Il giorno 26 giugno 2008

l'Amministrazione della Banca d'Italia, rappresentata dal Segretario Generale Paolo Piccialli, dal Capo del Servizio Personale Inquadramento Normativo ed Economico Augusto Aponte e da Francesco Nicolò e Antonella Caronna del medesimo Servizio, nonché da Alberto Martiello del Servizio Personale Gestione Risorse

e

la FISAC-CGIL, rappresentata da
PELLEGRINI GUIDO
CECCHI PAOLO
PANDOLFI ENEO
VICI MARINA
VITTORI GIANNI
il SINDIRETTIVO-CIDA, rappresentato da
BARRA STEFANO, ACAMPA EMANUELE, ARGENTIERI MAURIZIO,
ARRUZZOLI CARLO, CACCARESE FABRIZIO, CARCIZZA SIMONE,
CIUFOLI ANTONELLA MARIA, D'ARRIGO VIRGINIA, DE CECCHIS GIOVANN. FRANCESCO,
GIACOMINI MARINA, MANCINI PASQUALE, MAZZUCA ETTORE, NAPOLITANO GIUSEPPE,
PARISI ORESTE, SILVI MAURIZIO
il SIBC-CISAL, rappresentato da
DARY MASSIMO, CACCIAGNO MARIO,
DAMIANI FRANCESCO, DE SANCTIS ANTONELLA
INNOCENTI RICCARDO

la FABI, rappresentata da
MARANESI ANGELO, SERVASCONI FABRIZIO, DEL PURO ALESSANDRO
FERRAZZA GIUSEPPE, GOVONI ROBERTO, PIRUNA CORRA CORRADO,
RICCIARELLA GIUSEPPE, TARANTINI MARIO, TOSCANELLI MASSIMO

la FIBA-CISL, rappresentata da
ROMOLI GIANVITTORIO
MARIANI PIETRO
MARRONE ROBERTO

la UILCA-UIL, rappresentata da
SENO FLAVIO, CASCIONE ANTONIETTA,
CAPUOZZO CARLO, CARUSI GIANNI,
GIULIANI MARCO

hanno stipulato il seguente accordo in tema di utilizzo da parte delle Organizzazioni Sindacali di alcune funzionalità dell'Intranet della Banca.

CONVENZIONE CON LE ORGANIZZAZIONI SINDACALI SU BACHECA ELETTRONICA – ACCESSO SELETTIVO AD INTRANET

1. Clausole generali

La Banca d'Italia mette a disposizione della Segreteria Nazionale di ciascuna Organizzazione Sindacale un distinto spazio nell'Intranet aziendale nel quale pubblicare, ai sensi dell'art. 7 della vigente Convenzione per i diritti sindacali, comunicati riguardanti materie di interesse sindacale o attinenti al rapporto di lavoro, liberamente consultabili da parte della generalità del personale.

La Banca d'Italia mette altresì a disposizione delle predette Segreterie Nazionali una funzione di consultazione delle informazioni gestite, sempre nell'ambito dell'Intranet aziendale, dalle applicazioni "Situazione del personale", "Consultazione normativa", "Rassegna stampa" ed "Elenco telefonico".

2. Modalità di accesso

L'accesso alle funzionalità sopra descritte avverrà, per ciascuna Organizzazione Sindacale, esclusivamente attraverso due postazioni di lavoro, ai fini di *recovery*, appositamente dedicate, collegate alla rete aziendale della Banca, la cui installazione, configurazione, aggiornamento e manutenzione saranno effettuate esclusivamente dalla Banca d'Italia, sulla base degli *standard* applicati nell'Istituto, che ne sopporterà anche ogni relativo onere. L'installazione potrà avvenire esclusivamente nei locali messi a disposizione delle Segreterie Nazionali dalla Banca medesima.[1]

Le caratteristiche e la configurazione di ogni postazione di lavoro, definite in relazione alle funzionalità cui essa è dedicata e agli specifici presidi di sicurezza individuati, sono descritte nell'allegato A). Eventuali modifiche, che dovessero essere richieste dalle Segreterie Nazionali in relazione a sopravvenute esigenze, saranno valutate dalla Banca d'Italia, restando fin d'ora esclusa ogni possibilità di installazione e/o impiego sulla postazione medesima di prodotti non forniti dall'Istituto.

