STATO MAGGIORE DELL'ESERCITO

III Reparto Impiego delle Forze/Centro Operativo Esercito

Ufficio Sicurezza e Informazioni

DIRETTIVA

Sicurezza dei Sistemi Informatici e di Telecomunicazione non classificati
Politica di Sicurezza dell'Esercito
(SME INFOSEC 001)

Edizione 2010

La presente direttiva consta di n. 32 pagine.

INDICE

STATO MAGGIORE DELL'ESERCITO

III Reparto Impiego delle Forze/Centro Operativo Esercito

Ufficio Sicurezza e Informazioni

ATTO DI APPROVAZIONE

Approvo la Direttiva "Sicurezza dei Sistemi Informatici e di Telecomunicazione non classificati. Politica di Sicurezza dell'Esercito"(SME INFOSEC 001)

Roma, 29 SET. 2010

IL CAPO DI SM DELL'ESERCITO

Gen. C.A. Giuseppe VALOTTO

CAPO I

Premessa

La garanzia del possesso delle informazioni in tutte le sue diverse forme di rappresentazione è un elemento fondamentale per consentire alla Forza Armata il pieno ed efficace assolvimento di tutti i compiti istituzionali.

L'evoluzione delle tecnologie informatiche ha permesso allo strumento militare di dotarsi di sistemi informativi e di Comando e Controllo automatizzati che permettono l'immagazzinamento e lo scambio di enormi quantità di dati/informazioni in "tempo utile" a decidere ai vari livelli di comando. L'utilizzo di tali strumenti tuttavia ha reso l'Organizzazione militare vulnerabile ad una serie di rischi provenienti sia dall'esterno sia dall'interno della stessa. Al fine di tutelare il patrimonio informativo nella sua totalità, assume sempre maggiore importanza la necessità di garantire la disponibilità, l'integrità e la confidenzialità sia dei sistemi/mezzi di comunicazione sia delle informazioni gestite/memorizzate/scambiate.

In tale ambito, la presente Direttiva – a similitudine di quanto previsto in ambito NATO – costituisce il riferimento normativo di base sul quale viene costruito, nel tempo, il corpo dottrinale completo della sicurezza informatica della Forza Armata conformemente anche alle indicazioni dello Stato Maggiore della Difesa che ha individuato negli Stati Maggiori delle Forze Armate gli *Enti Utenti Principali* – **EPU** – del sistema di sicurezza informatica della Difesa.

Scopo e ambito di applicazione

Scopo della presente Direttiva è quello di fornire una visione d'insieme della politica di sicurezza ICT (*Information and Communication Technology*) dell'Esercito limitatamente al dominio NON CLASSIFICATO in termini di obiettivi da perseguire nell'ambito di tutta la FA. Essa ha precedenza su qualsiasi altra disposizione in materia che dovesse presentarsi in contrasto, qualora non espressamente abrogata, e deve essere applicata a tutti le risorse ICT di Forza Armata schierati/impiegati sia in Madrepatria sia nei T.O.

Al Comando Trasmissioni e Informazioni Esercito (CoTIE), in qualità di Ente responsabile delle reti[1] della Forza Armata, spetta il compito di tradurre le linee di policy generale tracciate nella presente Direttiva in regolamenti attuativi attraverso la definizione delle tecnologie, degli strumenti, delle misure ritenute tecnicamente più efficaci per garantire un livello di sicurezza adeguato. Tali disposizioni dovranno essere diramate in maniera organica fino ai singoli Enti/Distaccamenti/Reparti mediante apposite direttive, da aggiornare periodicamente, al fine di facilitarne la comprensione e la successiva attuazione.

Per quei sistemi che si configurano come "isolati" (ad es. reti LAN confinate all'interno di singoli Comandi e non connesse con altre reti) è responsabilità dei Comandanti, che si avvalgono del personale tecnico preposto, ispirarsi ai criteri di sicurezza contenuti nella presente direttiva.

Di seguito vengono stabiliti:

- i criteri generali di sicurezza;
- i ruoli e le responsabilità riguardanti l'area della sicurezza ICT;
- le modalità di gestione degli incidenti informatici e la continuità dei servizi.

[1] Nel presente documento si utilizzerà, per semplicità, il termine "responsabile delle reti" intendendo con esso la responsabilità di attuazione, in aderenza alle direttive dello Stato Maggiore Esercito, della politica di sviluppo e di sicurezza dei sistemi C4 campali e di infrastruttura dell'Esercito.

CAPO II

ORGANIZZAZIONE DELLA SICUREZZA ICT

Lo Schema Nazionale Sicurezza ICT

L'organizzazione della sicurezza ICT dell'Amministrazione Difesa opera in conformità allo schema nazionale proposto dal Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni, riportato in Figura 1.

Figura 1 – *Schema nazionale sicurezza ICT (CNSI)*

La struttura organizzativa per la sicurezza informatica della Difesa

Le informazioni e i servizi informatici dell'Amministrazione Difesa sono parte integrante del proprio patrimonio ed elemento fondamentale per lo svolgimento delle finalità istituzionali, pertanto si presuppone il corretto svolgimento delle azioni di prevenzione, protezione e contrasto.

Le logiche organizzative generali sono:

presidio globale, mediante una visione unitaria e strategica in grado di valutare sia il rischio operativo sia le necessarie misure di sicurezza;

corretta responsabilizzazione, mediante una valutazione del rischio e l'individuazione di ruoli dell'amministrazione dotati di responsabilità;

bilanciamento Rischio/Sicurezza;

separazione dei compiti, secondo il principio che chi esegue non controlla e viceversa.

Di seguito, si riportano le funzioni e le relative principali responsabilità che costituiscono la struttura organizzativa della Difesa in materia di sicurezza ICT (per maggiori dettagli a riguardo si rimanda alla pubblicazione "SMD-I-019"):

Consigliere tecnico del Ministro della Difesa per la Sicurezza ICT

E' il consulente strategico del Ministro, l'interfaccia tra il Comitato di Sicurezza ICT ed il titolare del Dicastero.

Comitato per la Sicurezza ICT

E' l'organo di coordinamento strategico, cui viene demandata la politica di sicurezza delle infrastrutture tecnologiche e del patrimonio informativo. Tale Comitato, presieduto dal Sottocapo di SMD, coincide con il **Comitato di Coordinamento per l'ammodernamento e l'innovazione**.

Comitato di Coordinamento per la Sicurezza ICT (CCSI)

E' la struttura esecutiva del Comitato per la Sicurezza ICT composta dai rappresentanti dello SMD, di Segredifesa/DNA, delle Forze Armate e del Comando Generale dell'Arma dei Carabinieri. E' presieduto dal Vice Capo Reparto del II Reparto Informazioni e Sicurezza dello SMD ed è responsabile della elaborazione delle politiche di sicurezza generali per le Reti non classificate della Difesa da sottoporre all'approvazione del Comitato per la Sicurezza ICT.

Dirigente Responsabile dei Sistemi Informativi Automatizzati dell'AD (DGReSIAD)

È il referente cui compete la pianificazione degli interventi di automazione, l'adozione delle cautele e delle misure di sicurezza, la committenza delle attività da affidare all'esterno. Coincide con il Capo del VI Reparto dello SMD.

Responsabile della Sicurezza ICT (Difesa)

E' il Comandante del Comando C4 Difesa posto alla dipendenza gerarchico-funzionale del Capo del VI Reparto di SMD, responsabile dell'attuazione delle politiche di sicurezza ICT per le reti telematiche della Difesa.

La struttura organizzativa per la sicurezza informatica della Forza Armata

Per poter rispondere al meglio alla minaccia ai sistemi ICT, la Forza Armata ha inteso dotarsi di una propria organizzazione, secondo il modello seguente:

Responsabile della Sicurezza ICT di FA

È il soggetto al quale compete la definizione della politica generale di sicurezza presso la Forza Armata in conformità con gli indirizzi e le policy di sicurezza emesse dal Comitato per la Sicurezza ICT.
In tale ambito ha la responsabilità, tra l'altro, di:

- emanare le misure e i provvedimenti direttivi di alto livello per il raggiungimento/mantenimento del grado di sicurezza informatica auspicato;
- condurre attività di coordinamento con le Autorità/Organi responsabili della sicurezza ICT della Difesa e delle altre Forze Armate, secondo le regole ed i tempi concordati;
- indirizzare, se necessario, le attività del CERT di Forza Armata nella gestione di incidenti informatici, in coordinamento con il CERT della Difesa;
- notificare alla Difesa eventuali situazioni di vulnerabilità/attenzione, qualora non già fatto dal CERT di Forza Armata.

Si identifica nell'Ufficiale Generale Delegato alla Sicurezza dell'Esercito.

Ufficio Sicurezza e Informazioni dello Stato Maggiore dell'Esercito

E' l'organo di cui il Responsabile alla Sicurezza ICT si avvale nella definizione della politica generale di sicurezza della Forza Armata. In tale contesto:

- rappresenta il naturale referente della Forza Armata nei confronti di analoghi attori dello Stato Maggiore della Difesa (SMD) e degli SM delle altre Forze Armate;
- partecipa ai maggiori consessi sia in ambito Difesa (ad esempio, Comitato di

Coordinamento per la Sicurezza ICT) sia in contesti internazionali;
- propone l'adozione di misure eccezionali a salvaguardia della sicurezza ICT;
- fornisce il proprio parere sulle proposte avanzate dal CoTIE in tema di sicurezza ICT;
- vigila, anche attraverso attività ispettive, sulla corretta attuazione delle misure di sicurezza da parte di tutti gli Enti/Distaccamenti/Reparti.

Comando Trasmissioni e Informazioni Esercito

Come anticipato nel Capo I, in quanto Ente responsabile delle reti ICT della Forza Armata, il CoTIE ha il compito principale di tradurre le linee di policy generale definite dal Responsabile della Sicurezza ICT di Forza Armata in una serie di misure tecnologiche e procedurali, cui tutti gli Enti/Distaccamenti/Reparti sono tenuti a conformarsi. Egli agisce, pertanto, in autonomia per quanto concerne la definizione delle azioni discendenti dalla presente Direttiva, mentre formula proposte, attraverso l'Ufficio Sicurezza e Informazioni dello SME, per quelle soluzioni la cui natura non presenta uno stretto legame con i contenuti di essa. Il CoTIE è, inoltre, responsabile di tutte le azioni, attive e passive, per fronteggiare attacchi ovvero incidenti informatici, per mitigarne gli effetti e per il successivo ripristino delle funzionalità della rete, azioni che esprime attraverso il *Computer Emergency Response Team* della Forza Armata (CERT EI – vds. successivo CAPO IV).

La Struttura operativa di sicurezza ICT dell'Esercito

Oltre agli attori di riferimento indicati in precedenza, l'organizzazione di sicurezza ICT di Forza Armata prevede la costituzione di ulteriori strumenti di controllo per:
- la difesa da eventuali intrusioni dall'esterno;
- la difesa da comportamenti malevoli interni;
- preservare l'immagine di fiducia (trust) del proprio dominio (EInet) e delle sue connessioni esterne (DIFENET, internet).

A tal fine è istituita una struttura funzionale per la gestione delle problematiche informatiche che prevede, oltre al CERT-EI, anche una organizzazione territoriale capillare in tutto il dominio Esercito.

Ogni Comandante, nella piena consapevolezza della necessità di dover proteggere le informazioni elaborate localmente e in aderenza alla normativa vigente, è tenuto a intervenire attraverso l'efficace sensibilizzazione/addestramento del personale dipendente ed il contrasto ai comportamenti anomali.

Con questi presupposti, si attua una strategia di sicurezza univoca di Forza Armata che si basa:
- sulla definizione delle criticità e sulla individuazione delle risorse da proteggere;
- sull'aumento delle capacità del personale di impiegare in modo "sicuro e responsabile" i sistemi e i programmi informatici;
- sul rafforzamento delle capacità di gestione delle attività, attraverso la creazione ed il supporto di gestori/amministratori dei sistemi e figure di responsabilità (U. alla Sic. EAD designato / Responsabile Operativo locale della Sicurezza) capaci ed affidabili;
- sulla protezione delle risorse, mediante il controllo degli apparati condivisi e una compartimentazione dei "contenitori" delle informazioni, sulla base della reale necessità di conoscere;
- sulla presenza di misure/tecnologie di protezione e sull'applicazione di misure restrittive;
- sulla individuazione di comportamenti anomali/malevoli, per il tramite di una ricerca attiva e continua di eventuali azioni non autorizzate;
- sulla pronta reazione a tutti i livelli di Comando, allo scopo di sanzionare e correggere quei comportamenti sospetti e/o inaccettabili con provvedimenti disciplinari e, se necessario, legali.

