

Fonte: Allegato A al Contratto

Rif.	ID	Descrizione Requisito	ID Selex	Inserimenti Selex
Pag. 1	A1	Il SISTRI deve essere in grado di evolvere per seguire cambiamenti organizzativi e procedurali in corso d'opera che richiedano interventi sia sulle componenti hardware che software (di base e applicativo).	SYS-CON-GEN-02001	
	A2	Il SISTRI deve essere realizzato con una struttura modulare integrata, che permetta una facile e graduale apertura della stessa all'introduzione di nuove funzionalità, sia da un punto di vista hardware che software (di base e applicativo).	SYS-CON-GEN-02002	
	A3	Le apparecchiature del Centro Operativo devono essere dotate delle certificazioni aderenti agli standard	SYS-CON-INF-02003	
	A4	Il SISTRI deve garantire l'integrità e l'accessibilità controllata dei documenti attraverso l'implementazione di un idoneo ambiente dotato di supporti fisici di memorizzazione, dei materiali di protezione, delle procedure per il trattamento nonché dei sistemi di memorizzazione, in grado di garantire la conservazione per quattro anni. L'integrità deve essere mantenuta anche dopo un eventuale evento disastroso implementando una soluzione di recupero dei dati	SYS-CON-SEC-02004	
	A5	Il SISTRI deve adottare metriche adeguate per descrivere le informazioni geografiche ed i servizi di informazione relativi all'identificazione, all'estensione degli spazi temporali e spaziali, i relativi riferimenti e la distribuzione degli elementi su base geografica	SYS-CON-FUN-02005	
Pag. 2	A6	L'archivio del SISTRI deve contenere le informazioni complete ed esatte sulle operazioni effettuate relative ai documenti, ivi compresi i processi ed i dati ad essi associati. Tali informazioni sono riportate come dati incorporati associati ai documenti. In aggiunta, esse possono essere registrate e mediante controlli di sistema mantenute almeno finché il documento cui si riferiscono è conservato nell'archivio del SISTRI.	SYS-CON-SEC-02006	
	A7	La metodologia per la gestione dei documenti deve essere aderente alla normativa ISO in termini di qualità.		SYS-CON-SEC-02006 Gestione dei documenti e delle operazioni su di essi
	A8	La conservazione dei documenti deve poter essere svolta anche in luogo diverso dal Centro Operativo, in modo da garantire la conservazione dei dati anche in caso di evento disastroso, mantenendo le responsabilità e la gestione a carico del Centro Operativo.	SYS-CON-SEC-02007 - SYS-INF-GEN-90001	
	A9	Il SISTRI documentale deve garantire l'autenticità, l'affidabilità e l'utilizzabilità dei documenti per tutto il periodo di conservazione, anche a seguito di una qualunque modifica dei servizi, comprese una conversione di formato o una migrazione tra sistemi operativi, hardware o specifiche applicazioni software.	SYS-CON-SEC-02008	
	A10	Il servizio documentale operato attraverso il sistema SISTRI deve fornire il supporto e deve garantire che i processi lavorativi non vengano ostacolati, le procedure e i sistemi di comunicazione devono essere integrati con la gestione dei documenti	SYS-CON-GEN-02009	
	A11	Il SISTRI deve mantenere un alto grado di disponibilità, ridondando gli elementi critici al fine di evitare single point of failure, per garantire l'operatività sette giorni su sette, H24. Il valore di disponibilità minimo richiesto è del 98%.	SYS-CON-INF-02010 - SYS-INF-GEN-02110	
	A12	Il SISTRI deve prevenire l'introduzione dei dati non aventi i requisiti formali e di congruenza richiesti, realizzando un sistema di protezione automatico dei dati nel caso di chiusura anomala della transazione.	SYS-CON-FUN-02011	

Fonte: Allegato A al Contratto

Pag. 3	A13	Il SISTRI deve garantire facilità d'uso delle procedure e della strumentazione attraverso un'interfaccia amichevole dotata di aiuto in linea che suggerisca l'azione in caso di difficoltà e che renda disponibili informazioni di supporto legate al contesto operativo, come normative di legge, (help operativi) facendo uso di tecniche ipertestuali, vocabolari e thesauri.	SYS-CON-FUN-02012	
	A14	Il SISTRI deve mantenere e correlare le informazioni relative a periodi distinti prevedendo sistemi di memorizzazione in archivi digitali basati su tecnologie SAN e CAS	SYS-CON-FUN-02013	
	A15	Il SISTRI dovrà essere progettato per abilitare il "modello di interscambio" al fine di garantire l'erogazione dei servizi specifici del dominio applicativo sia l'interazione, il colloquio e l'interoperabilità con altri sistemi, già esistenti o in via di sviluppo/realizzazione. Deve garantire modalità di accesso via Web agli operatori obbligati ad iscriversi al sistema SISTRI.	SYS-CON-INF-02014	
	A16	Il SISTRI deve prevedere il back up dei dati mediante meccanismi minimi di replica giornaliera. *	SYS-CON-SEC-02015 - SYS-INF-GEN-90001	
	A17	Il SISTRI deve consentire l'accesso selettivo ad utenti con livelli di autorizzazione diversi, prevedendone l'identificazione di tipo forte basata su token USB in dotazione alla utenza, e prevedere la registrazione delle operazioni.	SYS-CON-SEC-02016	
	A18	Deve essere inibito l'uso non autorizzato alle funzionalità applicative nonché l'accesso diretto alle postazioni operative del Centro Operativo con meccanismi di tipo hardware (es. porta con chiave) e/o di tipo software (es. setup iniziale, definizione privilegi utenti).	SYS-CON-SEC-02017	
	A19	Deve essere predisposto il "Piano della Sicurezza", in accordo alle "politiche di sicurezza per i sistemi informatici" adottate a livello di Pubblica Amministrazione.	SYS-CON-SEC-02018	
	A20	Il SISTRI deve adottare tecnologie leader del mercato, che rappresentino uno standard a livello nazionale e internazionale, in modo da facilitare anche lo scambio e l'acquisizione di dati con/da altri Enti.	SYS-CON-GEN-02019	
Pag. 4	A21	L'Ambiente operativo e le banche dati devono essere caratterizzati da Sistemi operativi ed applicazioni user friendly con interfaccia grafica a finestre e data base management system di tipo relazionale (RDBMS), sui quali implementare gli strati applicativi e le interfacce verso l'utente utilizzatore.	SYS-CON-INF-02020	
	A22	Devono essere adottati strumenti e linguaggi tecnologicamente avanzati rispondenti al paradigma OO aperti e avviati a diventare standard consolidati quali la programmazione Object Oriented, di tipo "visuale", l'adozione di middleware standard, XML per il trattamento degli schemi di rappresentazione, *	SYS-CON-GEN-02021	
	A23	La localizzazione GNSS dovrà essere basata sullo standard globale WGS84	SYS-CON-FUN-02022	
		Sono di seguito elencati i requisiti del software applicativo che dovranno essere considerati:	na	
	A24	• modularità e standardizzazione della soluzione per le componenti applicative, nell'ottica della graduale introduzione di nuove funzionalità;	SYS-CON-GEN-02023	
	A25	• completa trasparenza all'utente finale, delle modalità di integrazione e connessione tra dati geografici e alfanumerici associati;	SYS-CON-FUN-02024	
	A26	• scalabilità e portabilità;	SYS-CON-GEN-02025	
	A27	• indipendenza dei programmi dal RDBMS utilizzato;	SYS-CON-FUN-02026	
	A28	• sviluppo basato su ambiente di modellizzazione basato su strumenti CASE;	SYS-CON-GEN-02027	
	A29	• utilizzo di linguaggi di programmazione aderenti a standard ANSI, ISO, IEEE,;	SYS-CON-GEN-02028	

