PROTOCOLLI DI CONTROLLO *EX* D.LGS. 231/2001

Reati informatici

Parte Speciale B

PROTOCOLLI DI CONTROLLO *EX* D.LGS. 231/2001 N.6

ATTIVITÀ SENSIBILI

I presenti Protocolli trovano applicazione nei confronti dei Destinatari del Modello di Organizzazione, Gestione e Controllo (di seguito anche solo "**Modello**") adottato da CARBOSULCIS S.p.A. (di seguito anche solo "**CARBOSULCIS**" o la "**Società**") ai sensi del D.Lgs. 231/2001, i quali, a qualunque titolo, per conto o nell'interesse della Società, siano coinvolti nella gestione della sicurezza e manutenzione dei sistemi informativi, nell'ambito delle seguenti attività "sensibili", come individuate nella Mappatura delle attività a rischio-reato di cui al paragrafo 2.5 della Parte Generale II del Modello:

- Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali;
- Gestione dei contenuti (foto, video, brani musicali) destinati al sito internet della Società;
- Utilizzo di software nell'ambito dei sistemi informativi aziendali.

PROTOCOLLI DI CONTROLLO SPECIFICI

Con riferimento alle attività "sensibili" sopra individuate, CARBOSULCIS ritiene necessario che i Destinatari del Modello si uniformino ai principi di controllo di seguito rappresentati:

B.A.1 l'invio della documentazione per l'attuazione degli adempimenti obbligatori presso gli Enti Pubblici può avvenire, laddove previsto, anche per via telematica, secondo quanto stabilito dalla disciplina di accesso ai *software* gestionali di trasmissione dei dati protetti (e.g. tramite l'utilizzo di *Smart Card* personali fornite dall'Ente Pubblico), in conformità con le disposizioni di legge vigenti in materia. In tal caso, il procuratore responsabile della trasmissione all'Ente Pubblico deve farsi garante dell'integrità e correttezza dei dati trasmessi, attraverso il controllo degli accessi da parte del solo personale a ciò autorizzato. Detto personale non può apportare alcuna modifica ai dati che non sia stata previamente autorizzata per iscritto dal procuratore;

B.A.2 viene individuato e nominato formalmente l'Amministratore di Sistema in conformità alle disposizioni del Garante per la protezione dei dati personali;

B.A.3 le utenze di "Amministratore" dei *computer* presenti in azienda sono limitate al *management* aziendale e al personale della Funzione *Personale e Informatica*; in ogni caso, è vietata l'installazione di programmi e applicativi in via autonoma senza il coinvolgimento della medesima Funzione;

B.A.4 le licenze di utilizzo dei *software* presenti sui *computer* a disposizione del personale aziendale sono gestite dalla Funzione *Personale e Informatica*;

B.A.5 è fatto divieto agli utenti di installare *software* particolari e non inclusi nella lista dei *software* approvati, se non dopo formale invio della richiesta al Responsabile della Funzione *Personale e Informatica* e intervento di quest'ultimo soggetto;

B.A.6 il Responsabile della Funzione *Personale e Informatica* effettua verifiche periodiche a campione al fine di accertare e rimuovere eventuali *software* non autorizzati e per controllare l'accesso da parte degli utenti a siti di *download* di contenuti, assicurando apposita evidenza formale del controllo svolto;

B.A.7 i sistemi informativi aziendali sono periodicamente oggetto di *audit*, volti a verificare, a titolo esemplificativo, l'autorizzazione delle richieste di accesso agli applicativi gestionali, la revisione periodica delle utenze nonché la disabilitazione di quelle non più attive;

B.A.8 l'accesso alle informazioni che risiedono sui *server* aziendali, ivi inclusi i *client*, è limitato da strumenti di autenticazione;

B.A.9 l'accesso alle applicazioni da parte del personale è garantito attraverso strumenti di autorizzazione;

B.A.10 la rete di trasmissione dati aziendale è protetta da adeguati strumenti di limitazione degli accessi (fisici e logici);

B.A.11 il personale accede al sistema informativo aziendale unicamente attraverso i codici di identificazione assegnati, provvedendo alla modifica periodica;

B.A.12 PERIN interviene, su richiesta di COAMB, per garantire la manutenzione e la gestione del sistema informatico di rilevamento dati ambientali (parte hardware e software).

FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza richiede alle Funzioni/Direzioni aziendali coinvolte di inviare su base periodica – **mediante compilazione dello "*schema di segnalazione all'OdV*" allegato alla presente Parte speciale** – adeguati flussi informativi che consentano di effettuare un'attività sistematica e formalizzata di monitoraggio delle anomalie, delle eccezioni e delle deroghe registrate nel periodo di riferimento rispetto all'attuazione del Protocollo.

Per il dettaglio sul contenuto e sulla periodicità dei flussi, nonché sui soggetti responsabili del relativo invio, si rinvia al documento "*Report dei flussi informativi*" predisposto e approvato dall'Organismo di Vigilanza.