In definitiva, la struttura operativa di sicurezza ICT dell'Esercito può essere sintetizzata come

schematizzato nella figura n. 2 riportata di seguito:

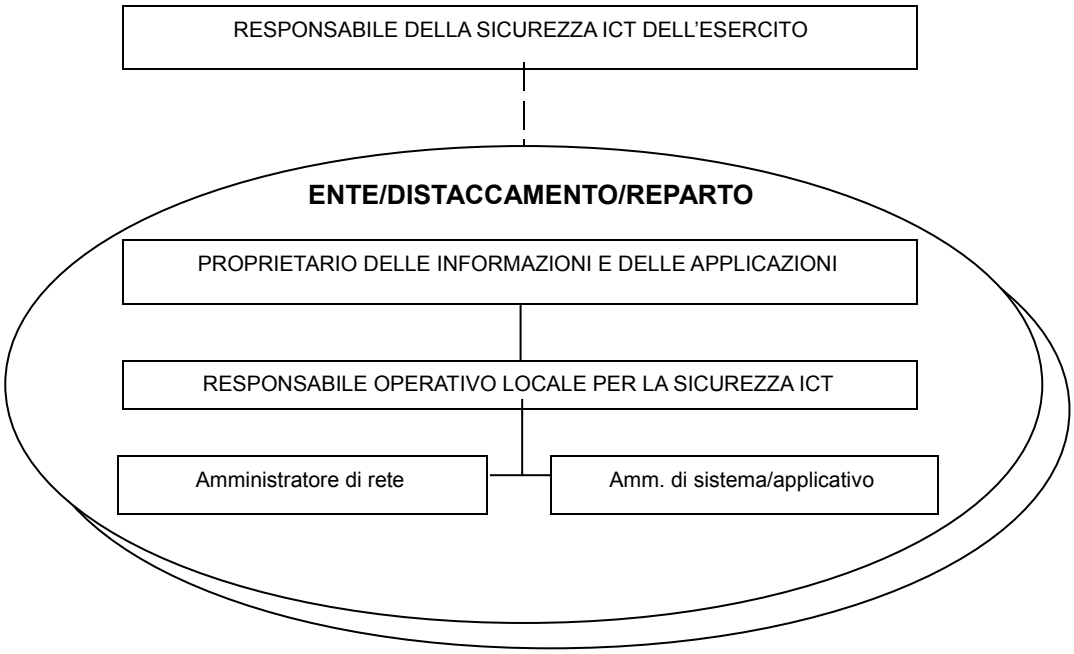


Figura 2

– – – – Dipendenza funzionale per via gerarchica
———— Dipendenza funzionale

Presso ciascun Ente/Distaccamento/Reparto (E/D/R) vi è, pertanto, la presenza del:

Proprietario delle informazioni e delle applicazioni

E' il soggetto responsabile nei confronti degli utenti e delle istituzioni, del corretto trattamento delle informazioni e impiego delle applicazioni nel rispetto delle normative nazionali e della policy dell'Esercito. Di norma coincide con il Comandante dell'E/D/R in cui si svolgono i trattamenti e presso cui sono installate/utilizzate le applicazioni.

Responsabile Operativo locale per la Sicurezza ICT

Nominato dal Comandante, è responsabile:

- del controllo delle attività di sicurezza ICT nell'ambito del proprio E/D/R e di quelli gerarchicamente dipendenti;
- dell'applicazione delle norme afferenti al settore della sicurezza ICT (Sistemi EAD non classificati, compresa internet).

Allo scopo di garantire una visione globale della sicurezza EAD (classificata e non) dell'intero Ente, il Responsabile Operativo locale per la Sicurezza si identifica, di norma, con l'Ufficiale alla Sicurezza EAD designato. Tuttavia, in virtù della complessità della struttura in cui ci si trova ad operare, il Comandante può assegnare il citato incarico a persona diversa, nel qual caso egli dipende funzionalmente dall'Ufficiale alla Sicurezza EAD designato.

Ove non diversamente specificato, nel seguito della presente Direttiva con il termine Responsabile Operativo locale per la Sicurezza si intenderà l'Ufficiale alla Sicurezza EAD designato.

Amministratore di rete e Amministratore di Sistema/Applicativo

Sia l'Amministratore di rete, sia l'Amministratore di sistema/applicativo, sono nominati dal Comandante. La scelta deve essere effettuata sulla base di una riconosciuta affidabilità ed *expertise* accumulata nello specifico settore. A tali figure, che avranno dipendenza funzionale dal Responsabile Operativo locale per la Sicurezza ICT, è attribuita la diretta responsabilità di attuare sia sulle reti, sia sui sistemi/applicativi di pertinenza le soluzioni tecnologiche adatte a implementare, all'interno del proprio E/D/R, la policy di sicurezza ICT e le direttive applicative discendenti, fermo restando che è preciso compito di ciascun Comandante controllarne la corretta applicazione.

CAPO III

SICUREZZA DELLE RISORSE ICT

Obiettivi di sicurezza

Il "dominio Esercito" (inteso come l'insieme di sistemi, applicativi, reti di calcolatori, informazioni) deve avere caratteristiche di sicurezza tali da poter essere considerato un dominio affidabile (*trusted*) ossia capace di assicurare senza soluzione di continuità la confidenzialità, l'integrità e la disponibilità delle informazioni gestite e conservate nei propri sistemi informatici e di telecomunicazione.

Ciascun E/D/R della Forza Armata deve garantire la diffusione e l'applicazione dei principi generali di sicurezza ICT, all'interno dei propri domini di competenza in modo da assicurare il raggiungimento del livello minimo comune di sicurezza.

L'affidabilità del dominio Esercito è data dalla minima affidabilità assicurata da ciascun sottodominio che lo costituisce[2]. Pertanto, su ogni sottodominio, come sull'intera EInet devono essere perseguiti gli stessi obiettivi minimi di sicurezza. Inoltre le interconnessioni con reti *untrusted* (es. reti di pubblico dominio, internet) devono essere costantemente monitorate e se non necessarie dovranno essere disattivate.

Il Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS)

Nella figura n. 3, è rappresentato lo schema del Sistema di Gestione della Sicurezza delle Informazioni dell'Esercito (SGSI o nella dicitura anglosassone *Information Security Management System*) quale complesso delle politiche, linee guida, procedure, misure di protezione fisiche, tecniche e relative al personale che opera con i sistemi.

Attraverso il SGSI, devono essere sviluppate le politiche, gli standard, le linee guida e le procedure operative e di sicurezza dei sistemi informatici della Forza Armata.

[2] Principio dell'"anello più debole"

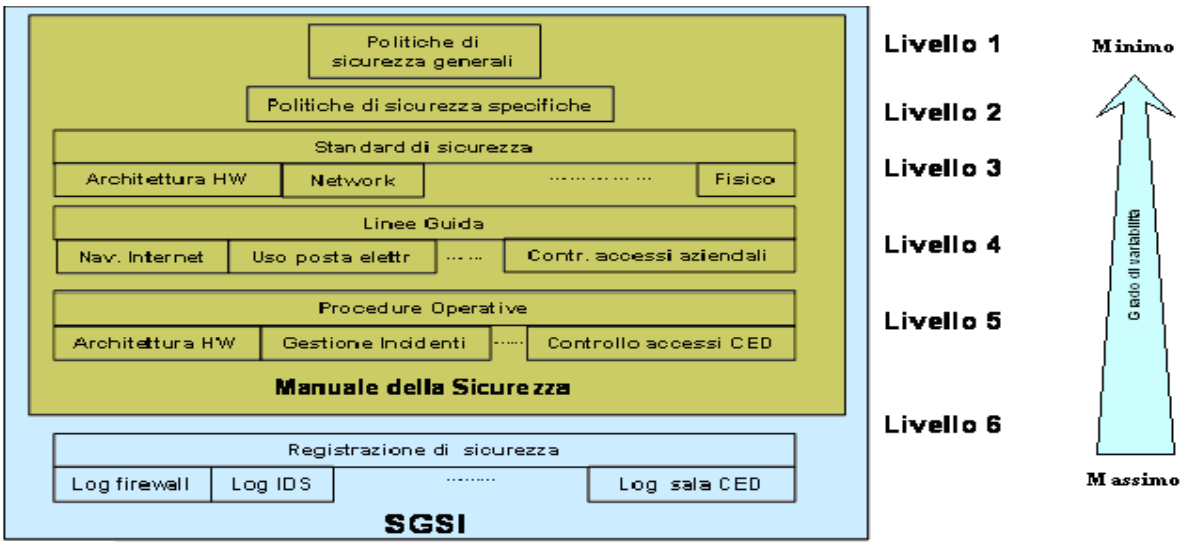


Figura 3 – La gerarchia della documentazione all'interno del sistema documentale

Il modello per il controllo dei processi da applicare al sistema documentale indicato in figura 3, per una ottimale gestione del rischio è il PDCA (Plan, Do, Check, Act) ossia:

- Pianificazione (emanazione della policy e delle direttive);
- implementazione (della policy e delle direttive);
- verifica dell'efficacia;
- aggiornamento e miglioramento della documentazione.

Procedura di autovalutazione per la gestione della sicurezza

Ogni E/D/R deve adottare ed applicare, almeno annualmente, un processo di autovalutazione del proprio livello di sicurezza[3], secondo la procedura definita in Allegato 1, al fine di:

- acquisire conoscenza delle minacce e delle vulnerabilità che incombono sui propri sistemi;
- poter dirigere sforzi e risorse a difesa delle aree più a rischio e assicurare la citata base minima di sicurezza.

Nel caso in cui dall'autovalutazione scaturisse un livello di sicurezza "NON ADEGUATO", si dovranno porre in essere tutte le azioni ritenute necessarie (eventualmente con il supporto tecnico del CoTIE) per elevare tale livello fino ad "ADEGUATO".

Il Responsabile della Sicurezza ICT dell'Esercito ha la facoltà di imporre, in ambito Forza Armata, la metodologia ritenuta più idonea in modo da uniformare processi di valutazione, risultati e terminologia utilizzata.

La classificazione delle risorse

La protezione delle informazioni attraverso l'applicazione dei principi di confidenzialità, di integrità e di disponibilità delle stesse, non può prescindere da una propedeutica attività di identificazione, classificazione e controllo delle risorse, il cui possesso "integro" è essenziale per la Forza Armata e la Difesa.

La classificazione ha l'obiettivo di consentire l'adozione di misure di sicurezza commisurate al valore della risorsa stessa, mediante l'acquisizione della consapevolezza del livello di importanza e la suddivisione in classi sulle quali poter poi predisporre servizi di sicurezza differenziati.

Ciascuna *risorsa* deve essere associata ad un *proprietario* il quale ha i seguenti compiti:

garantire che la risorsa sia classificata in modo appropriato;

[3] Attività in aderenza alla Direttiva 16 gennaio 2002 del Presidente del Consiglio dei Ministri – Dipartimento per l'Innovazione e le Tecnologie "Sicurezza Informatica e delle Telecomunicazioni nelle P.A. Statali"

definire e rivedere periodicamente le classificazioni applicate;

assicurare la protezione delle informazioni personali.

Un elenco, non esaustivo delle risorse da considerare è il seguente:

le banche dati/archivi;

le reti di comunicazione e le connessioni geografiche utilizzate per lo scambio delle informazioni;

le applicazioni;

gli impianti tecnologici di supporto (impianti elettrici, di riscaldamento, di rivelazione e spegnimento incendi, di condizionamento ecc);

i servizi offerti;

Ciascuna risorsa individuata dovrà essere localmente censita e mantenuta in inventario, al fine di poterla univocamente identificare, localizzare ed associare correttamente alla struttura organizzativa proprietaria, allo scopo di procedere ad una valutazione delle risorse stesse.

La classificazione deve essere effettuata secondo lo schema riportato di seguito:

Classificazione in base al valore della risorsa		*Descrizione*
1	**Minimo**	Bassa rilevanza. Una eventuale perdita, distruzione o alterazione non comporta impatti economici e organizzativi di rilievo. Impatto localizzato.
2	**Normale**	Rilevanza marginale. Nel caso di distruzione o alterazione l'impatto economico ed organizzativo è marginale e circoscritto.
3	**Base**	Importante. Nel caso di perdita, distruzione o alterazione è necessario un ripristino al più nell'arco di pochi giorni per evitare ripercussioni negative anche gravi su una o più organizzazioni della Difesa.
4	**Critico**	Alto valore per processi critici della Forza Armata. L'eventuale perdita, distruzione o alterazione può avere conseguenze molto rilevanti sulla capacità operativa dell'intero sistema informatico.
5	**Essenziale**	Estremo valore. La loro eventuale perdita, distruzione o alterazione può portare al blocco completo dell'operatività dell'intera Forza Armata.