Fonte: Allegato A al Contratto

	A30	• produzione in accordo allo standard ISO/9000;	SYS-CON-GEN-02029	
	A31	• produzione di documentazione tecnica e operativa secondo gli standard di qualità;	SYS-CON-GEN-02029	
Pag. 5	A32	• realizzazione di help su come utilizzare l'applicazione e operativi (legati al contesto applicativo, ad es. relativi alla normativa di legge) che facciano uso di tecniche come ipertesti, gestione thesaurus;	SYS-CON-GEN-02030	
	A33	• interfaccia utente di tipo grafico, che semplifichi al massimo il dialogo con il Sistema, riduca al minimo i tempi di apprendimento e le possibilità di errore connesse all'inserimento di dati, nonché integri perfettamente la componente grafica dei dati con quella descrittiva;	SYS-CON-FUN-02031	
	A34	• gestione delle unità logiche di commit e rollback (logical unit of work), in particolare la gestione dei dati deve avvenire in modo da assicurarne la congruenza e la consistenza (two phase commit o altro);	SYS-CON-FUN-02032	
	A35	• compressione dei messaggi per ridurre il traffico sulla rete	SYS-CON-FUN-02033	
		• uso di crittografia per garantire le opportune condizioni di sicurezza;	SYS-CON-SEC-02034	
	A36	• logging delle applicazioni;	SYS-CON-FUN-02035	
	A37	Registrazione su diversi livelli delle operazioni effettuate da ogni utenza,	SYS-CON-FUN-02035	
	A38	Registrazione dei codici di errore e relativa descrizione, o gestione standardizzata della messaggistica di errore,	SYS-CON-FUN-02035	
	A39	gestione dei codici di ritorno.	SYS-CON-FUN-02036	
Pag. 6		Relativamente alle Banche Dati, l'architettura del SISTRI deve essere definita in modo da consentire:	na	
	A40	• l'inclusione di nuovi schemi dati o aggiornamenti degli esistenti, in modo consistente con quanto già presente nel Sistema;	SYS-CON-GEN-02037	
	A41	• l'export di particolari schemi dati in formati standard di interscambio (ad esempio XML), in modo da condividere esigenze specifiche con altri Enti;	SYS-CON-FUN-02038	
	A42	• l'inserimento di nuovi processori, forniti dagli Enti richiedenti, dedicati ad analisi specifiche e/o ad interpretazione e conoscenza di particolari dati, in modo trasparente per il Progetto SISTRI stesso;	SYS-CON-GEN-02039	
	A43	• all'aggiunta dei suddetti processori deve corrispondere l'aggiornamento di esistenti regole d'uso e/o la definizione di nuove;	SYS-CON-GEN-02039	
	A44	• il supporto di qualunque tipo di piattaforma hardware senza limitazioni al processo;	SYS-CON-GEN-02040	
	A45	• la implementazione di soluzioni per la disponibilità dei dati, la data protection e il fail over;	SYS-CON-SEC-02041 SYS-INF-GEN-90001	
	A46	• la gestione attraverso interfaccia Web;	SYS-CON-FUN-02042	
	A47	• la realizzazione di configurazioni cluster;	SYS-CON-INF-02043	
	A48	• archivi dati nativi con tecnologie di ricerca spaziale basate su standard W3C;	SYS-CON-FUN-02044	
	A49	la realizzazione di procedure di interfaccia basate su SQL e linguaggi di interrogazione	SYS-CON-GEN-02045	

Fonte: Allegato A al Contratto

	A50	Il SISTRI deve fornire le funzioni atte a proteggere dati e le risorse da eventi accidentali o intenzionali, garantendo quanto segue:	na	
	A51	• riservatezza: il dato deve essere disponibile solamente ai processi che lo devono elaborare e all'utilizzatore che ne ha le responsabilità e ne è pertanto legittimato all'utilizzo tramite preventiva autorizzazione da parte del Ministero dell'Ambiente, della Tutela del Territorio e autenticazione;	SYS-CON-SEC-02046	
	A52	• integrità: ogni dato deve essere realmente quello originariamente immesso nel SISTRI ovvero successivamente solo legittimamente modificato;	SYS-CON-SEC-02047	
	A53	• disponibilità: prevenzione dalla impossibilità di utilizzo un'informazione o risorsa, nel caso in cui l'utilizzo sia espressamente autorizzato.	SYS-CON-SEC-02048	
	A54	Lo scopo della sicurezza deve essere quello di abilitare gli accessi ai servizi applicativi secondo il profilo Registrato (identificato ed autorizzato dal Ministero dell'Ambiente, della Tutela del Territorio e del Mare), rendendo disponibili e "sicure" le risorse a chi ne è legittimato all'utilizzo, e non di impedirli.	na	SYS-CON-SEC 16903
Pag. 7	A55	Le misure di sicurezza adottate devono influenzare il meno possibile la flessibilità dell'architettura del SISTRI, potendo costituire dei vincoli architettureali solo in particolari situazioni. La progettazione di tali misure deve:	SYS-CON-SEC-02049	
	A56	• consentire l'evoluzione di quanto realizzato;	SYS-CON-SEC-02049	
	A57	• prevedere la pianificazione delle attività di sensibilizzazione, addestramento, controllo, monitoraggio e aggiornamento a seguito di malfunzionamenti per gli operatori del Centro Operativo;	SYS-CON-SEC-02049	
	A58	• tener conto delle necessarie certificazioni.	SYS-CON-SEC-02049	
	A59	La sicurezza deve essere garantita da misure tecniche (realizzate tramite meccanismi hardware e/o software) di tipo fisico, procedurale o sul personale del Centro Operativo (funzioni di tipo organizzativo e logistico).	SYS-CON-SEC-02049	
	A60	Si deve considerare, quale base minima per la sicurezza, l'adesione alla direttiva del 16 gennaio 2002 del Presidente del Consiglio dei Ministri Dipartimento per l'innovazione e le tecnologie "Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni statali".		SYS-CON-SEC-02050 : ISO27000 e requisiti di legge
	A61	La gestione della sicurezza informativa viene attuata tenendo in considerazione lo standard ISO27000, nell'ambito del quale progettare e mantenere, in modo organico, le suddette misure di sicurezza, di natura tecnica, organizzative e sul personale.	SYS-CON-SEC-02050	
	A62	In tale ambito dovrà essere gestito il Piano della Sicurezza, con aggiornamento almeno annuale.	SYS-CON-SEC-02050	
	A63	Le misure di sicurezza dovranno offrire le specifiche funzionalità atte alla:	SYS-CON-SEC-02050	
	A64	• protezione perimetrale per evitare tentativi di intrusioni,	SYS-CON-SEC-02050	
	A65	• sicurezza dei dati, anche attraverso meccanismi di back up,	SYS-CON-SEC-02050	
	A66	• protezione nella trasmissione dei dati e della proprietà dei documenti,	SYS-CON-SEC-02050	
	A67	• gestione della sicurezza (auditTracciabilità, assegnazione di privilegi e controllo utenti/accessi, backup e ripristino, antivirus).	SYS-CON-SEC-02050	
Pag. 7	A68	Devono essere garantite le necessarie capacità per le seguenti funzioni:	na	
	A69	• Identificazione e Autenticazione: in modo da permettere la verifica dell'identità degli utenti che chiedono l'accesso a risorse del Sistema; oltre al controllo specifico, deve essere garantita l'inclusione e l'eliminazione di utenti dall'elenco di quelli autorizzati ad accedere a determinate risorse del Sistema.	SYS-CON-SEC-02051	