La Segreteria Nazionale di ciascuna Organizzazione Sindacale segnalerà formalmente gli utenti da abilitare all'utilizzo delle postazioni di lavoro, individuati tra i dipendenti della Banca d'Italia. L'abilitazione di nuovi utenti, anche in sostituzione di elementi già autorizzati, sarà richiesta con le medesime modalità, nel rispetto dei principi di stretta necessità e di minimizzazione degli oneri di gestione delle postazioni.

3. Modalità di utilizzo

Lo spazio per la pubblicazione di documenti a carattere sindacale sarà identificato con un'apposita icona, presente nella *home page* dell'Intranet aziendale e denominata "Comunicazioni delle Organizzazioni Sindacali" [od altra equivalente], dalla quale sarà possibile accedere agli spazi a disposizione delle singole Organizzazioni Sindacali, individualmente identificati con la sigla di ciascuna di esse.

[1] I locali in questione sono ubicati in Via Panisperna, 30-32 ed in Via Milano, 64.

Ai fini della gestione dello spazio disponibile nell'Intranet aziendale ciascuna Organizzazione Sindacale potrà elaborare, modificare, archiviare, cancellare, nonché inserire nello spazio o rimuovere dallo stesso, i documenti a carattere sindacale (cc.dd. funzioni di "scrittura/lettura"); i formati dei documenti in questione saranno quelli gestiti dai prodotti software previsti dalla configurazione della postazione di lavoro, e riportati anch'essi nell'allegato A).

La Banca d'Italia si riserva di definire e/o modificare la "veste grafica" degli spazi a disposizione delle Organizzazioni Sindacali in relazione all'introduzione di *standard* grafici uniformi per l'Intranet aziendale.

L'accesso alle quattro applicazioni dell'Intranet aziendale, sopra indicate, consentirà invece la sola funzione di "lettura" (comprensiva di stampa) dei dati e delle informazioni ivi presenti.

La Banca d'Italia si impegna a garantire alle Organizzazioni Sindacali la disponibilità dei servizi sopra descritti secondo gli *standard* previsti per la generalità degli utenti della rete Intranet aziendale. Resta a carico delle Organizzazioni Sindacali porre in essere opportune misure di *contingency*, eventualmente basate su procedure manuali, atte a consentire la diffusione dei comunicati sindacali anche in caso di indisponibilità della Intranet aziendale e/o degli strumenti hardware e software disponibili localmente.

La Banca assicurerà, ove necessario, la formazione dei dipendenti segnalati dalle Segreterie Nazionali ai fini dell'utilizzo delle postazioni di lavoro, nonché l'assistenza informatica attraverso l'apposita funzione di *help desk* a disposizione degli utenti della rete aziendale.