Per una corretta, classificazione si dovrà tenere conto dei seguenti fattori:

possibili danni materiali;

impatto operativo derivante dal mancato trattamento in sicurezza delle informazioni.

La classificazione delle risorse dovrà essere soggetta a periodiche rivisitazioni, anche sulla base delle linee guida che saranno definite dal CoTIE.
Tra le risorse, particolare importanza assumono le informazioni.

La classificazione delle informazioni

In ambito Difesa vengono individuate tre tipologie di informazioni:

- informazioni dell'amministrazione;
- informazioni del personale;
- informazioni di log o di registrazione.

Informazioni dell'amministrazione: informazioni relative ai processi funzionali della specifica organizzazione. Tali informazioni hanno spesso una valenza generalizzata e quindi vengono anche trattate al di fuori dell'organizzazione che le ha generate. Il rischio derivante da una cattiva o mancante classificazione dell'informazione è elevato. Ad esse si applicano le limitazioni basate sul principio che l'informazione appartiene a colui che la genera e derivanti dallo specifico procedimento che l'amministrazione svolge.
Informazioni del personale: ad esse si applicano le limitazioni nel trattamento previste dalla normativa vigente sulla tutela delle informazioni personali.
Informazioni di log o di registrazione del sistema ICT sono relative al funzionamento e all'utilizzo dello stesso sistema. Tali informazioni possono essere utilizzate per verificare l'uso del sistema ICT da parte degli utilizzatori, piuttosto che delle azioni di pirateria informatica provenienti dalla rete interna o da Internet.
Per una corretta classificazione delle informazioni è opportuno inoltre tener conto:

- dei risvolti operativi e gestionali:
  - per quanto tempo sono trattenuti prima di essere distrutti,
  - come sono trattati (dati confidenziali, pubblici, ecc.),
  - come sono protetti.

- dei rischi:
  - perdita di informazioni critiche dovuta a un trattamento inadeguato;
  - compromissione di informazioni confidenziali durante la trasmissione;
  - distruzione o danneggiamento delle informazioni in seguito all'omissione o all'insufficienza di misure di sicurezza;
  - diffusione di informazioni non autorizzate a causa di carente o non presente classificazione.

Infine deve essere:

- individuato il livello di rischio (alto/medio/basso);
- applicato l'insieme di contromisure per la sua riduzione in relazione al livello di criticità della risorsa protetta, secondo quanto definito dal CoTIE.

Sicurezza del personale

Il personale dell'Amministrazione Difesa è parte attiva del processo di gestione del rischio e, quindi, deve essere a conoscenza delle politiche e delle procedure di sicurezza adottate.

Nella maggior parte dei casi, la minaccia ai sistemi informatici è da attribuire ad errati comportamenti interni all'organizzazione. Tali comportamenti censurabili possono essere ordinati in quattro differenti categorie:

- comportamenti volutamente malevoli, il cui risultato è l'intenzionale compromissione e/o la distruzione di informazione e dei servizi offerti dai sistemi, con evidente riduzione della capacità di operare da parte degli altri utenti interni;
- superficialità nell'applicazione delle procedure di sicurezza, che può comportare:
  - pubblica diffusione di informazioni;
  - immagazzinamento di informazioni classificate su supporti/sistemi non autorizzati;
  - errata/non opportuna distruzione di informazioni;
  - non adeguata protezione/controllo del materiale informatico (in particolare se classificato e/o sensibile) al di fuori delle strutture militari controllate.

superamento dei propri limiti di necessità di conoscere, eccedendo o abusando dei propri diritti di accesso alle risorse allo scopo di esplorare – se non di manipolare – il sistema informativo su cui si è autorizzati ad operare;

scarsa conoscenza nell'uso dei sistemi, delle politiche e delle procedure di sicurezza.

Pertanto, la sicurezza presuppone il coinvolgimento di tutti gli utenti finali, rendendo necessaria una maggiore diffusione della cultura della sicurezza ed una capillare e continua azione di informazione, finalizzata a sensibilizzare e responsabilizzare tutti gli utenti.

Ciascun E/D/R della Forza Armata sino a livello reggimento/battaglione autonomo o equivalente deve garantire la disponibilità di proprio personale opportunamente addestrato per la gestione della sicurezza informatica dei sistemi e dei servizi ICT di propria competenza e/o utilizzazione.

In tale ambito assume particolare importanza la corretta e puntuale pianificazione delle attività di formazione del personale in parola.

Sicurezza Fisica ed Ambientale

Al fine di assicurare la disponibilità delle risorse fisiche, è necessario innanzitutto predisporre un ambiente fisico protetto attraverso misure di controllo correlate ai rischi e al valore delle risorse.

Di seguito, sono indicati i principi ritenuti basilari in ambito Amministrazione Difesa.

a. Protezione del personale

La tutela della sicurezza e della salute delle persone fisiche è obiettivo primario che deve

essere garantito mediante una costante e capillare attività di informazione e formazione supportata dalla messa in sicurezza dei locali ed apparati.
Il personale, oltre ad essere a conoscenza della specifica modalità di accesso e fruizione della struttura in cui opera, deve essere informato sulle procedure da attuare in situazioni di emergenza. In tutte le aree di lavoro, deve esistere la documentazione prevista per i comportamenti nei casi di emergenza (almeno di evacuazione e di sgombero) e quadri di sintesi che consentano l'intervento anche da parte di personale non specificatamente addetto.

b. <u>Individuazione dei parametri di sicurezza</u>

Per prevenire i rischi di perdita o sottrazione di risorse informative, devono essere ben individuati i perimetri fisici di sicurezza con accesso selezionato in funzione al grado di criticità delle attività che vi si svolgono e del valore delle informazioni che vi sono conservate.
In particolare, tali perimetri si suddividono in:

Aree pubbliche a libero comune accesso;

Aree interne, dove il personale interno espleta le normali attività di lavoro e possono comprendere quelle aree di eventuale carico e scarico di materiali in cui è permesso l'accesso anche di personale esterno debitamente autorizzato;

Aree EAD ed Aree riservate EAD, ad accesso proporzionalmente ristretto e controllato, laddove sono ospitate infrastrutture ICT.

c. <u>Controllo degli accessi fisici</u>

Prima di accedere nelle aree precedentemente citate, specialmente quelle EAD, normalmente si è sottoposti ad una identificazione presso dei punti di controllo, nel quale viene controllata la sussistenza di adeguata autorizzazione.

d. <u>Protezione dei cablaggi</u>

I cablaggi elettrici e quelli relativi alla trasmissione delle informazioni devono essere protetti da danneggiamenti o interruzioni, al fine di evitare impatti sui servizi forniti. In particolare, le linee elettriche dovrebbero essere separate dalle linee informazioni (che possono eventualmente richiedere schermature e protezioni contro eventuali intercettazioni).

e. <u>Protezione delle apparecchiature informatiche</u>

Tutte le apparecchiature informatiche devono preferibilmente essere allocate in quelle aree in cui l'accesso di personale non addetto all'elaborazione delle informazioni è ridotto al minimo.

f. <u>Sicurezza dei Centri di Elaborazione Dati (Data Center)</u>

I Data Center rappresentano da sempre elementi particolarmente delicati nella continuità di funzionamento di una infrastruttura ICT. La presenza al loro interno di apparati e risorse informatiche di specifica rilevanza, fa si che, essendo solitamente locali non specificatamente progettati per tale scopo (in quanto edifici costruiti con diversa destinazione e quindi in possesso delle ovvie lacune e limitazioni per gli aspetti strutturali e logistici), devono essere costantemente sottoposti ad adeguamenti tecnologici.
Per quanto sopra, è opportuno sempre verificare l'idoneità (in termini di fattori di rischio) di:

ambienti e confini (zone sismiche, rischi inondazioni e maremoti, depositi carburanti, industrie chimiche ecc);

struttura dell'edificio, progettato per consentire l'idonea distribuzione degli impianti tecnologici e strutturali e facilmente gestibile in caso di emergenza, evacuazione e di controllo degli accessi;

impianto elettrico, ben dimensionato, distribuito e ridondante con disponibilità di gruppi di continuità. Inoltre devono essere previste e regolamentate attività periodiche per il controllo dei sistemi ausiliari e di ridondanza;

impianto di telecomunicazione, realizzato con reti TLC distinte e ridondanti;

impianto di condizionamento, ben dimensionato al progetto per il mantenimento della corretta temperatura indispensabile al funzionamento del sistema;

impianto antincendio, nel quale deve essere ben determinato il sistema di rivelazione e neutralizzazione degli incendi in base al progetto e dimensionamento dei locali. La protezione dal fuoco deriva anche da opportune scelte strutturali, quali la possibilità di contenimento del fuoco nelle diverse sezioni, l'assenza di materiali infiammabili e la presenza di isolanti e contro soffittature. Devono inoltre essere previste e regolamentate attività periodiche di simulazione antincendio per tutto il personale addetto;

controllo accessi, da effettuare rigorosamente mediante identificazione personale. Nei Data Center di rilevante importanza è auspicabile la presenza di sistemi di sorveglianza continua e di controllo degli accessi;

sistemi di monitoraggio e di allarme, con procedure automatiche di *escalation* a seconda dei fattori di pericolosità rilevata;

manutenzione apparecchiature.

Sicurezza dei Sistemi e delle reti

La riorganizzazione dell'intero sistema informativo dell'Amministrazione Difesa verso il modello architetturale "*Net Centric Information Management System* (NC-IMS)" e la conseguente volontà di perseguire un'ampia distribuzione ed articolazione delle utenze che accedono alle applicazioni ed ai servizi erogati, impone sempre più l'attuazione e il rispetto di requisiti di sicurezza, mediante una maggiore sensibilità alle specifiche problematiche e la loro puntuale osservanza.

Pertanto l'accesso alle risorse informatiche deve essere formalmente autorizzato in base alle reali esigenze operative e alle credenziali degli utenti.

I gestori dei singoli sistemi, EInet inclusa, devono individuare i servizi considerati essenziali e critici, valutando l'impatto massimo che potrebbe avere la loro mancata disponibilità e predisponendo appositi piani per assicurarne la continuità e il ripristino (*Business Continuity Plan* e *Disaster Recovery Plan*). I Responsabili Operativi Locali di Sicurezza ICT devono effettuare una continua e puntuale attività di monitoraggio, allo scopo di assicurare:

l'aggiornamento dei piani citati;

la loro efficacia nel tempo.

Tali verifiche dovranno prevedere esercitazioni pratiche con cadenza periodica almeno annuale che forniscano indicazioni circa i risultati ottenuti dall'applicazione dei piani. L'esito di ogni esercitazione dovrà essere sommariamente registrato e tenuto a disposizione (a cura del Responsabile Operativo Locale della Sicurezza ICT) per almeno tre anni per eventuali ispezioni.

a. Connessioni tra la rete EInet ed altre reti della Difesa/P.A. e servizi internet

Nel caso in cui, per esigenze operative, dovranno essere interconnessi sistemi della Forza Armata con sistemi appartenenti ad altri Enti della Difesa/P.A., dovrà essere necessariamente chiesta la preventiva autorizzazione da parte dell'Ufficio Sicurezza e Informazioni dello SME, per i riflessi sulla sicurezza che tale misura comporta.

Per quanto concerne l'esposizione di servizi su internet da parte di qualsiasi E/D/R della Forza Armata (ad esempio realizzazione di siti web), essa dovrà essere sottoposta alla valutazione e successiva autorizzazione da parte dello Stato Maggiore dell'Esercito e comunque dovrà avvenire attraverso i gateway di Forza Armata. In particolare, in considerazione dell'importanza che riveste l'informazione veicolata all'esterno, la competenza ed il coordinamento della stessa risale direttamente all'Ufficio Affari Generali dello SME, mentre per quanto concerne gli aspetti tecnici e quelli relativi alla sicurezza dovranno essere interessati, rispettivamente, l'Ufficio Comunicazioni e Sistemi e l'Ufficio Sicurezza e Informazioni.

b. <u>Politiche di controllo degli accessi</u>

Per ciascun utente o gruppo di utenti e per i fornitori di servizi, devono essere definite, a cura del CoTIE le modalità e le regole per implementare la corretta politica degli accessi alle risorse e a internet (ad esempio fissando e controllando i punti/siti di accesso attraverso cui gli utenti EInet possono/devono collegarsi a internet).