Fonte: Allegato A al Contratto

	A70	* Il controllo di accesso, e in particolare per la scrittura e/o lettura dei documenti deve essere garantito attraverso l'utilizzo di certificati memorizzati su appositi dispositivi di utente (Token USB per le Imprese).	SYS-CON-SEC-02052	
	A71	* Controllo Accessi: in modo da controllare il flusso delle informazioni fra processi e garantire l'uso delle risorse del Sistema da parte dei processi stessi;	SYS-CON-SEC-02053	
	A72	* Accountability: in modo da tener traccia delle azioni effettuate dalle varie entità (utenti o processi) in modo che le conseguenze di tali azioni possano essere addebitate a chi le ha svolte (Prestazioni di Accounting). Le azioni alle quali si fa qui riferimento sono quelle significative dal punto di vista della sicurezza;	SYS-CON-SEC-02054	
	A73	* audit: in modo da registrare e analizzare gli eventi che potrebbero rappresentare una minaccia alla sicurezza allo scopo di individuare eventuali attacchi alla sicurezza del Sistema sulla base delle osservazioni di comportamenti che si scostano dal suo uso abituale;	SYS-CON-SEC-02055	
	A74	* Object reuse: in modo da permettere la riutilizzazione di spazi di memoria centrale o di massa impedendo che questo costituisca una minaccia alla sicurezza, per esempio: la cancellazione o l'inizializzazione di supporti riutilizzabili (dischi, memorie, etc.) quando non sono in uso;	SYS-CON-SEC-02056	
Pag. 9	A75	* Accuracy: in modo da evitare qualunque tipo di modifica illecita dei dati e segnalare, o possibilmente prevenire, alterazioni, cancellazioni e inclusioni di nuove parti nei dati, scambiati tra processi o passati da un oggetto ad un altro;	SYS-CON-SEC-02057	
	A76	* Availability: In modo da assicurare che le risorse siano accessibili e utilizzabili su richiesta da qualsiasi entità autorizzata entro tempi prefissati;	SYS-CON-SEC-02058	
	A77	* data exchange: in modo da garantire la sicurezza dei dati durante la loro trasmissione sui canali di comunicazione previsti, eventualmente anche attraverso opportuni meccanismi di cripting.	SYS-CON-SEC-02059	
	A78	L'accesso ai servizi sarà possibile attraverso il dispositivo Token USB che è di ausilio all'autenticazione forte degli utenti del sistema SISTRI.		SYS-CON-FUN-02073 : Token: funzioni crittografiche
	A79	* Il Token USB del sistema SISTRI è composto da due componenti		SYS-CON-INF-02060 : Token USB del SISTRI
	A80	* Il Token USB del sistema SISTRI è composto da due componenti, la parte Hardware deve essere compatibile con lo standard USB 2.0 e deve essere possibile archiviare la componente software di gestione del sistema SISTRI.	SYS-CON-INF-02060	
	A81	* La componente Hardware del Token USB deve essere provvista di un identificativo seriale che lo rende univoco ed identificabile "Vendor-ID Volum Number Serial number".	SYS-CON-FUN-02061	
	A82	* La componente Software del Token deve essere multiplatforma e deve poter essere eseguita sui sistemi operativi Microsoft Windows XP, Microsoft Windows Vista, Linux,	SYS-CON-FUN-02062	
	A83	* La componente Software del Token USB deve essere realizzata in modo da rendere sicuro l'accesso al sistema SISTRI.	SYS-CON-SEC-02063	
	A84	* Il token USB deve consentire la memorizzazione sicura delle credenziali utente (profili personali, certificati digitali) e dei dati. Gli utenti memorizzati possono essere più di uno.	SYS-CON-FUN-02064	
	A85	* Lo scambio delle informazioni per la verifica di autenticità delle chiavette (serial number, volume number, etc.) deve avvenire in modo sicuro e non devono essere possibile intercettare le informazioni in transito	SYS-CON-SEC-02065	