4. Presidi di sicurezza e responsabilità degli utenti

Le Segreterie Nazionali si impegnano ad utilizzare le funzionalità sopra descritte esclusivamente per scopi connessi alle proprie attività istituzionali e nel rispetto della vigente disciplina legislativa, ivi compresa quella concernente l'utilizzo degli strumenti informatici e la protezione dei dati personali.
Le Segreterie Nazionali si impegnano altresì al rispetto della vigente normativa interna della Banca in materia di corretto utilizzo delle risorse informatiche dell'Istituto, di sicurezza informatica e di riservatezza delle informazioni, relativamente alle previsioni applicabili agli strumenti ed ai servizi oggetto della presente Convenzione, e garantiscono il rispetto della normativa stessa da parte degli utenti abilitati ad operare sulle postazioni di lavoro dedicate. A tal fine, si richiama l'attenzione delle Organizzazioni Sindacali sulle disposizioni di servizio, i cui estremi sono riportati in dettaglio nell'allegato B, nel quale sono contenute talune istruzioni applicative della vigente normativa); dette disposizioni sono reperibili nell'archivio elettronico della normativa, dal quale può esserne tratta copia anche a fini di *recovery*.
Fermo restando che il presidio dello stabile, nel quale sono installate le postazioni di lavoro, è assicurato dalla Banca d'Italia, le Segreterie Nazionali sono responsabili della custodia delle apparecchiature in questione, sulla base degli *standard* di sicurezza fisica applicati nell'Istituto.

Le Organizzazioni Sindacali segnaleranno senza indugio qualunque danneggiamento, malfunzionamento e/o evento anomalo riscontrato nell'utilizzo delle postazioni di

lavoro, al fine di consentire un tempestivo intervento della competente funzione ed il conseguente ripristino della normale funzionalità della postazione stessa. In tali circostanze, gli utenti abilitati assicureranno la propria collaborazione nell'effettuazione degli interventi che fossero richiesti dalla competente funzione, nella prima fase di verifica ed assistenza telefonica, con particolare riferimento alla diagnosi dei malfunzionamenti e alla bonifica da "virus informatici".

Le Segreterie Nazionali terranno indenne l'Istituto da eventuali oneri economici correlati ad interventi di manutenzione, riconfigurazione e ripristino di strumenti informatici, elaboratori, connessioni di rete, nonché di programmi ed applicazioni, che dovessero rendersi necessari a seguito di comportamenti in violazione della normativa informatica, posti in essere dagli utenti abilitati ad operare sulle postazioni di lavoro dedicate. Resta ferma la facoltà della Banca d'Italia, in caso di violazioni della normativa di particolare gravità, di risolvere la presente Convenzione con effetto immediato nei confronti della Segreteria Nazionale responsabile.

La Banca d'Italia non risponde di eventuali comportamenti illeciti compiuti, attraverso gli strumenti oggetto della presente Convenzione, nei confronti di altri soggetti. Resta fermo quanto previsto dal richiamato art. 7 della Convenzione per i diritti sindacali in tema di ascrivibilità dei comunicati alle strutture sindacali.

5. Clausole finali

La presente Convenzione ha durata quadriennale e si intende rinnovata tacitamente alla scadenza per due anni e così successivamente, di biennio in biennio, qualora non venga formalmente disdettata dalle parti, con comunicazione scritta, almeno 6 mesi prima di ciascuna scadenza (quadriennale ovvero biennale).

La presente Convenzione è altresì risolta in caso di:
- violazioni della normativa di particolare gravità, secondo quanto previsto al precedente paragrafo 4;
- risoluzione della Convenzione per i diritti sindacali.

Eventuali modifiche saranno concordate tra le parti previa specifica richiesta scritta.

Le parti si danno atto che resta integralmente confermata la disciplina in tema di albi sindacali, contenuta nel ripetuto art. 7 della Convenzione per i diritti sindacali. Decorso un anno dall'attivazione dello spazio nell'Intranet aziendale, le parti si incontreranno per definire una revisione degli spazi destinati all'affissione in un'ottica di razionale utilizzo degli strumenti disponibili.

Per le esigenze tecniche connesse all'utilizzo degli strumenti informatici oggetto della presente Convenzione le Organizzazioni Sindacali si rivolgeranno direttamente alla competente funzione informatica.

Allegato A)

CARATTERISTICHE TECNICHE, FUNZIONALI E DI SICUREZZA DELL'AMBIENTE PER LA BACHECA ELETTRONICA E L'ACCESSO SELETTIVO AD INTRANET

Caratteristiche e configurazione del posto di lavoro

Ogni postazione di lavoro sarà dotata di stampante locale laser monocromatica formato A4; sarà inoltre fornito ad ogni Organizzazione Sindacale uno scanner a colori formato A4 dotato di alimentatore automatico di fogli e software OCR.

