamento costituisce informativa ai sensi dell'art. 13 del D.lgs. 30 giugno 2003, n. 196 e dell'art. 4, comma 3, della Legge 20 maggio 1970 n. 300 e s.m.i. circa le modalità e finalità del trattamento dei dati personali connessi all'uso delle risorse informatiche e dei servizi di rete.

L'Istituto Nazionale di Geofisica e Vulcanologia assicura al presente Regolamento, ai manuali operativi ed ai suoi successivi aggiornamenti la più ampia diffusione presso gli utenti, mediante:

1. Pubblicazione nella intranet aziendale.
2. Comunicazione del testo a tutti i dipendenti e a coloro che a vario titolo prestano servizio o attività per conto e nelle strutture dell'Istituto.
3. Consegna del testo alle rappresentanze sindacali per la pubblicazione presso i loro albi.
4. Messa a conoscenza a tutti i futuri dipendenti e a coloro che a vario titolo prestano servizio o attività per conto e nelle strutture di dove reperire il testo e i manuali operativi.
5. Pubblicazione del testo sul sito internet nazionale dell'INGV.
6. Il presente Disciplinare che ha valenza nazionale e per tutte le sedi Abroga e sostituisce integralmente tutti i precedenti adottati in materia.

21. CLAUSOLA DI REVISIONE

Il presente Regolamento verrà aggiornato qualora dovessero sussistere mutamenti normativi in materia nonché quelli connessi all'evoluzione tecnologica e organizzativa.