Fonte: Allegato A al Contratto

	A86	Deve essere realizzato un sistema di gestione in grado di censire tutti i Token e tenere traccia dello stato del singolo componente Token e devono essere gestiti gli stati permettendo la gestione del ciclo di vita dello stesso.	SYS-CON-FUN-02066	
Pag. 10	A87	• Deve essere possibile gestire la configurazione del dispositivo; L'operatore che realizza la configurazione deve avere un profilo autorizzato e deve poter accedere al sistema dove sono stati censiti i Token	SYS-CON-SEC-02067	
	A88	• Il Token deve poter contenere in modo altamente sicuro la coppia di chiavi ed il certificato dell'utente al quale verrà assegnato.	SYS-CON-SEC-02068	
	A89	• Il Token deve poter rendere possibile la memorizzazione di dati sia in chiaro, che di dati in modalità protetta (crittografati), secondo adeguati livelli di sicurezza delle informazioni che devono essere previsti dal sistema SISTRI.	SYS-CON-FUN-02069	
	A90	• Il Token deve avere tutto il software necessario al collegamento con il centro SISTRI a bordo e non deve essere possibile avere i permessi Di super utente quando viene eseguito sul PC ospite.	SYS-CON-SEC-02070	
	A91	• Il Token non deve lasciare traccia all'interno del PC dove viene inserito e devono essere presi gli accorgimenti necessari per evitare che si possano lasciare file all'interno del PC ospite.	SYS-CON-SEC-02071	
	A92	• Il Token deve essere utilizzato al portale, attraverso l'esecuzione manuale di una procedura contenente un menu autoguidato per l'accesso al sistema. Se il token non è collegato al PC non deve essere possibile accedere al sistema SISTRI nella modalità protetta. Non dovranno essere possibili altre utilizzazioni ed ogni file non riconosciuto dal sistema per gli scopi previsti dal sistema dovranno essere eliminati ad ogni connessione al SISTRI.	SYS-CON-SEC-02072	
	A93	• L'accesso al sistema SISTRI deve avvenire mediante funzioni crittografiche che prevedono l'autenticazione forte con dispositivi di firma e certificati installati all'interno del Token stesso e devono essere garantiti gli standard SSI e X.509V3	SYS-CON-FUN-02073	
Pag. 11	A94	• Deve essere possibile gestire centralmente il versioning delle configurazioni e delle versioni software presenti all'interno del Token USB.	SYS-CON-FUN-02074	
	A95	• La gestione ed il rilascio dei certificati deve avvenire secondo gli standard previsti ovvero la generazione della coppia di chiavi deve essere archiviata all'interno del Token.	SYS-CON-SEC-02075	
	A96	• Devono essere predisposti accorgimenti software in grado di garantire la sicurezza della coppia di chiavi depositate all'interno del Token stesso.	SYS-CON-SEC-02076	
	A97	• Il Token implementa la funzionalità PKCS11 le aree di storage del token sono cifrate e gestite interamente. Il token implementa il funzionamento di una SmartcardToken USB e può essere utilizzato dai più comuni applicativi che utilizzano le funzionalità di firma elettronica.	SYS-CON-FUN-02077	
	A98	• Il Token deve esporre le funzionalità più utilizzate dagli applicativi di firma e cifratura, secondo quanto descritto nel documento [RSA01].	SYS-CON-FUN-02078	
	A99	• Le funzioni crittografiche principali necessarie da supportare saranno: General-purpose functions, Slot and Token Management Functions, Session Management Functions, Object Management Functions, Encryption Functions, Decryption Functions, Message Digest Functions, Signing Functions, Functions for Verifying Signatures, Key Management Functions, Random Number Generation Functions.	SYS-CON-FUN-02079	
	A100	La black box è costituita da un contenitore delle dimensioni di circa 15x10x5 cm, che integra al suo interno i seguenti moduli	SYS-CON-FUN 16900	SYS-CON-FUN 16900
	A101	• Ricevitore GPS per la determinazione della posizione del veicolo	SYS-CON-FUN-02080	
Pag. 12	A102	• Modulo di comunicazione dati GPRS per la trasmissione di allarmi da parte dell'utente o per consentire il tracciamento da parte delle Forze dell'Ordine nei casi previsti dalla legge	SYS-CON-FUN-02081	

Fonte: Allegato A al Contratto

	A103	• Modulo di elaborazione basato su processore ARM e sistema operativo linux per la gestione dei dati e delle logiche applicative tra le diverse componenti		SYS-CON-FUN-02082 BB: caratteristiche HW e del SO
	A104	• Modulo di sicurezza costituito da smart card e sw applicativo specifico, finalizzato alla cifratura dei dati ed alla mutua autenticazione tra black box e token USB	SYS-CON-FUN-02083	
	A105	• Modulo di interfaccia con il token USB	SYS-CON-FUN-02084	
	A106	• Batteria Tampone per consentire l'alimentazione della black box in caso di assenza di alimentazione del veicolo	SYS-CON-FUN-02085	
	A107	• Memoria locale per consentire la memorizzazione dei dati di posizione e allarmi prima del trasferimento sul token USB a fine percorso	SYS-CON-FUN-02086	
	A108	Inoltre separati dalla black box ma ad essa collegati con cavi sono presenti i seguenti moduli	SYS-CON-FUN-02087	
	A109	• Antenna GPS	SYS-CON-FUN-02087	
	A110	• Antenna GPRS	SYS-CON-FUN-02087	
	A111	• Pulsante di allarme	SYS-CON-FUN-02087	
	A112	Gli utenti con i mezzi di trasporto, come previsti dal SISTRI, dovranno equipaggiare ogni mezzo con una Black Box le cui specifiche in dettaglio sono riportate di seguito.	na	
	A113	• La Black Box deve rispettare il requisito di Tamper-Proof / Tamperevident in modo da rendere evidente il fatto che la Black-Box sia stata aperta.	SYS-CON-FUN-02088	
Pag. 13	A114	• La Black Box deve rispettare l'aderenza alle normative Comunitarie (CE) e deve essere condotta secondo le norme previste e queste devono sfociare nella certificazione CE.	SYS-CON-GEN-02089	
	A115	• La Black Box deve essere collegata ad un pulsante di panico che preveda l'invio di una segnalazione al centro operativo indicando le coordinate geografiche della posizione del mezzo.	SYS-CON-FUN-02090	
	A116	• La Black Box deve rispondere a dei meccanismi di sicurezza sui dati in transito mediante un modello crittografico utilizzando lo standard RSA, coppie di chiavi e l'utilizzo di certificati digitali da installare all'interno delle SMART-CARD presente all'interno della Black Box.	SYS-CON-SEC-02091	
	A117	• La generazione dei certificati deve essere prevista secondo le specifiche dallo standard operativo previsto dalla PKI del centro SISTRI.	SYS-CON-SEC-02092	
	A118	• La Black Box deve essere identificata da un numero seriale che permette di riconoscere in modo univoco la componente Hardware.	SYS-CON-FUN-02093	
	A119	Sulla Black Box deve essere predisposta una porta USB in grado di accogliere i Token del SISTRI per il trasferimento dei dati.	SYS-CON-FUN-02094	
	A120	Il trasferimento delle informazioni tra la Black Box ed il centro SISTRI deve avvenire tramite la porta USB in grado di accogliere i Token del SISTRI per il trasferimento dei dati.	SYS-CON-FUN-02094	
	A121	Inoltre, deve essere prevista una funzione di aggiornamento del software presente all'interno della Black Box.	SYS-CON-FUN 16901	SYS-CON-FUN 16901
	A122	Le funzioni della Black Box sono le seguenti:	na	
	A123	• deve archiviare tutti i dati di posizione rilevati dal GPS in un file ciclico in grado di permettere che siano reperiti in occasioni di richieste.	SYS-CON-FUN-02095	
	A124	• deve fornire satelliti utilizzati per il fix e la lista dei satelliti in visibilità.	SYS-CON-FUN-02096	