Per quanto riguarda il corredo software applicativo, ogni posto di lavoro sarà dotato dei prodotti Microsoft Office (Word, Excel, Power Point) nonché dei prodotti Microsoft FrontPage e Adobe Acrobat Professional per la predisposizione dei documenti e/o delle pagine destinate alla pubblicazione sulla Intranet.

La configurazione sistemistica e di sicurezza dei posti di lavoro sarà conforme agli *standard* e alle *policy* previsti per le postazioni di lavoro Windows XP della Banca collegati alla rete aziendale.

Tenuto conto peraltro della peculiarità dell'ambiente operativo nel quale tali postazioni dovranno essere utilizzate, i PC saranno dotati di presidi di sicurezza volti a ridurre i rischi derivanti dall'utilizzo improprio delle risorse informatiche dell'Istituto. In particolare:

- l'accesso al posto di lavoro sarà consentito, previa autenticazione, alle sole utenze definite per il personale segnalato dall'Organizzazione Sindacale assegnataria della postazione, nonché all'utenza di "amministratore locale" (c.d. utenza "administrator");
- tali utenze, diverse da quelle già attribuite al personale per l'utilizzo in Banca, saranno abilitate ad operare unicamente sui citati posti di lavoro e saranno soggette alle stesse regole di autenticazione e tracciabilità previste per il dominio UTENZE;
- sul posto di lavoro saranno installati i soli componenti software necessari per garantire le funzionalità previste dalla Convenzione;
- dal posto di lavoro sarà consentito l'accesso alle sole risorse informatiche locali e/o remote (applicazioni, dati, servizi) necessarie per garantire la corretta operatività delle suddette funzionalità.

Per maggiori dettagli sui presidi di sicurezza attivi e sulle istruzioni per il corretto utilizzo dei posti di lavoro si fa rinvio all'allegato B).

Funzionalità disponibili

Le funzionalità di "bacheca elettronica" e di "accesso selettivo ad Intranet" saranno rese disponibili avvalendosi dell'ambiente tecnologico e degli strumenti informatici in uso in Banca per la fruizione dei servizi offerti dalla Intranet aziendale.

In relazione alle evoluzioni tecnologiche che potranno interessare tale ambiente, le funzionalità sopra indicate potranno essere oggetto di revisione in termini di strumenti informatici e/o modalità di fruizione. Di tali eventuali evoluzioni sarà data adeguata informativa a tutti gli utenti interessati.

Di seguito si fornisce, per ognuna delle due funzionalità, una sintetica descrizione delle soluzioni applicative previste e dei connessi strumenti informatici a supporto[2].

Bacheca elettronica

Dal punto di vista tecnologico e funzionale la bacheca elettronica sindacale sarà assimilabile alle Intranet locali oggi presenti nell'ambiente Intranet aziendale.

A tal fine il Servizio E.S.I. renderà disponibili i modelli di riferimento utilizzati per le Intranet locali; in alternativa, le Organizzazioni Sindacali potranno realizzare, in autonomia e sotto la propria responsabilità, una veste grafica personalizzata nei limiti e con le modalità consentite dall'ambiente tecnologico oggi in uso per tali ambienti.

La componente server della bacheca elettronica sarà attestata sugli elaboratori collocati presso le strutture centrali gestite dalle competenti funzioni del Servizio E.S.I.. In tale ambiente saranno disponibili le funzionalità per la gestione delle diverse fasi del ciclo di vita dei documenti.

Sarà responsabilità di ogni Organizzazione Sindacale provvedere in autonomia alla corretta gestione dei diritti di accesso ai documenti (*file* e/o "cartelle") contenuti nella propria bacheca elettronica.