Le regole per il controllo degli accessi devono essere supportate almeno da:

procedure formali;

responsabilità chiaramente definite.

Il profilo dell'utente deve essere sempre coerente con i controlli di accesso configurati all'interno dei sistemi e delle applicazioni a cui l'utente ha necessità di accedere. La procedura che una organizzazione deve attuare nella gestione degli accessi è composta dalle seguenti fasi principali:

registrazione degli utenti, dove viene verificata l'identità dell'utente e vengono consegnati le credenziali per l'utilizzo dei sistemi informatici;

gestione dei privilegi, concessi per consentire operazioni particolari che normalmente non sono ad appannaggio degli utenti o programmi utente, ma solo di utenti amministratori e di programmi di sistema;

gestione delle *password* di utente (almeno 6 caratteri alfanumerici che devono essere variate periodicamente);

revisione periodica dei diritti di accesso, da riesaminare ad intervalli regolari e dopo ogni cambiamento di ruolo dell'utente (promozione, trasferimento o fine rapporto).

c. <u>Responsabilità degli utenti</u>

Tutti gli utenti devono essere resi consapevoli, attraverso specifici e periodici indottrinamenti, dell'importanza di un comportamento responsabile al fine di mantenere efficace il controllo degli accessi. Adeguata rilevanza deve essere posta in merito all'utilizzo delle *password* e dei dispositivi di sicurezza loro affidati e in generale ad ogni sistema/dispositivo/informazione gestita, che deve essere utilizzato nel pieno rispetto dei regolamenti e della legislazione vigente. Tale disposizione deve essere espressamente indicata/richiamata nei Documenti Programmatici di Sicurezza editi da ciascun E/D/R.

d. <u>Controllo dell'accesso alla rete</u>

L'accesso degli utenti alle reti e ai servizi deve avvenire in modo da non compromettere la loro sicurezza, evitando la possibilità di accessi non autorizzati. Pertanto, è opportuna la predisposizione di appropriati meccanismi di autenticazione di controllo degli accessi a qualunque servizio informatico disponibile in rete, in particolare nell'interconnessione tra differenti Domini o con le reti pubbliche. <u>L'utilizzo dei servizi offerti da Internet utilizzando qualsiasi postazione di proprietà dell'A.D</u>., ovvero che appartenga o meno alla intranet di Forza Armata – Einet, <u>dovrà avvenire esclusivamente attraverso i proxy server individuati dal CoTIE ed approvati dallo Stato Maggiore dell'Esercito, salvo autorizzazioni da concedere in via del tutto eccezionale da esaminare caso per caso</u>. <u>Ogni</u>

altra soluzione priva di qualsiasi forma di controllo da parte del CoTIE (ad esempio attraverso telefoni cellulari, modem, ecc.) è espressamente vietata.
Deve essere assicurata la massima sicurezza nell'interconnessione delle reti, utilizzando adeguate politiche di protezione e soluzioni tecniche che garantiscano la sicurezza degli accessi e dello scambio di informazioni, sia a livello di porta di rete, sia a livello di utenti.
I Responsabili Operativi Locali della sicurezza ICT delle singole reti/infrastrutture e sistemi dovranno determinare le regole di accesso al proprio dominio, in linea con quanto previsto dalla presente Direttiva e da quelle applicative emanate dal CoTIE.

e. Controllo degli accessi al sistema operativo

Si elencano di seguito le prescrizioni minime da implementare per un corretto accesso al sistema operativo:

- l'accesso ai sistemi operativi deve essere regolato da funzioni di sicurezza interne che consentono di autenticare gli utenti autorizzati in accordo con una definita politica degli accessi;
- i tentativi di accesso rifiutati dal sistema devono essere registrati, in apposito file di log;
- tutti gli utenti devono disporre di un User ID e di una *password* di uso strettamente personale per consentire l'identificazione e l'autenticazione dell'utente o di un *token* di autenticazione;
- il sistema di gestione delle *password* deve essere interattivo e garantire la qualità delle *password* (almeno 6 caratteri alfanumerici con scadenza al più semestrale);
- le sessioni di lavoro dovranno essere chiuse dopo un periodo stabilito di inattività della postazione di lavoro, garantendo la chiusura delle applicazioni aperte e la chiusura del collegamento in rete.

f. Controllo degli accessi alle applicazioni ed alle informazioni

Ciascun E/D/R è tenuto a implementare su tutte le postazioni/dispositivi il sistema di protezione antivirus fornito dalla Forza Armata.
E' opportuno che ogni applicazione software preveda dei meccanismi di controllo degli accessi alle informazioni gestite in modo da evitare accessi non autorizzati. La restrizione degli accessi alle applicazioni e alle informazioni deve essere definita a partire dalle esigenze lavorative ed operative dell'utente.
La politica di controllo degli accessi all'applicazione deve essere coerente con la politica degli accessi definita dall'organizzazione responsabile della gestione dell'applicazione. Il risultato di tale operazione deve produrre una mappatura completa tra i diversi utenti previsti dall'applicazione e le funzioni richiamabili abilitando ciascun utente alle sole funzioni pertinenti con il ruolo svolto. I sistemi applicativi che trattano informazioni particolarmente sensibili e/o informazioni personali devono prevedere una gestione speciale atta a garantire protezioni aggiuntive, per evitare perdite di informazioni o divulgazione indesiderata di informazioni.

g. Requisiti di sicurezza dei sistemi informatici

Tutti i sistemi informatici della Forza Armata, devono prevedere requisiti di sicurezza. Tali requisiti devono essere redatti, in linea con quanto previsto dalla presente politica di sicurezza ICT, dall'ente committente e/o approvvigionante.
I sistemi di interconnessione con i domini della Difesa richiedono una approvazione a livello SMD.
In particolare, nella fase di preparazione dei Requisiti Operativi[4] del progetto, devono essere parallelamente redatti i Requisiti di Sicurezza come parte integrante delle specifiche tecniche e funzionali che il sistema informativo da realizzare dovrà soddisfare.

[4] Requisiti Operativi Preliminari (ROP), Requisiti Operativi Definitivi (ROD)

Le specifiche di sicurezza devono riguardare tutti gli apparati previsti nel progetto e devono interessare anche i servizi manuali e di controllo che sarà necessario attivare per la loro gestione. I requisiti di sicurezza ed i processi devono, quindi, essere integrati sin dalle prime fasi all'interno del progetto per la realizzazione o l'evoluzione di un sistema informativo. Per i prodotti acquistati, si dovrebbe seguire un formale processo di valutazione e di acquisizione, atto a confermare la piena rispondenza del prodotto riguardo i requisiti di sicurezza richiesti ai fornitori.
Per l'acquisizione di sistemi o apparati particolarmente critici, è prevista la loro preventiva valutazione e certificazione secondo gli standard ISO/IEC 15408 in conformità allo "Schema Nazionale per la valutazione e la certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione".

h. Elaborazione corretta nelle applicazioni e impiego di meccanismi crittografici

Allo scopo di prevenire errori, perdite, modifiche o cattivo utilizzo delle informazioni, è importante predisporre una validazione delle informazioni in ingresso, al fine di accertarne la rispondenza a quanto previsto dall'applicazione e la loro integrità.
L'obiettivo da perseguire è quello di garantire sempre la riservatezza, l'integrità, la disponibilità, l'autenticità e il non ripudio dell'informazione e a tal fine vengono impiegati diversi meccanismi di protezione che potranno variare in base alla sensibilità delle informazioni stesse.
Laddove ritenuto necessario, potranno essere usati specifici meccanismi crittografici. Le chiavi di cifratura utilizzate devono essere adeguatamente protette da modifiche, accessi non autorizzati, distruzione e perdita, mentre gli eventuali apparati impiegati per la loro generazione, memorizzazione e archiviazione devono essere fisicamente protetti da eventuali azioni fraudolente.

i. Sicurezza dei files di sistema

Deve essere garantito il controllo degli accessi ai file di sistema ed ai codici sorgente dei programmi la cui proprietà intellettuale è della Forza Armata e comunque laddove ciò sia possibile. Tale accesso deve essere limitato al solo personale tecnico responsabile. L'installazione degli aggiornamenti del software e delle applicazioni dovrà essere effettuata esclusivamente da parte degli amministratori e dal personale preposto al fine di minimizzare il rischio di danneggiamento dei suddetti sistemi.

j. Sicurezza dei processi di sviluppo e di manutenzione

Per garantire la sicurezza dei programmi applicativi e delle informazioni, occorre assicurare lo stretto controllo delle attività di sviluppo e di manutenzione mediante:

- procedure per il controllo delle modifiche effettuate, valutando l'impatto che si avrebbe sulle applicazioni stesse, sull'ambiente di elaborazione che ospita l'applicazione ed eventuali ripercussioni su sistemi ad essi collegati;
- revisioni tecniche delle applicazioni in seguito a modifica dell'ambiente operativo, ottenute tramite verifiche mirate alla rilevazione di possibili malfunzionamenti;
- un attento controllo delle attività effettuate sui software applicativi e sull'ambiente operativo, tramite il monitoraggio dell'attività svolta dal personale tecnico, la supervisione e la verifica dei software affidati a fornitori esterni.

k. Gestione delle vulnerabilità tecniche

Una efficace attività di aggiornamento presuppone una costante rilevazione delle vulnerabilità presenti sui sistemi impiegati prevedendo tempestive applicazioni di rimedi resi (patch) periodicamente disponibili dalle società fornitrici dei sistemi.

CAPO IV

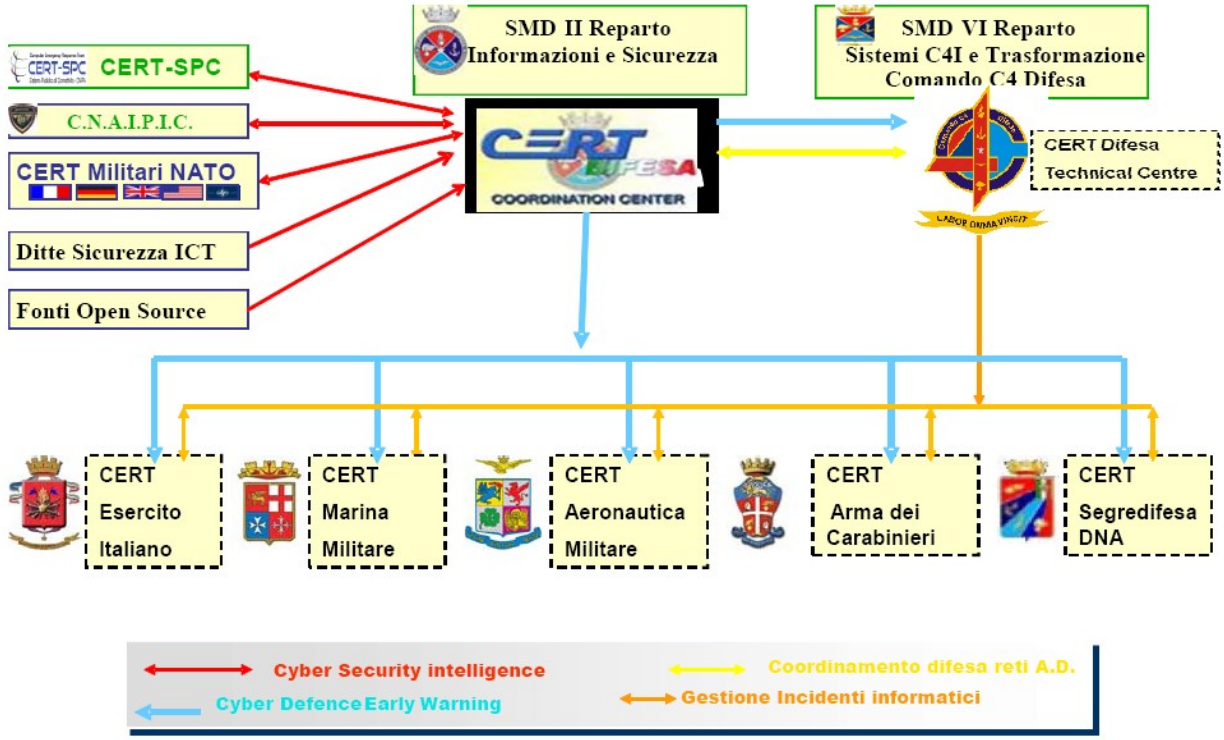
GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA E DELLA CONTINUITA' DEI SERVIZI