Fonte: Allegato A al Contratto

	A125	• deve essere memorizzato con cadenza configurabile (es. 1 sec. ... 30 sec.) l'intervallo temporale dei dati raccolti dal GPS	SYS-CON-FUN-02096	
	A126	• deve prevedere una modalità di funzionamento " non in servizio". Questa funzionalità è ad uso delle officine.	SYS-CON-FUN-02097	
Pag. 14	A127	Il ricevitore GPS presente all'interno della BB dovrà essere appositamente configurato in modo da produrre il riferimento temporale ed i dati di posizionamento in formato NMEA-0183 ed in modalità configurabile.	SYS-CON-FUN-02080	
	A128	Il comunicatore della Black Box deve essere basato su tecnologia GPRS.		SYS-CON-FUN-02081 BB: comunicazione GPRS
	A129	Le funzionalità in assenza di alimentazione saranno garantite per minimo 10 minuti attraverso la batteria interna per consentire il salvataggio degli ultimi dati registrati.	SYS-CON-FUN-02098	
	A130	La Black Box deve rispettare il requisito di resistenza alle povere secondo quanto previsto dallo standard IP 54. I requisiti di alimentazione della Black Box devono prevedere il funzionamento sia a 12 Volt che a 24 Volt.	SYS-CON-FUN-02098	
	A131	La soluzione di monitoraggio dei siti sensibili dovrà prevedere l'installazione di due telecamere in corrispondenza dei varchi di transito dei siti, in maniera tale da consentire la ripresa della targa anteriore e di quella posteriore dei veicoli	SYS-CON-GEN-02099	
		La soluzione dovrà comporsi di:	na	
	A132	• Sottosistemi Periferici installati sul territorio;	SYS-CON-GEN-02099	
	A133	• Sottosistema Centrale installato presso un Centro di gestione;	SYS-CON-GEN-02099	
	A134	• Una infrastruttura di comunicazione.	SYS-CON-GEN-02099	
	A135	I "Sottosistemi Periferici" dovranno effettuare la raccolta dei dati di transito leggendo le targhe dei veicoli; i dati raccolti dovranno essere inviati al sottosistema centrale, parte del sistema SISTRI, per essere processati ed archiviati.	SYS-CON-FUN-02100	
	A136	Gli apparati di ripresa dovranno essere delle telecamere fisse digitali in grado di soddisfare i seguenti requisiti:	SYS-CON-FUN-02101	
Pag. 15	A137	• Risoluzione non inferiore a 1280x720 e comunque adeguata al corretto rilevamento di immagini per l'identificazione della targa;	SYS-CON-FUN-02101	
	A138	• Sensore CMOS Progressive Scan da 1/3";	SYS-CON-FUN-02101	
	A139	• Interfaccia di trasmissione IP;	SYS-CON-FUN-02101	
	A140	• Compressione video standard (Ad esempio: H264 o MPEG4);	SYS-CON-FUN-02101	
	A141	• Filtro a infrarossi automatico per riprese diurne/notturne;	SYS-CON-FUN-02101	
	A142	• Messa a fuoco automatica;	SYS-CON-FUN-02101	
	A143	• Illuminazione minima Colore: 2 lux a 301RE, F1.8, Modalità in bianco e nero: 0,2 lux a 301RE, F1.8;	SYS-CON-FUN-02101	

Fonte: Allegato A al Contratto

	A144	• Durata otturazione Da 1/10000 sec a 1/2 sec;	SYS-CON-FUN-02101	
	A145	• Zoom ottico 10x e zoom digitale 12x , complessivamente pari a 120x;	SYS-CON-FUN-02101	
	A146	• Velocità di trasmissione 30/25 fps a tutte le risoluzioni;	SYS-CON-FUN-02101	
	A147	• Protezione mediante password;	SYS-CON-FUN-02101	
	A148	• Filtri per indirizzi IP;	SYS-CON-FUN-02101	
	A149	• Crittografia HTTPS;	SYS-CON-FUN-02101	
	A150	• Controllo degli accessi di rete IEEE 802.1X;	SYS-CON-FUN-02101	
	A151	• Autenticazione mediante digest;	SYS-CON-FUN-02101	
	A152	• Registro degli accessi utente;	SYS-CON-FUN-02101	
	A153	• Protocolli supportati: HTTP, HTTPS, QoS Layer 3 DiffServ, FTP, SMTP, Bonjour, UPnP, SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS.	SYS-CON-FUN-02101	
	A154	Gli apparati di ripresa dovranno essere installati con adeguati componenti di sostegno (pali, staffe, ...) e completi di accessori (ottica, custodia, ...).	SYS-CON-FUN 16902	SYS-CON-FUN 16902
	A155	Il flusso video proveniente dalle telecamere dovrà essere processato al fine di rilevare i veicoli in transito mediante algoritmi di elaborazione delle immagini; per ciascun veicolo in transito, dovrà essere eseguita la lettura automatica della targa e dei codici Kemler ed ONU	SYS-CON-FUN-02102	
Pag. 16	A156	L'algoritmo di rilevazione della targa dei veicoli deve associare l'immagine in cui è visibile il veicolo e leggibile la targa corrispondente, con le stringhe alfanumeriche ottenute mediante il processo di OCR.	SYS-CON-FUN-02103	
	A157	I dati elaborati (immagini e targhe rilevate) dovranno essere inviati al sottosistema centrale attraverso rete wireless (Ad esempio GPRS).	SYS-CON-FUN-02104	
	A158	Il sistema di elaborazione periferico dovrà prevedere un cabinet dedicato al contenimento degli apparati di campo; il processamento del flusso video della telecamera dovrà avvenire su un elaboratore dedicato con le seguenti caratteristiche:	SYS-CON-INF-02105	
	A159	• Processore con capacità elaborativa equivalente ad un Intel Core 2 Duo P9600, 2.66GHz, 6MB cache;	SYS-CON-INF-02105	
	A160	• Sistema Operativo Linux;	SYS-CON-INF-02105	
	A161	• Hard Disk interno SATA da almeno 60GB per mantenere i dati rilevati durante gli eventuali periodi di assenza del collegamento wireless.	SYS-CON-INF-02105	
	A162	Per il "Sottosistema Centrale" dovranno essere previsti i seguenti componenti principali:	SYS-CON-INF-02106	
	A163	• server ed applicativi per l'acquisizione delle informazioni remote;	SYS-CON-INF-02106	
	A164	• server ed applicativi per la gestione dei sistemi periferici;	SYS-CON-INF-02106	
	A165	• server ed applicativi per l'elaborazione e relative interfacce applicative verso le applicazioni del progetto SISTRI;	SYS-CON-INF-02106	
	A166	• server ed applicativi per la gestione dei dati acquisiti e relativo database;	SYS-CON-INF-02106	
	A167	• server ed applicativi per le interfacce verso il front-end e la gestione degli eventi;	SYS-CON-INF-02106	

Fonte: Allegato A al Contratto

	A168	• elementi di rete e sicurezza per l'interfaccia verso l'esterno e l'integrazione con gli altri servizi del Centro Operativo SISTRI (firewall, switch);	SYS-CON-INF-02106	
	A169	• soluzione di archiviazione costituita da un sistema di storage e disk	SYS-CON-INF-02106	
Pag. 17	A170	Il dimensionamento e la realizzazione del sistema SISTRI come pure la fornitura dei servizi ad esso relativi deve essere basata sulla seguente mappatura numerica. Si precisa che i dati di seguito riportati sono del tutto presuntivi. Il numero esatto degli Utenti e la loro ripartizione saranno quelli che risulteranno a seguito dell'iscrizione.		SYS-CON-INF-15530 : Numero di Utenti previsti e dotazioni tecniche
	A171	• Utenti di SISTRI: 640.331 (396.745 soggetti obbligati + 243.586 veicoli)		SYS-CON-INF-15530 : Numero di Utenti previsti e dotazioni tecniche
	A172	• Totale soggetti obbligati: 396.745		SYS-CON-INF-15530 : Numero di Utenti previsti e dotazioni tecniche
	A173	• Totale veicoli: 243.586		SYS-CON-INF-15530 : Numero di Utenti previsti e dotazioni tecniche
	A174	• Totale (soggetti obbligati + Veicoli) =641.746		SYS-CON-INF-15530 : Numero di Utenti previsti e dotazioni tecniche