Per la predisposizione dei contenuti da pubblicare sulla bacheca elettronica gli utenti si avvarranno degli strumenti software disponibili sui posti di lavoro. L'eventuale acquisizione da fonte esterna di documenti - purché di formato compatibile con gli strumenti di predisposizione presenti sul posto di lavoro - dovrà avvenire nel rispetto delle disposizioni di sicurezza informatica (cfr. allegato B).

In ogni caso le caratteristiche dei documenti e/o delle pagine da pubblicare - in termini, ad esempio, di formato e dimensione - dovranno essere tali da non alterare le condizioni di funzionalità, efficienza e sicurezza degli ambienti informatici aziendali.

Accesso selettivo ad Intranet

Da ogni posto di lavoro sarà possibile accedere alla Intranet aziendale limitatamente alle applicazioni previste dalla Convenzione nonché alle sezioni di interesse delle "Guide

[2] Per i dettagli sulle funzioni disponibili e le relative modalità d'uso si fa rinvio alle specifiche istruzioni riportate nelle "Guide utente" disponibili sulla Intranet aziendale.

utente". Saranno inoltre fruibili le funzioni di utilità generale[3] disponibili per gli utenti della Intranet aziendale.

Livelli di servizio

I livelli di servizio saranno omogenei con quelli in essere per la generalità degli utenti della rete Intranet aziendale.

Con riferimento al servizio di assistenza tecnica e manutenzione dei posti di lavoro e dei relativi dispositivi periferici, le segnalazioni di malfunzionamenti e/o guasti dovranno essere rivolte all'Help-Desk Unificato del Servizio E.S.I. che provvederà per i conseguenti interventi tecnici, in linea con i livelli di servizio previsti per la manutenzione dei posti di lavoro *standard* aziendali.

Le richieste di materiali di consumo EAD (ad es. *toner* per stampanti, supporti di memorizzazione, ecc.) dovranno essere formalmente rappresentate al Servizio E.S.I. con le modalità previste per le diverse tipologie di fornitura.

Eventuali esigenze di supporto connesse con l'utilizzo degli strumenti informatici sopra illustrati potranno essere rivolte al citato servizio di Help-Desk Unificato del Servizio E.S.I.; il personale incaricato di fornire supporto potrà attivare, previo assenso dell'interessato, il servizio di assistenza remota secondo le modalità in uso per la generalità degli utenti della Banca.

[3] Ad esempio: *help*, ricerca, funzioni (quali il *banner*) per la segnalazione di novità e/o di interventi sui sistemi elaborativi, ecc.

Allegato B)

NORMATIVA RIGUARDANTE L'UTILIZZO DI STRUMENTI INFORMATICI

Circolare n. 172 del 1992 – Sviluppo e gestione della risorsa informatica

Circolare n. 184 del 1993 – Norme in materia di sicurezza informatica e relativo Manuale degli *standard* di sicurezza informatica

Circolare n. 257 del 2004 – Disposizioni in materia di trattamento dei dati personali

* * *

In applicazione delle vigenti normative in materia di utilizzo delle risorse informatiche si riportano di seguito le istruzioni specifiche per l'ambiente informatico a disposizione delle Organizzazioni Sindacali. Tali istruzioni integrano le prescrizioni contenute nel M.A. del Servizio E.S.I. n. 658505 dell'8 giugno 2006 ("Windows XP: prescrizioni di sicurezza").

A tal proposito si ricorda che l'uso improprio delle risorse informatiche costituisce una fonte di rischio per il patrimonio informativo dell'Istituto.