Generalità

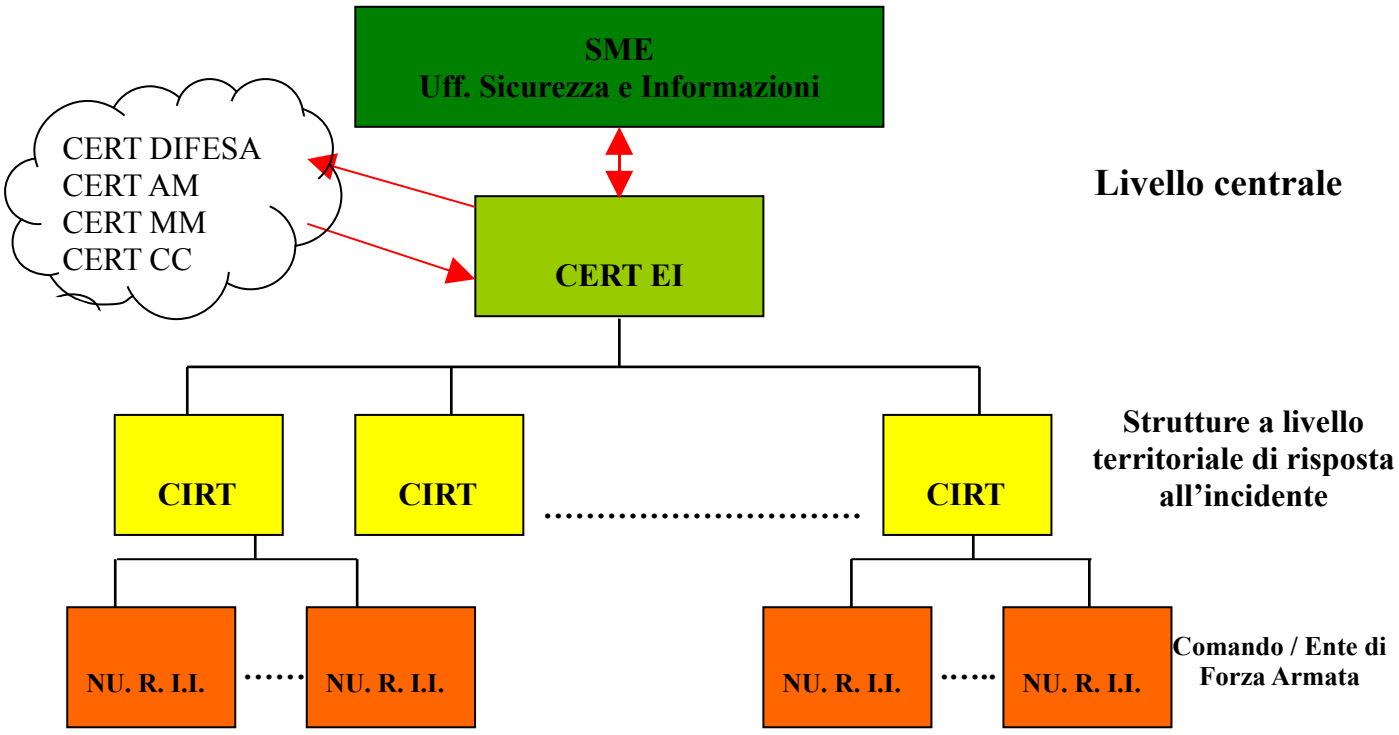
La necessità di dotare anche l'Esercito Italiano di una reale capacità di "Difesa Cibernetica", impone l'avvio della costituzione di una struttura ben definita.

L'organizzazione per gestire gli incidenti di sicurezza informatica e per garantire la continuità dei servizi di Forza Armata si articola su una rete capillare strutturata su tre livelli, secondo il principio della "difesa in profondità":

- il Computer Emergency Response Team, a livello "centrale";
- i Computer Incident Response Team a livello di bacino;
- i NUcleo Risposta Incidenti Informatici presso ciascun E/D/R.



Modello organizzativo di Sicurezza ICT adottato in ambito Difesa



Modello organizzativo di Sicurezza ICT adottato in ambito F.A.

Il CERT Esercito

CERT-Esercito deve essere in grado di rispondere e gestire adeguatamente agli attacchi/incidenti informatici ai sistemi e alle reti della F.A. al pari di quanto già avviene per lo Stato Maggiore della Difesa e in aderenza a quanto previsto dalle direttive SMD-I-013 e SMD-I-019[5].

In generale il CERT-EI ha lo scopo di:

- prevenire gli incidenti informatici;
- minimizzare l'impatto degli incidenti informatici;
- supportare le attività di ripristino.

La struttura in parola, costituita in seno al CoTIE, ha i seguenti compiti di dettaglio:

- emanare bollettini per una efficace prevenzione in merito a minacce telematiche insistenti sulle reti ICT dell'Esercito;
- individuare e definire gli standard di sicurezza ICT da implementare in Forza Armata;
- supportare e fornire consulenza in tema di sicurezza e protezione alle reti ICT della Forza Armata e della Difesa;
- collaborare con i corrispondenti CERT in ambito nazionale, coordinandosi e scambiando informazioni con essi, tenendo informato l'Ufficio Sicurezza e

[5] Rispettivamente "Procedure di risposta agli incidenti informatici riguardanti le reti telematiche della Difesa" e "Politica di Sicurezza per i Sistemi di Telecomunicazione e Informatici non classificati della Difesa".

Informazioni dello SME delle attività più critiche/rilevanti;

- riportare all'Ufficio Sicurezza e Informazioni dello SME ogni evento che possa configurarsi come incidente informatico ovvero ogni evento che possa essere considerato di rilievo ai fini della sicurezza ICT mantenendolo costantemente informato dei successivi sviluppi fino alla "chiusura" dell'incidente;
- verificare, anche mediante l'uso di tools automatizzati, l'implementazione in ambito Forza Armata della politica di sicurezza ICT al fine di una efficace gestione e contenimento degli incidenti riguardanti la rete ed i sistemi ricadenti entro il Dominio di Sicurezza della F.A, ivi comprese le sue estensioni nei Teatri Operativi. A tal fine, tutti gli apparati attivi di rete e le funzionalità di sicurezza (controllo accessi, firewall, router, ecc.) afferenti la EInet sono posti sotto il controllo operativo del CoTIE;
- informare prontamente e mantenere costantemente aggiornato l'Ufficio Sicurezza e Informazioni dello SME in merito a violazioni della politica di sicurezza ICT da parte di E/D/R della Forza Armata. Solo in caso di evidenze che indichino gravi violazioni si potrà procedere a ispezioni "on site" chiedendo, se ritenuto necessario, anche la presenza di personale di Ufficio Sicurezza e Informazioni di SME;
- gestire, controllare e approvare a livello centralizzato il rilascio e l'applicazione degli aggiornamenti di sicurezza (patches) dei sistemi operativi, degli applicativi e del software in uso in Forza Armata;
- censire tutti gli applicativi e il software di Forza Armata definendo la lista dei possibili software da installare sulle postazioni connesse alla EInet;
- svolgere funzioni di supervisione, gestione e coordinamento generale dell'attività di individuazione, contenimento e risposta degli incidenti informatici e mantenere aggiornato l'elenco dei punti di contatto di ogni struttura in ambito Forza Armata preposta alla gestione degli incidenti;
- raccogliere le segnalazioni di scoperta incidente comunicandoli al CERT Difesa;
- mantenere aggiornato un archivio degli incidenti e delle contromisure intraprese per ciascuno di essi.

Gli altri livelli

Come accennato, l'organizzazione per gestire gli incidenti di sicurezza informatica e per garantire la continuità dei servizi di Forza Armata si completa con le seguenti strutture a livello territoriale:

a. il **Computer Incident Response Team** (**CIRT**), istituito presso ciascun Centro Sistemi C4 presente sia sul territorio nazionale sia nei Teatri Operativi, relativamente alle estensioni delle reti di Forza Armata. Al riguardo, si evidenzia che ciascun CIRT è responsabile direttamente della gestione e del contenimento degli incidenti riguardanti la rete ed i sistemi ricadenti entro il proprio bacino di responsabilità, in coordinamento con il CERT EI;
b. il **NUcleo Risposta Incidenti Informatici** (**NU.R.I.I.**), istituito presso ogni E/D/R, si identifica nel team preposto alla gestione dei sistemi informatici/rete dell'E/D/R stesso (Amministratori di Rete/Sistema/Applicativi e personale tecnico) che, di concerto con il Responsabile Operativo Locale di Sicurezza ICT, dovrà essere in grado di gestire, sotto la supervisione e il coordinamento del CERT EI, ovvero del CIRT competente, gli incidenti riguardanti la propria rete di competenza. Al verificarsi di un presumibile incidente informatico il NU.R.I.I. deve informare con tempestività il CIRT competente per territorio ed eventualmente il CERT EI.

Organizzazione del CERT EI

Per poter far fronte alle proprie funzioni, il CERT EI è organizzato in due squadre principali: l'Incident Response Team (IRT) e l'Hardening Team (HT).

Incident Response Team - IRT

Un *Incident Response Team* (IRT) è una squadra specializzata con risorse dedicate e che esegue processi coordinati in caso di emergenza.
L'IRT ha il compito di:

- intervenire in tutti gli incidenti (o presunti tali) utilizzando procedure investigative ufficiali e ben organizzate;
- confermare o escludere rapidamente se si è effettivamente verificato un attacco o un'intrusione;
- valutare il danno o la portata dell'attacco;
- tenere sotto controllo e contenere l'attacco;
- raccogliere e documentare tutte le prove relative all'attacco;
- mantenere la catena di custodia (proteggere le prove dopo averle raccolte);
- mantenere la riservatezza sull'attacco, evitando di diffondere inutilmente notizie che possono ledere l'immagine della Forza Armata,;
- fornire all'E/D/R interessato direttive sulle azioni da svolgere per una pronta risposta all'attacco.

Hardening Team - HT

E' la squadra incaricata di:

- attività di "*vulnerability assessment*" per l'*hardening* dei sistemi in uso presso il Comando/Ente e dei sistemi remoti;
- diffondere le informazioni di sicurezza preventiva inerenti i sistemi in possesso dei Comandi/Enti.

Formazione del personale del CERT

In considerazione del continuo evolversi e mutare della minaccia relativa allo specifico settore, risulta estremamente importante che il personale del CERT sia formato da personale altamente qualificato che gli consenta di guadagnare credibilità e reputazione nell'ambito della comunità informatica della Difesa allo scopo di operare con il massimo rendimento.
E' auspicabile che tutto il personale dell'Hardening Team e dell'Incidente Response Team abbia frequentato, con profitto, specifici corsi, nonché un corso "ad hoc" relativo alle attività del CERT.
Il personale preposto a tale ruolo dovrà, inoltre, essere in possesso almeno dei seguenti *skill*:

- buona conoscenza delle tematiche legate all'IT classica;
- ottima conoscenza di problematiche di *networking*;
- precedenti attività sistemistiche e di *network administration* con adeguata esperienza non inferiore a cinque anni;
- ottime conoscenze delle apparecchiature di sicurezza (*firewall*, IDS, *router*, etc);
- buona conoscenza dei processi di gestione incidenti (*Incident Handling*).

Tutto il personale del CERT potrà essere chiamato a effettuare, come docente, anche corsi sulla Sicurezza ICT.

Procedura per la gestione di un incidente informatico

Di seguito si riportano i principali "*macro step*" che devono essere seguiti per una corretta gestione di un incidente:

Monitoraggio continuo dell'intrusione/danni

In caso di reato, informare immediatamente l'Arma dei Carabinieri per le competenti azioni di Polizia Giudiziaria

Analisi e stima dei danni causati fino a quel momento

Valutazione inferenziale dell'obiettivo finale dell'incidente ("attacco")

Definizione delle misure di contrasto

Attuazione delle misure di contrasto

Ripristino dei sistemi danneggiati

Ripristino globale del sistema

Messa in sicurezza ed esercizio del sistema

CAPO V

LINEE GUIDA PER LA COMPILAZIONE DEL DISCIPLINARE INTERNO PER L'UTILIZZO DEI SERVIZI NON CLASSIFICATI DI POSTA ELETTRONICA ED ACCESSO AD INTERNET

Generalità

La Direttiva 26 maggio 2009, n. 2 con la quale il Dipartimento della Funzione Pubblica della Presidenza del Consiglio dei Ministri interviene in merito all'utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro sancisce che "*Le Pubbliche Amministrazioni, in quanto datori di lavoro, sono tenute ad assicurare la funzionalità ed il corretto impiego degli strumenti ICT da parte dei propri dipendenti, definendone le modalità di utilizzo nell'organizzazione dell'attività lavorativa ed adottando le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informativi*".