Devono essere fornite delle BB per tracciare la posizione dei mezzi su gomma adibiti al trasporto nell'ambito SISTRI

SYS-CON-FUN-02107

Fonte: Integrazione contrattuale

Rif.	ID	Descrizione Requisito	Inserimenti Selex
Art. 1	IC1	Modifica della Pianificazione delle consegne dei Dispositivi USB e delle Black Box e alle modalità di fatturazione e pagamento come da Allegato D1	nok
	IC2	Le parti convengono che per tutte le iscrizioni successive alla data di sottoscrizione della presente scrittura integrativa, Selex sarà tenuta alla consegna a ciascun utente dei dispositivi USB entro 7 giorni e delle Black Box entro 12 giorni dall'iscrizione fino a concorrenza di richieste di dispositivi pari a 20000 unità	nok
	IC3	Selex garantirà comunque una scorta di magazzino delle predette tecnologie pari a n. 20000 per tipologia e sarà tenuta a ripristinare la predetta quantità in caso di diminuzione ogni mese	nok
	IC4	Le Parti convengono che per i motivi esposti precedentemente nel Caso in cui le richieste dei nuovi utenti esauriscano, entro 7 giorni lavorativi tutte le scorte di magazzino, la Selex garantirà la consegna a ciascun utente del dispositivo USB in 12 giorni lavorativi e della black bpx in 22 giorni lavorativi decorrenti dalla data di iscrizione limitatamente ad ulteriori 20000 per tipologia. Per quantità superiori le Parti si incontreranno per individuare la relativa tempistica di consegna	nok
		In parziale deroga alle previsioni contenute nell'articolo 8 del contratto di cui al precedente punto A):	nok
	IC5	I. Selex per i dispositivi (USB e black box) consegnati nel 2010 provvederà ad emettere fattura al 28 dicembre 2010 e per la stessa si provvederà ad emettere il relativo mandato di pagamento entro i successivi 90 giorni;	nok
	IC6	II. Ministero procederà ad emettere i mandati di pagamento in relazione a quanto previsto dall'articolo 8, 1o comma, per il 2010 secondo la seguente tempistica:	nok
	IC7	la quota di euro 5.000.000,00 (iva inclusa) entro la fine del 2010;	nok
	IC8	la quota di euro 20.000.000,00 (più iva) e la quota di euro 9.676.395,00 (più iva) entro 30 giorni da quando saranno disponibili sul capitolo 7082 del Ministero dell'Ambiente le somme versate da parte degli utenti.	nok
	IC9	III. Per il corrispettivo di cui alla lettera b dell'articolo 7, per ciascun anno di durata del contratto successivo al 2010, sarà emesso il relativo mandato di pagamento entro il 31 luglio di ciascun anno.	nok
	IC10	Selex da atto di effettuare gli ordini delle tecnologie ai propri fornitori in ragione del numero degli iscritti effettivi e non sulla base delle stime originarie, fatti salvi gli ordini degli apparecchi relativi alla videosorveglianza che, invece, vengono approntate da Selex e pagate dal Ministero sulla base delle previsioni contenute nel contratto.	nok
Art. 2	IC11	E' facoltà del Ministero dell'Ambiente di individuare altri impianti su cui installare la videosorveglianza nell'ambito dei dispositivi ordinati, pari a n. 800.	nok
	IC12	Selex garantisce che ciascuna videosorveglianza venga installata entro 5 giorni lavorativi, fatte salve oggettive circostanze evidenziate dalla Selex	nok
Art. 4	IC13	Con la sottoscrizione della presente scrittura integrativa le Parti si danno atto che Selex si impegna a completare, con oneri esclusivamente a proprio carico, il piano di comunicazione di cui all'allegato A).	nok

Fonte: integrazione contrattuale

Alf. A		Adeguamenti o nuovi Sviluppi Applicativi/Infrastrutturali	
Alf. A	IC14	Progettazione, sviluppo e test del servizio di interoperabilità con i gestionali, ivi incluse tutte le attività di raccolta requisiti e gestione delle riunioni con i relativi attori	SYS-CON-INF-15540
	IC15	Esecuzione della fase di sperimentazione con centinaia di imprese verso le quali è stato necessario procedere con le attività di iscrizione, creazione anagrafiche/ruoli, personalizzazione e distribuzione dei dispositivi USB, ed i relativi servizi di assistenza. In particolare la sperimentazione coinvolge circa 300 imprese per oltre 1.500 dispositivi USB.	SYS-CON-GEN 15541
	IC16	Progettazione e realizzazione di una piattaforma dimostrativa appositamente dedicata per le attività di sperimentazione e dimostrazione nuovi servizi	SYS-CON-FUN 15542
	IC17	Adeguamenti applicativi, di work flow e sulle basi dati per tener conto dei decreti correttivi di Febbraio e Luglio in particolare:	SYS-CON-FUN-15543
	IC18	o Applicazione di iscrizione attraverso l'integrazione e gestione di nuove categorie	SYS-CON-FUN-15543
	IC19	o Algoritmo di calcolo pagamenti	SYS-CON-FUN-15543
	IC20	o Basi dati e ruoli per tener conto delle nuove categorie (vedi agricoltori, etc.)	SYS-CON-FUN-15543
	IC21	o Applicazione scheda movimentazione	SYS-CON-FUN-15543
	IC22	Adeguamento dell'applicativo di prenotazione officine per consentire la prenotazione giornaliera e non settimanale e la consultazione per regione di competenza dello stato di installazione per ogni trasportatore	SYS-CON-FUN 15544
	IC23	Adeguamenti applicativi per consentire la consegna con eccezione da parte delle Camere di Commercio sulla base del nuovo scenario definito in Agosto	SYS-CON-FUN 15545
	IC24	Sviluppo di un nuovo applicativo con relativo servizi per consentire all'utente di "sanare" la pratica (rispetto ai disallineamenti evidenziati da Ecocerved) da remoto, con conseguente abilitazione vincolata del dispositivo e personalizzazione da remoto	SYS-CON-FUN 15546
	IC25	Ampliamento della componente portale con nuove aree tematiche in particolare il sistema di knowledge management per garantire risposte informatiche alle problematiche degli utenti.	SYS-CON-GEN 15547
	IC26	Ampliamento delle capacità del CRM, sviluppo applicazione di tracciatura e monitoraggio dei flussi operativi ed ampliamento del sistema gestione documentale	SYS-CON-FUN 15548
	IC27	Discariche: Lavorazioni extra (impiantistica, scavi, etc.) su 27 discariche (ad eccezione delle 4 della Campania) che non presentavano i requisiti e le predisposizioni attese	SYS-CON-GEN 15549
	IC28	Rifacimento di alcune parti della Caserma del Corpo dei Carabinieri -NOE di via Aurelia	SYS-CON-FUN 15549
	IC29	Allestimento laboratorio del Corpo dei Carabinieri NOE di via Faustiniana (Centro Sistri)	SYS-CON-FUN 15549