Comunicazione del Responsabile per la sicurezza informatica

Ogni Organizzazione Sindacale dovrà comunicare formalmente al Servizio E.S.I. e per conoscenza al Servizio Personale I.N.E., tramite lettera conforme allo schema riportato nell'Allegato "S/0", il nominativo di un dipendente dell'Istituto che, per conto dell'Organizzazione Sindacale, assume il ruolo di responsabile per quanto attiene ai profili di sicurezza connessi con l'utilizzo degli strumenti informatici a disposizione dell'Organizzazione Sindacale e la gestione delle relative utenze[4].
Ferme restando le responsabilità individuali di ciascun utente finale, il suddetto nominativo assume il ruolo di Responsabile dei profili di sicurezza con riferimento in particolare a:

- le richieste di creazione, revoca e cancellazione delle utenze di pertinenza della propria sigla sindacale nonché le richieste di riattivazione e riassegnazione delle password delle suddette utenze[5];
- la gestione delle utenze privilegiate definite sul posto di lavoro (utenza di tipo "administrator" e relative password, password di "setup" e password di accensione);
- la gestione degli incidenti virali e i connessi adempimenti;

---

[4] Di seguito indicato come "Responsabile". Sarà cura dell'Organizzazione Sindacale comunicare formalmente al Servizio E.S.I. ogni variazione, anche temporanea, relativa al nominativo incaricato di svolgere tale ruolo.

[5] Il Servizio E.S.I. darà seguito alle richieste relative alle utenze sindacali solo se pervenute dal nominativo indicato come Responsabile.

- la manutenzione del posto di lavoro (custodia della chiave fisica del PC, adempimenti connessi con gli interventi di assistenza tecnica e manutenzione hardware e software e con le richieste di materiali di consumo);
- la sensibilizzazione degli utenti finali in ordine all'utilizzo degli strumenti informatici aziendali nel pieno rispetto della normativa vigente (rispetto del *copyright*, utilizzo del solo software aziendale, non alterazione della configurazione dei sistemi, rispetto della legge sulla *privacy*, ecc.).

Istruzioni per il Responsabile

Di seguito sono riportati gli adempimenti operativi a carico del Responsabile con riferimento alle richieste di abilitazioni delle utenze sindacali, alla gestione della sicurezza fisica e logica del posto di lavoro e alla gestione degli incidenti virali.

Richieste di abilitazioni

Tutte le richieste relative ad abilitazioni (creazione, revoca e cancellazione dell'utenza sindacale, riattivazione e riassegnazione della password), di competenza del Responsabile, saranno formalmente indirizzate al Servizio E.S.I. e, per conoscenza, al Servizio Personale I.N.E., tramite invio di lettere conformi agli schemi riportati negli allegati. Eventuali richieste urgenti potranno essere anticipate via fax e successivamente formalizzate.

- Creazione, revoca e cancellazione di una utenza sindacale

Per le richieste di creazione di un'utenza sindacale, ovvero di revoca o cancellazione di un'utenza sindacale già attribuita, il Responsabile avrà cura di effettuare la segnalazione conformemente allo schema riportato nell'Allegato "S/1".

La nuova USERID sindacale sarà definita dal Servizio E.S.I. utilizzando la stessa nomenclatura in uso per la USERID di UTENZE già in carico all'interessato, previa sostituzione del primo carattere con la lettera "s". A tal proposito si rammenta che, come di consueto, ogni situazione anomala dovrà essere prontamente segnalata al Servizio E.S.I..

In caso di cessazione dal servizio dell'utente assegnatario della USERID sindacale, il Servizio E.S.I. procederà d'ufficio alla cancellazione di tale utenza.

- Riattivazione e riassegnazione della password di una USERID sindacale

Per le richieste di riattivazione e di riassegnazione della password di una USERID relativa a un'utenza sindacale già attribuita, il Responsabile avrà cura di effettuare la segnalazione conformemente allo schema riportato nell'Allegato "S/2".