In particolare le P.A. nell'esercizio del potere di controllo devono attenersi alle seguenti regole generali:

- rispetto del principio di proporzionalità, che si concreta nella pertinenza e non eccedenza delle attività di controllo. Le limitazioni della libertà e dei diritti individuali devono, infatti, essere proporzionate allo scopo perseguito; è in ogni caso esclusa l'ammissibilità di controlli prolungati, costanti e indiscriminati;
- l'introduzione di tecnologie e di strumenti per il controllo sull'uso della rete e della posta

elettronica deve essere fatto rispettando le procedure di informazione/consultazione delle rappresentanze dei lavoratori previste dai contratti collettivi;
- i lavoratori devono essere preventivamente informati dell'esistenza di dispositivi di controllo atti a raccogliere i dati personali.

Principi di redazione del "Disciplinare Interno"

Il Disciplinare Interno, predisposto dal CoTIE per tutta la Forza Armata e approvato dallo SME, dovrà tener conto sia della vigente normativa in materia di privacy[6], sia della politica di sicurezza inerente l'utilizzo della posta elettronica e di internet.

Il Ministero della Difesa garantisce che il trattamento delle informazioni personali dei propri dipendenti, effettuato per verificare il corretto utilizzo della posta elettronica e di internet, si conforma ai seguenti principi:

- il ***principio di necessità***, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di informazioni personali e di informazioni identificativi in relazione alle finalità perseguite (art. 3 del Codice; par. 5.2 del Provvedimento);
- il ***principio di correttezza***, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 11, comma 1, lett. a, del Codice) poiché le tecnologie dell'informazione, in modo più marcato rispetto ad apparecchiature tradizionali, permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa, anche all'insaputa o, comunque, senza la piena consapevolezza dei lavoratori (par. 3 del Provvedimento);
- il ***principio di pertinenza e non eccedenza*** (par. 6 del Provvedimento), in virtù del quale:
  - i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b) del Codice; par. 4 e 5 del Provvedimento);
  - il datore di lavoro deve trattare le informazioni "nella misura meno invasiva possibile";
  - le attività di monitoraggio devono essere svolte solo da soggetti preposti (par. 8 del Provvedimento) ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione delle informazioni e, se pertinente, del principio di segretezza della corrispondenza" (Parere n. 8/2001 del 13.09.2001, punti 5 e 12).

Informativa sulle modalità di utilizzo di posta elettronica ed internet

I fruitori dei servizi in questione devono essere informati in merito alle modalità consentite di utilizzo di posta elettronica ed internet, attraverso la pubblicazione delle relative politiche in uso, all'interno dei siti intranet dell'Amministrazione.

L'utilizzo del servizio di posta elettronica e di internet nei domini della EInet deve essere disciplinato in conformità alle leggi vigenti e alle ulteriori disposizioni emanate in ambito Difesa.

Il Disciplinare Interno varrà anche come informativa sulle finalità e modalità del trattamento delle informazioni personali, ricavabili dalle attività di controllo tecnico svolte sul servizio di posta elettronica e di internet, ai sensi dell'art. 13 della legge 196/2003.

L'Amministrazione, sulla base delle direttive del Governo tese a promuovere la crescita delle comunicazioni in formato digitale e l'abbattimento di quelle cartacee, considera la posta elettronica e internet strumenti fondamentali, moderni e potenti mezzi di informazione da mettere a disposizione di tutti gli utenti autorizzati.

a. Scopo

Scopo del Disciplinare Interno sarà quello di assicurare che:

[6] D. Lgs. 196/03 "Codice in materia di protezione delle informazioni personali" che disciplina il trattamento effettuato dai soggetti pubblici e Provvedimento del Garante della privacy n° 13 del 01 marzo 2007, pubblicato sulla G.U. - Serie generale n. 58 del 10.03.2007 (indicato come "il Provvedimento")

gli utenti dei servizi di posta elettronica e di accesso ad internet siano informati delle disposizioni di legge vigenti e della giurisprudenza relativa alla disciplina del loro utilizzo;

i servizi di posta elettronica e di accesso ad internet siano utilizzati dagli utenti in conformità a tali disposizioni;

gli utenti dei servizi di posta elettronica e di accesso ad Internet siano informati in merito ai concetti di privacy e di sicurezza applicabili all'uso degli stessi;

i servizi di posta elettronica e di accesso ad internet siano fruibili con la massima continuità ed affidabilità.

b. Destinatari

Il Disciplinare Interno si applicherà a:

tutti i sistemi ed i servizi di posta elettronica e di Internet afferenti il dominio ".esercito.difesa.it";

agli amministratori e fornitori di tali servizi;

tutto il personale, militare e civile, dotato di una casella di posta elettronica, definita nel dominio ".esercito.difesa.it" nonché, autorizzato all'impiego dei servizi Internet;

ogni altra categoria di personale (ad esempio fornitori, consulenti, personale estraneo all'Amministrazione Difesa) cui venga fornito in modo temporaneo un account di posta elettronica e di accesso ai servizi Internet per lo svolgimento delle proprie attività e/o esigenze operative.

c. Condizioni Generali

(a) **Finalità dei servizi di posta elettronica e di Internet.**

Il Ministero della Difesa:

- incoraggia l'uso della posta elettronica per scambiare informazioni, migliorare le comunicazioni, scambiare idee e per rendere più efficaci ed efficienti i processi di lavoro a supporto della missione istituzionale dell'Amministrazione;
- rende disponibile agli utenti autorizzati, per scopi connessi al servizio, l'enorme patrimonio informativo presente sulla rete pubblica Internet costituendo inoltre, un ulteriore canale di comunicazione della A.D. alla stregua delle altre tradizionali modalità di comunicazione informale (telefonia, fax, ecc.).

(b) **Proprietà del Ministero della Difesa**.

I servizi di posta elettronica e di Internet, che vengono erogati tramite l'infrastruttura telematica di Enti dipendenti del Ministero della Difesa sono di proprietà del Ministero della Difesa, pertanto:

- ogni casella di posta elettronica associata al Ministero della Difesa (nel dominio "difesa.it") è di proprietà del Ministero della Difesa;
- l'accesso ai servizio di Internet delle postazioni informatiche è concesso a titolo gratuito ad ogni destinatario.
- sono espressamente vietate qualsiasi altre modalità di collegamento ad internet (cellulare, modem, ecc.) poiché potrebbero compromettere, ovvero aggirare, i meccanismi di sicurezza implementati sulla rete telematica della A.D..

(c) **Limitazioni di Responsabilità per l'Amministrazione**.

L'Amministrazione Difesa non può essere ritenuta responsabile per qualsiasi danno, diretto o indiretto, arrecato agli utenti ovvero a terzi e derivante da:

- eventuale interruzione del Servizio;
- accesso non autorizzato ovvero da alterazione di trasmissioni o informazioni dell'utente.
- messaggi inviati/ricevuti o da transazioni eseguite tramite il servizio di posta elettronica;

- dall'eventuale smarrimento di messaggi diffusi per mezzo del servizio di posta elettronica.

(d) **Restrizioni all'uso del servizio**.

Gli utenti dei servizi di posta elettronica e di Internet sono tenuti ad agire in modo responsabile, ovvero rispettando le leggi, le norme e le procedure dell'Amministrazione Difesa e secondo normali standard di cortesia, correttezza, buona fede e diligenza professionale. L'accesso ai servizi in questione può essere totalmente o parzialmente limitato dall'Amministrazione Difesa senza necessità di assenso da parte dell'utente e anche senza preavviso:

- quando richiesto dalla legge e in conformità ad essa;
- in caso di comprovati motivi che facciano ritenere la violazione delle direttive emanate o delle disposizioni di legge vigenti;
- al venir meno delle condizioni in base alle quali si ha facoltà di utilizzare i servizi (ad es. cessazione per qualsiasi motivo del rapporto di lavoro con l'Amministrazione);
- in casi eccezionali, quando richiesto per esigenze operative critiche e improcrastinabili.
- non deve essere prevista alcuna forma di indennizzo per il venir meno del servizio.

(e) **Assenso e Conformità**.

Prima di ogni ispezione alle registrazioni informatiche e/o alle casella di posta elettronica, l'Amministrazione è tenuta, in generale, ad ottenere l'assenso del titolare, fatta eccezione per quanto disposto al successivo punto (f).

D'altro canto, ci si attende che tutto il personale soddisfi eventuali richieste dell'Amministrazione riguardanti la fornitura di copie delle registrazioni di messaggi di posta elettronica, file e documenti in suo possesso che riguardino le attività lavorative o richieste per soddisfare obblighi di legge, indipendentemente dal fatto che tali registrazioni risiedano o meno su computer di proprietà dell'Amministrazione.

Il mancato rispetto di tali richieste può portare all'applicazione delle condizioni di cui al successivo punto (f).

(f) **Limitazioni all'accesso senza assenso**.

L'Amministrazione Difesa non ispeziona e non accede ai messaggi di posta elettronica dell'utente/titolare senza la sua autorizzazione, tuttavia, tratta le informazioni delle registrazioni (file di log) in forma anonima per l'esecuzione di statistiche sull'utilizzo dei servizi. D'altro canto, l'Amministrazione può permettere l'ispezione, il monitoraggio o l'accesso alla posta elettronica degli utenti, nonché le informazioni personali contenuti nei file di log anche senza l'assenso del titolare, nei seguenti casi:

- su richiesta dell'Autorità Giudiziaria nei casi previsti dalla normativa vigente;
- previo preavviso all'utente, per gravi e comprovati motivi che facciano ritenere che siano state violate le disposizioni di legge vigenti o le direttive dell'Amministrazione Difesa in materia di sicurezza;
- per atti dovuti;
- in situazioni critiche e di emergenza.

(g) **Registro elettronico**.

L'Amministrazione registra e conserva, in forma anonima, le informazioni delle caselle di posta elettronica e dell'utilizzo dei servizi di Internet, tramite scrittura in appositi file di log, delle seguenti informazioni minime (da acquisire e conservare in forma dissociata):

- posta elettronica:
  - mittente del messaggio;

- destinatario/i;
- giorno ed ora dell'invio;
- esito dell'invio.

– accesso ai servizi di Internet:
  - identificativo utente;
  - indirizzo IP (dinamico o statico) associato all'utente;
  - U.R.L. (Uniform Resource Locator) dei siti web visitati;
  - giorno ed ora del log-in e del log-off di accesso al servizio internet.

I file di registro devono essere conservati per un periodo di almeno **un anno** presso l'Ente che fornisce i servizi.

d. Avvertenze

Gli utenti dei servizi di posta elettronica e di internet sono avvisati del fatto che:

(a) la natura stessa della posta elettronica la rende meno sicura di quanto si possa immaginare. Ad esempio, i messaggi di posta elettronica spediti ad una persona possono essere facilmente inoltrati successivamente ad altri destinatari. Gli utenti pertanto devono esercitare la massima cautela nell'uso della posta elettronica per comunicare informazioni private o informazioni sensibili;

(b) la natura stessa di Internet, intesa come "rete mondiale" la rende meno sicura di quanto si possa immaginare. Ne consegue che, nonostante i meccanismi di sicurezza implementati sull'infrastruttura della Difesa possano comunque verificarsi problematiche a livello applicativo con alcuni siti e servizi Internet malevoli (bug del browser web, phishing, pharming, file infetti, ecc.). Gli utenti pertanto devono esercitare la massima cautela nell'uso di Internet durante l'utilizzo, evitando la navigazione in siti di dubbio contenuto.

(c) I messaggi di posta elettronica, la cronologia ed i contenuti dei siti web visitati, creati e conservati sia su apparati elettronici forniti dall'Amministrazione che su altri sistemi, possono costituire registrazioni di attività svolte dall'utente nell'espletamento delle sue attività lavorative. E' possibile quindi che venga richiesto di accedere ai contenuti dei messaggi per un eventuale utilizzo nell'ambito di contenziosi che coinvolgano l'Amministrazione. L'Amministrazione non darà corso automaticamente a tutte le richieste di accesso, ma le valuterà in relazione a precisi obblighi di legge quali la privacy ed altre normative applicabili. Gli utenti devono però tener presente che, per quanto detto, in nessun caso l'Amministrazione può garantire che non saranno accedute informazioni personali degli utenti residenti sui sistemi dell'Amministrazione.