Fonte: Integrazione contrattuale

IC30	Predisposizione del Sistema affinché, in via sperimentale, la tracciabilità dei mezzi di trasporti sia effettuata in tempo reale (gestione Flotta GPS) su richiesta da parte dell'Autorità che gestisce il Sistema (NOE). Il NOE, in questa fase sperimentale (di durata non superiore a 6 mesi), ha la possibilità di acquisire informazioni in contemporanea da 30 BB in modo da consentire il tracciamento in modalità circolare iterativa fino a 300 vettori e contemporaneamente potrà modificare le richieste di tracciamento dei vettori sulla base delle sue esigenze operative per poter controllare durante la giornata fino a 1000 vettori.	SYS-CON-GEN 15550
IC31	Alla fine di questa fase sperimentale, in cui il NOE avrà definito le procedure operative ed affinato la soluzione tecnica sarà in condizione di formalizzare l'eventuale richiesta di estensione del tracciamento giornaliero ad un numero di vettori più elevato di 1000, a cui seguirà offerta da parte del Concessionario. I costi relativi al traffico dial-up (acquisizione dati dalle BB in tempo reale) in fase	SYS-CON-GEN 15550
IC32	Predisposizione del Sistema affinché lo stesso avverta, tramite alert, il centro SISTRI (NOE) allorché il mezzo di trasporto si discosti dal percorso dichiarato, con pianificazione attraverso il Servizio GIS del portale, di una distanza configurabile dal Centro. I costi relativi al traffico SMS sono a carico dell'utente.	SYS-CON-GEN 15551
IC33	Acquisizione per la successiva consegna al NOE di un DRONE (per uso locale) sulla base delle specifiche richieste dal Cliente (modello, configurazione) per un costo complessivo fino ad un limite massimo di euro duecentomila. Il concessionario non avrà alcun onere e responsabilità relativi alla certificazione, omologazione, formazione e gestione operativa del dispositivo.	SYS-CON-GEN 15552
	Servizi Operativi e Formazione eseguiti fino alla data del presente atto*	
IC34	* Supporto al Ministero dell'Ambiente e Tutela del Territorio e del Mare con 7 tecnici distaccati presso la sede di via Cristoforo Colombo Roma con oneri a carico di Selex Sema per svolgere attività relative al Sistr	na
IC35	* Implementazione di un numero nero e 10 operatori dedicati alle officine. Gestione di circa 500 chiamate giornaliere con picchi di oltre 900	SYS-CON-GEN 15553
IC36	* Implementazione di un numero nero e di 2 operatori dedicati all'Albo gestori	SYS-CON-GEN 15553
IC37	* Implementazione di un numero nero e di 2 operatori dedicati alle Associazioni di categoria dei trasportatori	SYS-CON-GEN 15553
IC38	* Chiamate in ingresso al Call center di numero notevolmente superiore a quanto previsto da contratto (circa 6000 telefonate/giorno)	SYS-CON-GEN 15554
IC39	* Formazione di un team di installatori mobili formato da 30 risorse (15 fisse e 15 su base necessità) per assistenza on site verso officine/trasportatori con copertura nazionale	SYS-CON-GEN 15555
IC40	* Misure specifiche per il potenziamento del know how e produttività delle officine (newsletter settimanale, 1.500 DVD esplicativi, ulteriori 2 set di token per back up per un totale di 3.500)	SYS-CON-GEN 15556
IC41	Servizio operativo di ricontatto giornaliero con le officine per verifica installazioni/appuntamenti e ripianificazione degli appuntamenti mancati. Il servizio coinvolge 4 operatori dedicati con un numero medio di 300 chiamate outbound giornaliere Formazione delle officine: esecuzione di una seconda sessione nel 2010 per ulteriori 200 officine (iscrizione, verifica, formazione, rilascio token e certificati)	SYS-CON-GEN 15557 SYS-CON-GEN 15558
IC42	Formazione verso le associazioni di categoria; predisposizione di materiale formativo ed esecuzione di 9 sessioni per circa 200 utenti ciascuna	SYS-CON-GEN 15559
IC43	Prolungamento della fase di iscrizione (da gennaio tuttora in corso) nelle diverse modalità oltre i termini previsti dal primo decreto (75 giorni solari)	SYS-CON-GEN 15560

Fonte: Integrazione contrattuale

IC44	• Identificazione dei pagamenti effettuati attraverso l'analisi dei dati di Poste Italiane e Banca d'Italia	SYS-CON-GEN 15561
	Campagna di Comunicazione	
IC45	• Conferenza stampa del Ministro all inclusive il giorno 25 novembre 2010	SYS-CON-GEN 15562
IC46	• Uscite su quotidiani nazionali e locali il giorno 26 novembre 2010	SYS-CON-GEN 15562
IC47	• Inserto su il Sole 24 Ore in data 29 novembre 2010	SYS-CON-GEN 15562
IC48	• Pianificazione televisiva di 2 settimane su TV NAT GEO a partire dal 29 novembre 2010: un filmato da 2 minuti nel mese di dicembre per ca. 30 uscite	SYS-CON-GEN 15562

Fonte: D. Lgs. 152-2006 con aggiornamenti intervenuti fino al 10 febbraio 2012 - Parte Quarta - Solo articoli e commi di interesse