- Modalità di prima assegnazione di un'utenza sindacale e di riassegnazione della password

Nel caso di prima assegnazione di un'utenza sindacale o di riassegnazione della password, il Servizio E.S.I. provvederà a comunicare all'assegnatario la USERID e/o la relativa password tramite l'invio di un plico sigillato accompagnato da comunicazione formale indirizzata al Responsabile. Il Responsabile curerà la consegna di tale plico all'interessato il quale, dopo averne controllato l'integrità, confermerà l'avvenuta ricezione apponendo data e firma sul modulo di accompagnamento che verrà conservato a cura del Responsabile.

Gestione della sicurezza fisica e logica del posto di lavoro

Il Responsabile deve farsi carico della gestione delle utenze privilegiate di ogni posto di lavoro (utenza di tipo "administrator" e relative password, password di "setup" e password di accensione), nonché della chiave fisica di chiusura del "*cabinet*", provvedendo a conservarle con ogni possibile cautela, secondo quanto indicato dalla normativa vigente in materia. Sarà altresì cura del Responsabile conservare le eventuali copie delle chiavi di crittografia EFS[6] con le relative indicazioni della USERID e del PC di riferimento.

- Utilizzo dell'utenza di tipo "administrator" e impostazione della relativa password

L'utilizzo dell'utenza di tipo "administrator" è soggetto alle stesse restrizioni previste per le postazioni di lavoro aziendali. A tal proposito si ricorda che l'utenza di tipo "administrator", da non condividere con gli utenti finali, potrà essere utilizzata solo in casi eccezionali quali, ad esempio:

- interventi di assistenza tecnica e manutenzione del posto di lavoro;
- interventi di aggiornamento della configurazione software del posto di lavoro;
- bonifica virus.

Sarà cura del Responsabile provvedere all'impostazione della password dell'utenza di tipo "administrator", in occasione della prima installazione del posto di lavoro nonché a seguito di una sua reinstallazione o di un intervento di ripristino del disco di sistema.

- Utilizzo e impostazione della password di "setup" e della password di accensione

Su ogni posto di lavoro è predisposta una password di "setup" che protegge l'accesso alle funzioni di configurazione dell'hardware della macchina; tale configurazione, analogamente a quanto avviene sui posti di lavoro aziendali, deve prevedere l'inizializzazione del sistema operativo (*bootstrap*) prioritariamente dal disco fisso.
L'utilizzo della password di "setup" è soggetto alle stesse restrizioni previste per le postazioni di lavoro aziendali. Essa potrà essere utilizzata in caso di manutenzione o ripristino del PC.
Sarà cura del Responsabile provvedere all'impostazione della password di "setup" al termine della prima installazione del posto di lavoro e dopo ogni successivo intervento che ne richieda l'utilizzo.

Allo stesso modo il Responsabile dovrà impostare la password di accensione del posto di lavoro da consegnare agli utenti che opereranno sul PC stesso.

Gestione degli incidenti virali

Nel caso in cui sia stata rilevata la presenza di un virus sul disco fisso del PC è necessario procedere con la rimozione del virus (c.d. "bonifica"), segnalando tempestivamente l'accaduto al Servizio ESI.
Gli adempimenti relativi alle operazioni di bonifica e di stampa delle relative evidenze saranno svolti in collaborazione con il Servizio E.S.I.. In tale occasione sarà cura del Responsabile compilare il verbale secondo lo schema riportato nell'Allegato "S/3" e consegnarne copia al Servizio E.S.I.. Il Servizio E.S.I., in conformità alla normativa vigente, invierà copia del suddetto verbale all'Ispettorato Banca.
Nel caso in cui le operazioni di bonifica richiedessero l'utilizzo dell'utenza di tipo "administrator" o della password di "setup" del PC, al termine delle attività sarà cura del Responsabile provvedere a modificare la password utilizzata.

---

[6] Cfr. paragrafo "Istruzioni per gli utenti finali - Protezione dei dati".