(d) L'Amministrazione, non può e non intende porsi come valutatore dei contenuti dei messaggi di mail scambiati e/o nell'utilizzo della risorsa internet, né può proteggere gli utenti dalla ricezione di informazioni che possano essere considerate offensive. Gli utenti devono comunque attenersi a norme di comportamento non contrastanti con i principi etici e morali che contraddistinguono gli appartenenti all'Amministrazione. Inoltre, tutte le azioni intraprese con tale servizio non devono assolutamente costituire una minaccia per le risorse e servizi disponibili sulle reti della Difesa dal punto di vista dell'integrità e disponibilità.

(e) Non c'è garanzia, a meno di utilizzare sistemi di posta certificata (firma digitale – Carta Multiservizi Difesa ed altre Infrastrutture a Chiave Pubblica – P.K.I formalmente riconosciute), che i messaggi ricevuti provengano effettivamente dal mittente previsto, poiché è piuttosto semplice per i mittenti mascherare la propria identità, anche se ciò costituisce, tra le altre cose, una violazione del Disciplinare Interno stesso. Inoltre i messaggi di posta che arrivano come "inoltro" di precedenti messaggi, potrebbero essere stati modificati rispetto all'originale. Pertanto, in caso di dubbi, chi riceve un messaggio di posta elettronica è tenuto a verificare con il mittente l'autenticità delle informazioni ricevute.

(f) Il software installato sui sistemi connessi alle reti della Difesa deve essere obbligatoriamente in regola con la normativa inerente la "Tutela giuridica del Software" e conforme alle direttive emanate in materia dall'Amministrazione Difesa. E' pertanto espressamente vietato scaricare/condividere/installare software non espressamente autorizzato.

e. Uso consentito

L'uso dei servizi di posta elettronica e di Internet dell'Amministrazione Difesa è soggetto alle seguenti condizioni:

(a) Uso Personale

L'Amministrazione Difesa mette a disposizioni i servizi in parola quale ausilio in termini di efficienza ed efficacia allo svolgimento delle proprie attività lavorative. Tuttavia, in aderenza a quanto stabilito dalla Direttiva n. 2 del Dipartimento della Funzione Pubblica in materia di *Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro* (26 maggio 2009), "*l'utilizzo di internet per svolgere attività che non rientrano tra i compiti istituzionali può essere regolamentato e, quindi, consentito agli utenti per assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro (ad esempio per effettuare adempimenti "on line" nei confronti della P.A. e di concessionari di servizi pubblici, ovvero per tenere i contatti con istituti bancari e assicurativi)*". Tale utilizzo non dovrà essere causa, diretta o indiretta di disservizi dei sistemi elaborativi dell'Amministrazione (spam, phishing, virus, ecc.) e dovrà avvenire in aderenza alla normativa nazionale, della Difesa, della presente policy e alle direttive applicative.

Si rammenta, comunque, che tale uso deve essere limitato al minimo indispensabile e comunque nei limiti del rispetto di criteri di buon senso, onde non contravvenire alle disposizione dell'art. 314 c.p. il quale, oltre a tutelare il patrimonio della pubblica Amministrazione, mira ad assicurare anche il corretto andamento degli uffici sulla base di un rapporto di fiducia e di lealtà con il personale dipendente.

E' facoltà dell'utente e comunque nei limiti del rispetto del corretto utilizzo degli strumenti di lavoro a disposizione, utilizzare un proprio indirizzo elettronico (e-mail personale) presso sistemi esterni all'Amministrazione consultabili tramite Internet. L'utilizzo di tale strumento è consentito entro tollerabili limiti temporali.

(b) Proibizioni

Fermo restando quanto stabilito al para. precedente, è fatto divieto a tutti gli utenti di utilizzare i servizi di posta elettronica e di Internet per scopi di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di attività che possa arrecare danno all'Amministrazione Difesa. E' inoltre vietato l'uso del servizio di posta elettronica per propagare messaggi che inducano il destinatario a produrre altre copie da spedire, a propria volta, a nuovi destinatari (c.d. email "bufala" o "catene di San Antonio"), per la partecipazione a dibattiti, forum o mailing list, a scopi commerciali o di profitto personale e per attività illegali e la fornitura a qualsiasi titolo, di qualunque lista o elenco degli utenti del servizio. E' proibito fornire le proprie credenziali di accesso a sistemi o procedure, così come rispondere a messaggi e-mail che facciano richiesta di questo tipo di informazioni. Chiunque riceva comunicazioni della natura sopra indicata dovrà segnalarlo al CERT EI, attraverso il NURII di appartenenza, per le azioni di competenza.

f. Sicurezza e riservatezza

Oltre a quanto indicato al precedente punto d., gli utenti devono tener presente che, nell'assolvimento dei propri compiti, il personale che gestisce i sistemi di elaborazione e le reti di telecomunicazione può avere, saltuariamente, la necessità di analizzare le informazioni transazionali (database) dei messaggi di posta nonché dei file di log. per

garantire il corretto funzionamento del servizio e in queste occasioni è possibile che avvengano inavvertitamente accessi al contenuto stesso. Tale personale è tenuto comunque al rispetto di stretti vincoli di riservatezza qualora si verificassero i casi citati.

g. Violazioni

Ferme restando le responsabilità individuali di tipo civile e penale verso terze parti offese, colui che contravviene alle norme di sicurezza potrà essere oggetto, nei limiti previsti dalla legge, di azioni di accertamento delle responsabilità ed, eventualmente, delle conseguenti sanzioni.

Responsabilità del Titolare

Il Titolare del Comando/Ente è tenuto a:

- accertarsi che l'utente, prima di essere autorizzato ad usufruire di tali servizi, abbia preso conoscenza della presente direttiva di sicurezza oltre ad essere indottrinato sull'uso della rete;
- farsi coadiuvare dal Responsabile/Incaricato del trattamento informazioni così come previsto dal Disciplinare Interno che ogni Comando/Ente è tenuto a produrre ed aggiornare annualmente, per assicurare la protezione dei dati a norma di legge.

Misure di tipo organizzativo

Ogni E/D/R responsabile della gestione di sistemi informatici deve provvedere ad un'attenta valutazione dell'impatto dei controlli implementati sui diritti degli utenti riguardo le procedure attuate. Sul punto specifico, per ciò che riguarda le tipologie di utenti cui è accordato l'utilizzo dei servizi di posta elettronica e di Internet, si rinvia alle politiche sopra riportate.

In riferimento a quanto prescritto dal Provvedimento circa l'individuazione dell'ubicazione riservata alle postazioni di lavoro, al fine di ridurre il rischio di impieghi abusivi, si specifica che ogni dipendente riceve indicazione della postazione di lavoro a lui assegnata al momento dell'incarico, ovvero in caso di cambiamento della propria posizione. L'accesso a tali postazioni è protetto tramite sistema di autenticazione che richiede l'immissione di un apposito codice utente e della relativa *password*.

Misure di tipo tecnologico

a. **"Navigazione" in internet**

Con riguardo alla "navigazione" in internet, il CoTIE, in qualità di Autorità operativa responsabile della EInet, al fine di ridurre il rischio di usi impropri della rete (ovvero quegli usi consistenti in attività non correlate alla prestazione lavorativa quali, a titolo esemplificativo, la visione di siti non pertinenti, l'upload o il download di file, l'uso di servizi di rete con finalità ludiche o, comunque, estranee alle proprie mansioni), deve adottare tutte le misure tese al rigoroso rispetto delle politiche di sicurezza della Forza Armata.

In particolare, sono raccomandate l'adozione di misure di tipo tecnologico finalizzate:

- all'individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- alla predisposizione di liste di siti indesiderati (c.d. "*black list"*);
- alla configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni non correlate all'attività lavorativa (quali a titolo esemplificativo e non esaustivo l'upload, il download di file o software aventi particolari caratteristiche dimensionali o di tipologia di informazione, l'accesso ai siti inseriti nella *black list*);
- al trattamento di informazioni in forma anonima;
- alla conservazione nel tempo delle informazioni per il periodo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza ovvero in

adempimento di obblighi previsti dalla legge.

b. Posta elettronica

Al fine di adattare le esigenze di corretto ed ordinato svolgimento della vita lavorativa e di prevenzione di inutili intrusioni nella sfera personale dei lavoratori e di violazioni della segretezza della corrispondenza, è opportuno che il CoTIE espliciti regole e strumenti per l'utilizzo della posta elettronica.

Ciò consente, infatti, di evitare, ovvero almeno limitare, l'insorgere di difficoltà in ordine all'utilizzo della posta elettronica poiché, per la configurazione stessa dell'indirizzo e-mail, nei singoli casi, può risultare dubbio se l'utente, in qualità di destinatario o mittente, utilizzi la posta operando quale espressione dell'Amministrazione o ne faccia, invece, un uso personale pur restando nell'ambito lavorativo istituzionale

Pertanto, il CoTIE, preso atto della circostanza che il contenuto dei messaggi di posta elettronica, come pure le informazioni esteriori delle comunicazioni ed i file allegati, riguardano forme di corrispondenza assistite da garanzia di segretezza tutelate anche costituzionalmente, la cui ratio risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali (artt. 2 e 15 Cost.; Corte Cost. 17 luglio 1998, n. 281 e 11 Marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell'Amministrazione digitale), deve esplicitare nelle norme di utilizzo della posta elettronica il grado di confidenzialità che il lavoratore può legittimamente aspettarsi nell'uso di tale strumento. L'Amministrazione considera la posta elettronica uno strumento fondamentale di lavoro per tutti gli utenti, ai quali viene assegnata una casella nominativa per lo svolgimento delle proprie attività da parte della FA.

Per tale categoria di utenti, nel rispetto dei già citati principi di pertinenza e non eccedenza (par. 6 del Provvedimento), nonché per contemperare le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei dipendenti, al CoTIE è demandata l'adozione delle seguenti soluzioni:

- predisposizione di indirizzi di posta elettronica afferenti all'unità organizzativa di appartenenza e/o condivisi tra più utenti affiancandoli a quelli individuali;
- messa a disposizione di ciascun utente di un software di gestione di posta elettronica e Personal Information Management, dotato di apposite funzionalità facilmente utilizzabili che permettono di inviare automaticamente, in caso di assenze programmate (per licenza/ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" elettroniche e/o telefoniche di un altro soggetto ovvero altre utili modalità di contatto dell'ufficio/unità organizzativa;
- procedura per l'accesso di emergenza alla casella di posta elettronica dell'utente, su richiesta del Responsabile Operativo locale della Sicurezza ICT, previa autorizzazione del Titolare del trattamento delle informazioni personali, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa.

Trattamenti esclusi

In ottemperanza a quanto previsto dalla normativa nazionale in materia di tutela della privacy, l'Ente della Forza Armata fornitore dei servizi non deve effettuare controlli prolungati, costanti o indiscriminati circa l'uso dei servizi di internet e posta elettronica da parte degli utenti. Inoltre, non deve effettuare, in nessun modo ed in nessun caso, trattamenti di informazioni personali mediante sistemi hardware e software che mirino al controllo a distanza degli utenti e che vengano svolti tramite i seguenti mezzi:

- lettura e registrazione sistematica dei messaggi di posta elettronica degli utenti ovvero dei relativi dati, al di là di quanto tecnicamente necessario per fornire il servizio di posta elettronica;
- riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dall'utente;

- lettura e registrazione dei caratteri inseriti dall'utente tramite la tastiera ovvero dispositivi analoghi a quello descritto;
- analisi occulta dei dispositivi per l'accesso ad internet o l'uso della posta elettronica messi a disposizione degli utenti.

Monitoraggio e controlli

La FA, si avvale di sistemi di controllo che hanno la finalità di acquisire informazioni statistiche sull'uso dei servizi telematici e garantire inoltre la sicurezza nel trattamento delle informazioni e dell'uso della dotazione informatica e pertanto, non mirano ad un controllo a distanza degli utenti.

Le attività sull'uso del servizio di accesso ad internet vengono automaticamente registrate in forma elettronica nel rispetto delle disposizioni di legge in materia e cancellate dopo 12 mesi.

Il trattamento delle informazioni contenuti nei log può avvenire esclusivamente in forma anonima in modo tale da precludere l'identificazione degli utenti e/o delle loro attività.