Rif.	ID	Descrizione Requisito	ID Selex	ID Selex Integrato
Art. 183	DL1	Definizioni. 1. Ai fini della parte quarta del presente decreto e fatte salve le ulteriori definizioni contenute nelle disposizioni speciali, si intende per:		SYS-LAW-GEN-00122
	DL2	a) "rifiuto": qualsiasi sostanza od oggetto di cui il detentore si disfi o abbia l'intenzione o abbia l'obbligo di disfarsi;		non presente
	DL3	b) "rifiuto pericoloso": rifiuto che presenta una o più caratteristiche di cui all'allegato I della parte quarta del presente decreto;		non presente
	DL4	c) "oli usati": qualsiasi olio industriale o lubrificante, minerale o sintetico, divenuto improprio all'uso cui era inizialmente destinato, quali gli oli usati dei motori a combustione e dei sistemi di trasmissione, nonché gli oli usati per turbine e comandi idraulici;		non presente
	DL5	d) "rifiuto organico" rifiuti biodegradabili di giardini e parchi, rifiuti alimentari e di cucina prodotti da nuclei domestici, ristoranti, servizi di ristorazione e punti vendita al dettaglio e rifiuti simili prodotti dell'industria alimentare raccolti in modo differenziato;		non presente
	DL6	e) "autocompostaggio": compostaggio degli scarti organici dei propri rifiuti urbani, effettuato da utenze domestiche, ai fini dell'utilizzo in sito del materiale prodotto;		non presente
	DL7	f) "produttore di rifiuti": il soggetto la cui attività produce rifiuti (produttore iniziale) o chiunque effettui operazioni di pretrattamento, di miscelazione o altre operazioni che hanno modificato la natura o la composizione di detti rifiuti;		SYS-LAW-GEN-00123
	DL8	g) "produttore del prodotto": qualsiasi persona fisica o giuridica che professionalmente sviluppi, fabbrichi, trasformi, tratti, venda o importi prodotti;		
	DL9	h) "detentore": il produttore dei rifiuti o la persona fisica o giuridica che ne è in possesso;		SYS-LAW-GEN-00124
	DL10	i) "commerciante": qualsiasi impresa che agisce in qualità di committente, al fine di acquistare e successivamente vendere rifiuti, compresi i commercianti che non prendono materialmente possesso dei rifiuti;		SYS-LAW-GEN-00125
	DL11	l) "intermediario" qualsiasi impresa che dispone il recupero o lo smaltimento dei rifiuti per conto di terzi, compresi gli intermediari che non acquisiscono la materiale disponibilità dei rifiuti;		SYS-LAW-GEN-00126
	DL12	o) "raccolta": il prelievo dei rifiuti, compresi la cernita preliminare e il deposito, ivi compresa la gestione dei centri di raccolta di cui alla lettera "mm", ai fini del loro trasporto in un impianto di trattamento;		SYS-LAW-GEN-00128
	DL13	p) "raccolta differenziata": la raccolta in cui un flusso di rifiuti è tenuto separato in base al tipo ed alla natura dei rifiuti al fine di facilitarne il trattamento specifico;		non presente
	DL14	q) "preparazione per il riutilizzo": le operazioni di controllo, pulizia, smontaggio e riparazione attraverso cui prodotti		SYS-LAW-GEN-00129
	DL15	o componenti di prodotti diventati rifiuti sono preparati in modo da poter essere reimpiegati senza altro pretrattamento;		SYS-LAW-GEN-00129
	DL16	r) "riutilizzo": qualsiasi operazione attraverso la quale prodotti o componenti che non sono rifiuti sono reimpiegati per la stessa finalità per la quale erano stati concepiti;		non presente

Fonte: D. Lgs. 152-2006 con aggiornamenti intervenuti fino al 10 febbraio 2012 - Parte Quarta - Solo articoli e commi di interesse

	DL17	s) "trattamento": operazioni di recupero o smaltimento, inclusa la preparazione prima del recupero o dello smaltimento;		SYS-LAW-GEN-00130
	DL18	t) "recupero": qualsiasi operazione il cui principale risultato sia di permettere ai rifiuti di svolgere un ruolo utile, sostituendo altri materiali che sarebbero stati altrimenti utilizzati per assolvere una particolare funzione o di prepararli ad assolvere tale funzione, all'interno dell'impianto o nell'economia in generale. L'allegato C della parte IV del presente decreto riporta un elenco non esaustivo di operazioni di recupero;		SYS-LAW-GEN-00131
	DL19	u) "riciclaggio": qualsiasi operazione di recupero attraverso cui i rifiuti sono trattati per ottenere prodotti, materiali o sostanze da utilizzare per la loro funzione originaria o per altri fini. Include il trattamento di materiale organico ma non il recupero di energia né il ritrattamento per ottenere materiali da utilizzare quali combustibili o in operazioni di riempimento;		non presente
	DL20	z) "smaltimento": qualsiasi operazione diversa dal recupero anche quando l'operazione ha come conseguenza secondaria il recupero di sostanze o di energia. L'Allegato B alla parte IV del presente decreto riporta un elenco non esaustivo delle operazioni di smaltimento		SYS-LAW-GEN-00132
	DL21	aa) "stoccaggio": le attività di smaltimento consistenti nelle operazioni di deposito preliminare di rifiuti di cui al punto D15 dell'allegato B alla parte quarta del presente decreto, nonché le attività di recupero consistenti nelle operazioni di messa in riserva di rifiuti di cui al punto R13 dell'allegato C alla medesima parte quarta;		non presente
	DL22	bb) "deposito temporaneo": il raggruppamento dei rifiuti effettuato, prima della raccolta, nel luogo in cui gli stessi sono prodotti o, per gli imprenditori agricoli di cui all'articolo 2135 del codice civile, presso il sito che sia nella disponibilità giuridica della cooperativa agricola di cui gli stessi sono soci, alle seguenti condizioni: (le condizioni non sono riportate)		SYS-LAW-GEN-00133
	DL23	qq) "sottoprodotto": qualsiasi sostanza od oggetto che soddisfa le condizioni di cui all'articolo 184-bis, comma 1, o che rispetta i criteri stabiliti in base all'articolo 184-bis, comma 2.		non presente
Art. 184	DL24	Classificazione 1. Ai fini dell'attuazione della parte quarta del presente decreto i rifiuti sono classificati, secondo l'origine, in rifiuti urbani e rifiuti speciali e, secondo le caratteristiche di pericolosità, in rifiuti pericolosi e rifiuti non pericolosi.		presente parzialmente
	DL25	2. Sono rifiuti urbani:		non presente
	DL26	a) i rifiuti domestici, anche ingombranti, provenienti da locali e luoghi adibiti ad uso di civile abitazione;		non presente
	DL27	b) i rifiuti non pericolosi provenienti da locali e luoghi adibiti ad usi diversi da quelli di cui alla lettera a), assimilati ai rifiuti urbani per qualità e quantità, ai sensi dell'articolo 198, comma 2, lettera g);		non presente
	DL28	c) i rifiuti provenienti dallo spazzamento delle strade;		non presente
	DL29	d) i rifiuti di qualunque natura o provenienza, giacenti sulle strade ed aree pubbliche o sulle strade ed aree private comunque soggette ad uso pubblico o sulle spiagge marittime e lacuali e sulle rive dei corsi d'acqua;		non presente
	DL30	e) i rifiuti vegetali provenienti da aree verdi, quali giardini, parchi e aree cimiteriali;		non presente
	DL31	f) i rifiuti provenienti da esumazioni ed estumulazioni, nonché gli altri rifiuti provenienti da attività cimiteriale diversi da quelli di cui alle lettere b), c) ed e)		non presente
	DL32	3. Sono rifiuti speciali:		non presente
	DL33	a) i rifiuti da attività agricole e agro-industriali, ai sensi e per gli effetti dell'Art. 2135 c.c.;(*)		non presente
	DL34	b) i rifiuti derivanti dalle attività di demolizione, costruzione, nonché i rifiuti che derivano dalle attività di scavo, fermo restando quanto disposto dall'articolo 184-bis(*)		non presente
	DL35	c) i rifiuti da lavorazioni industriali, (fatto salvo quanto previsto dall'articolo 185, comma 1, lettera i);(**)		non presente
	DL36	d) i rifiuti da lavorazioni artigianali;		non presente
	DL37	e) i rifiuti da attività commerciali;		non presente