I dati anonimi non aggregati, riferibili all'intera struttura o a sue aree, sono mantenute presso l'Ente fornitore dei servizi e possono riguardare:

- per ciascun sito/dominio visitato le seguenti informazioni:
  - il numero di utenti che lo visitano;
  - il numero delle relative pagine richieste;
  - la quantità di dati scaricati;
- per ciascun utente le seguenti informazioni:
  - il numero di siti visitati;
  - la quantità totale di informazioni scaricate;
  - le postazioni di lavoro utilizzate per la navigazione.

I predetti controlli possono essere svolti nelle seguenti modalità in forma graduata da parte dell'Ente fornitore dei servizi:

(1) in via preliminare, si provvederà ad eseguire dei controlli su dati non aggregati, riferiti all'intera struttura della rete di competenza, ovvero a sue aree e dunque ad un controllo anonimo che si concluderà con un avviso generalizzato inerente l'eventuale utilizzo anomalo degli strumenti informatici;
(2) in assenza di successive anomalie non si effettueranno controlli su base individuale;
(3) nel perdurare delle anomalie si procederà all'aggregazione dei dati per controlli su base individuale o per postazioni di lavoro;
(4) in caso di abusi singoli e reiterati si procederà all'invio di avvisi individuali e si eseguiranno controlli nominativi o su singoli dispositivi e/o postazioni di lavoro;
(5) in caso di riscontrato e reiterato uso non conforme delle risorse informatiche sarà effettuata una segnalazione formale di tale comportamento al Titolare dell'Ente/Ufficio di appartenenza dell'utente per le conseguenti sanzioni.

CAPO VI

CONFORMITA' ALLA NORMATIVA

Generalità

La Forza Armata intende assumere una posizione di salvaguardia verso il proprio patrimonio informativo.

Tutti i soggetti autorizzati all'accesso e/o all'uso di risorse ICT sono tenuti ad utilizzarle per le attività istituzionali o derivanti da convenzioni o accordi approvati, purché l'utilizzo sia lecito, rispetti la policy di sicurezza e non sia in contrasto con la normale attività lavorativa e nel

rispetto del Regolamento di Disciplina.

L'accesso e/o l'impiego delle risorse ICT, deve essere effettuato secondo le modalità tecniche, le prescrizioni di sicurezza e le risorse tecnologiche messe a disposizione dall'Amministrazione Difesa.

In particolare deve essere sempre garantita la conformità:

al Codice in materia di protezione delle informazioni personali, come previsto con l'entrata in vigore del predetto Codice, e la conseguente attuazione delle misure minime descritte dall'Allegato B del D. Lgs. 196/2003 "Disciplinare tecnico in materia di misure minime di sicurezza";

alle norme di tutela del diritto d'autore, ed in particolare al divieto di download di file musicali o video che scaricati da internet consentono una vera e propria attività di commercio al limite della legalità.

L'approvazione, in ambito comunitario, della Direttiva sul Diritto di Autore e dei diritti connessi nella società dell'Informazione (2001/29) è un atto legislativo a cui adeguarsi per riaffermare il principio del diritto d'autore anche nell'ambito delle nuove realtà tecnologiche.

Riferimenti normativi

Costituisce parte integrante della presente policy di sicurezza ICT, tutta la normativa nazionale di riferimento vigente in materia. In particolare:

Direttiva SMD – I – 013 "Procedure di risposta agli incidenti informatici riguardanti le reti telematiche della Difesa";

Direttiva SMD – I – 019 "Politica di Sicurezza per i sistemi di telecomunicazione informatici non classificati della Difesa";

Direttiva SMD – I – 020 "Direttiva per l'attuazione delle disposizioni del Dirigente Generale Responsabile per i Sistemi Informativi dell'Amministrazione della Difesa (D.G.Re.S.I.A.D.) in aderenza alle politiche governative in materia di informatizzazione della P.A. e norme applicative in materia di dati personali" (Edizione 2009);

Garante privacy - Parere 8/2001 sul trattamento di informazioni personali nell'ambito dei rapporti di lavoro – adottato il 13 settembre 2001;

Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione delle informazioni personali;

Provvedimento del Garante della privacy del 2 febbraio 2006 – "Internet: proporzionalità nei controlli effettuati dal datore di lavoro"

Provvedimento generale del Garante della privacy n° 13 del 1 marzo 2007 (G.U. – Serie Generale n° 58 del 10 marzo 2007;

Provvedimento generale del Garante della privacy del 17 gennaio 2008 – Sicurezza delle informazioni di traffico telefonico e telematico (G.U. n° 30 del 5 febbraio 2008);

Provvedimento generale del Garante della privacy del 24 luglio 2008 – Recepimento normativo in tema di informazioni di traffico telefonico e telematico (G.U. n° 189 del 13 agosto 2008);

Decreto legislativo n° 159 del 4 aprile 2006 "Codice dell'Amministrazione digitale" – (G.U. del 29 aprile 2006, n. 99 - SO n. 105);

Direttiva 26 maggio 2009, n. 2 del Dipartimento della Funzione Pubblica in materia di Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro.

ALLEGATO 1

VALUTAZIONE DEL LIVELLO DI SICUREZZA

Note sul questionario di Auto - diagnosi

- Il questionario ha lo scopo di guidare ciascun Ente/Distaccamento/Reparto nel processo di auto-valutazione del proprio livello di sicurezza, rispetto alla base minima raccomandata.

- I risultati dell'auto-valutazione sono *proprietà riservata* dell'AD, la quale é libera di decidere come utilizzarli.

- Il questionario é stato impostato al fine di consentire un processo operativo affidabile e rapido

  A tale scopo sono state definite cinque schede, una per ciascuna delle aree chiave della sicurezza: Policy, Ruoli e Responsabilità, Norme e Procedure, Amministrazione della Sicurezza, Formazione e Sensibilizzazione.

PROCEDURA DI AUTOVALUTAZIONE

Al fine di accertare l'adeguatezza del livello di sicurezza informatico dell'Ente/Distaccamento/Reparto si raccomanda di seguire le istruzioni riportate a seguito in maniera sequenziale:

1. Rispondere a tutti i punti del questionario prima di aver visionato la tabella punteggi.
2. Utilizzando la "Tabella Punteggi" riempire la colonna risultati con i punteggi relativi ad ogni risposta data.
3. Sommare i risultati trascritti per settore riportando il totale nella riga "Punteggio Totale".
4. Valutare il risultato di settore utilizzando la tabella "Valutazione di Sicurezza".

Policy di Sicurezza			
Item	Domanda	Risposta	
1	E' stato redatto il Documento Programmatico di Sicurezza (DPS)?	si	
		no	
2	Il DPS è aggiornato annualmente?	si	
		no	
3	La presente direttiva di F.A. (SME INFOSEC 001) è conosciuta da tutto il personale dell'EDR?	si	
		no	
4	Sono stati predisposti i piani per assicurare la continuità e il ripristino dei sistemi ICT critici dell'EDR?	si	
		no	
Ruoli e Responsabilità			
Item	Domanda	Risposta	
5	E' stato nominato il Responsabile Operativo Locale per la Sicurezza ICT?	si	
		no	
6	Sono stati nominati l'Amministratore di rete e l'Amministratore di sistema/applicativo?	si	
		no	
7	Le figure citate agli item 5 e 6 conoscono le proprie responsabilità e i propri compiti?	si	
		no	
8	Le resposabilità ed i compiti loro assegnati vengono assolti regolarmente?	si	
		no	
Norme e Procedure			
Item	Domanda	Risposta	
9	E' stata effettuata la classificazione delle risorse ICT, come previsto dalla presente Direttiva?	si	
		no	
10	Le prescrizioni di sicurezza ICT sono sempre correttamente effettuate?	si	
		no	
11	E' stata definita e implementata una politica di controllo degli accessi tramite account e password univoche per ciascun utente?	si	
		no	
12	L'accesso ad internet di qualsiasi postazione dell'AD avviene esclusivamente attraverso i proxy server individuati dal CoTIE?	si	
		no	
13	Viene effettuato con continuità la gestione delle vulnerabilità tecniche dei sistemi critici (aggiornamento dei sistemi anti virus, patch di sistema ecc.)	si	
		no	

Amministrazione della sicurezza			
Item	Domanda	Risposta	
14	Le figure costituenti l'organizzazione interna di sicurezza ICT dell'EDR (Resp. Op. Loc. per la Sicurezza, Ammi. di rete/sistema..) sono state selezionate secondo i criteri di affidabilità e capacità	si	
		no	
15	E' garantità la disponibilità di personale opportunamente addestrato per la gestione della sicurezza informatica e dei sistemi e servizi ICT dell'EDR?	si	
		no	
16	La possibilità di sostituire con efficacia l'amministratore di rete/sistema, in caso di necessità, è costantemente garantita?	si	
		no	
17	Viene effettuata la periodica attività esercitativa per la verifica di efficienza dei piani per assicurare la continuità e il ripristino dei servizi critici dell'EDR?	si	
		no	
Sensibilizzazione e Formazione			
Item	Domanda	Risposta	
18	Viene periodicamente effettuata un'attività di sensibilizzazionedi tutto il personale in merito al rispetto della politica di sicurezza ICT di F.A.?	si	
		no	
19	Il personale dirigente, gli amministratori di sistema/rete vengono formati dal punto di vista della sicurezza per adempiere efficientemente ai loro compiti?	si	
		no	
20	La consapevolezza sull'importanza della sicurezza ICT è sufficientemente diffusa all'interno dell'EDR?	si	
		no	
21	Le modalità di segnalazione degli incidenti informatici sono note a tutto il personale dell'EDR?	si	
		no	

Schema di Autovalutazione: Tabella Punteggi

Settore	Domanda	Risposta	Punti	Risultato
POLICY DI SICUREZZA	**1**	SI	**3**	
		NO	**0**	
	2	SI	**3**	
		NO	**0**	
	3	SI	**1**	
		NO	**0**	
	4	SI	**3**	
		NO	**0**	
PUNTEGGIO TOTALE				
RUOLI E RESPONSABILITA’	5	SI	3	
		NO	0	
	6	SI	3	
		NO	0	
	7	SI	3	
		NO	0	
	8	SI	1	
		NO	0	
PUNTEGGIO TOTALE				
NORME E PROCEDURE	9	SI	3	
		NO	0	
	10	SI	1	
		NO	0	
	11	SI	3	
		NO	0	
	12	SI	3	
		NO	0	
	13	SI	1	
		NO	0	
PUNTEGGIO TOTALE				
AMMINISTRAZIONE DELLA SICUREZZA	14	SI	3	
		NO	0	
	15	SI	1	
		NO	0	
	16	SI	3	
		NO	0	
	17	SI	3	
		NO	0	
PUNTEGGIO TOTALE				
SENSIBILIZZAZIONE E FORMAZIONE	18	SI	3	
		NO	0	
	19	SI	3	
		NO	0	
	20	SI	1	
		NO	0	
	21	SI	3	
		NO	0	
PUNTEGGIO TOTALE				

Schema di Autovalutazione: Tabella Valutazione di Sicurezza

SETTORE	Punteggio		VALUTAZIONE DELLA SICUREZZA RISULTANTE
	Da	a	
POLICY DI SICUREZZA	0	8	**INADEGUATA**
	9	10	ADEGUATA
RUOLI E RESPONSABILITA'	0	8	**INADEGUATA**
	9	10	ADEGUATA
NORME E PROCEDURE	0	8	**INADEGUATA**
	9	11	ADEGUATA
AMMINISTRAZIONE DELLA SICUREZZA	0	8	**INADEGUATA**
	9	10	ADEGUATA
SENSIBILIZZAZIONE E FORMAZIONE	0	8	**INADEGUATA**
	9	10	ADEGUATA

NOTA

a. Il Risultato a cui ogni ENTE/DISTACCAMENTO/REPARTO deve tendere è una valutazione di "Sicurezza ADEGUATA" in tutti i cinque settori. Il risultato di autovalutazione di "sicurezza INADEGUATA" anche in un solo settore implica la mancata adeguatezza dell'intero ENTE/DISTACCAMENTO/REPARTO.
b. Se il risultato è una valutazione di "**Sicurezza INADEGUATA**" in più di uno dei settori analizzati, il livello di sicurezza informatica dell'ENTE/DISTACCAMENTO/REPARTO deve essere considerato **altamente RISCHIOSO** e devono essere individuate **immediatamente** tutte le azione e misure di sicurezza tese ad adeguare il livello di sicurezza ICT dell'ENTE/DISTACCAMENTO/REPARTO.