Istruzioni per gli utenti finali

L'utente finale è responsabile dell'utilizzo degli strumenti informatici aziendali nel pieno rispetto della normativa vigente (rispetto del *copyright*, utilizzo del solo software aziendale, non alterazione della configurazione dei sistemi, ecc.).
In tale ambito l'utente ha la responsabilità della corretta gestione dei dati locali sul PC al fine di assicurarne integrità, disponibilità e riservatezza anche ai fini della *privacy*.
In proposito si ricorda l'importanza di effettuare salvataggi periodici dei dati di interesse su supporti rimovibili al fine di evitarne la perdita a seguito di malfunzionamenti del sistema o di cancellazioni accidentali.

E' altresì a carico dell'utente finale la corretta gestione delle proprie credenziali di autenticazione che non possono essere in alcun caso condivise con altri utenti.

Protezione antivirus e protezione della rete aziendale

Il posto di lavoro è protetto dal software antivirus per la prevenzione delle minacce indotte da codice malevolo. Tale software è sottoposto a meccanismi di aggiornamento automatico, con periodicità almeno giornaliera. Tali meccanismi sono trasparenti agli utenti finali, i quali hanno comunque l'obbligo di verificare lo stato di funzionamento e di aggiornamento dell'antivirus sul posto di lavoro, segnalando al Servizio E.S.I. eventuali anomalie. Le istruzioni operative per la verifica dello stato del software antivirus sono riportate nella guida utente "Manuale d'uso del prodotto antivirus McAfee VirusScan Enterprise versione 8.0i" al paragrafo "Procedure operative per la verifica dello stato di funzionamento dell'antivirus", disponibile sulla Intranet aziendale.

In caso di rilevazione virus, il software antivirus ne prevede la segnalazione automatica all'utente finale e al sistema di gestione centralizzato, amministrato dal Servizio E.S.I.. In tal caso l'utente deve provvedere all'immediata disconnessione del PC infetto dalla rete aziendale e segnalare tempestivamente l'accaduto al Responsabile, al fine di avviare le procedure, da effettuare in collaborazione con il Servizio E.S.I., per la rimozione del virus (c.d. bonifica) e i relativi adempimenti amministrativi previsti dalla normativa vigente.

Al fine di prevenire possibili infezioni virali si ribadisce l'obbligo di:

- non alterare la configurazione presente sul posto di lavoro;
- utilizzare esclusivamente i programmi resi disponibili dal Servizio E.S.I.;
- sottoporre al controllo antivirus il contenuto di tutti i supporti rimovibili preventivamente al loro utilizzo sul PC;
- verificare il corretto funzionamento del software antivirus e del periodico aggiornamento delle impronte;
- segnalare al Servizio E.S.I. ogni possibile anomalia di funzionamento riscontrata.

Oltre al presidio antivirus il posto di lavoro è dotato di uno specifico presidio di sicurezza, basato sul software *Personal firewall*, volto a proteggere la postazione di lavoro da accessi indebiti da e verso la rete aziendale.
Analogamente a quanto previsto per il software antivirus, eventuali rilevazioni di accessi anomali via rete saranno inviati automaticamente dal software *Personal firewall* al sistema di gestione centralizzato, amministrato dal Servizio E.S.I..

Protezione dei dati

Al fine di proteggere i dati e le informazioni residenti sul posto di lavoro l'utente può utilizzare i meccanismi di controllo accessi ACL (*Access Control List*) resi disponibili dal sistema operativo Windows XP. Tali meccanismi consentono all'utente di impostare e definire quali utenti (USERID) possono accedere e con quali diritti a *file* e cartelle

(*directory*) presenti sul PC. Le istruzioni operative sono descritte nella guida utente "Configurazione delle ACL (Access Control List) sul posto di lavoro Windows XP", disponibile sulla Intranet aziendale.

Qualora l'utente intenda proteggere dati ritenuti particolarmente critici sotto il profilo della riservatezza potrà avvalersi della funzione di crittografia EFS (*Encrypting File System*), resa disponibile dal sistema operativo Windows XP, salvando su un supporto rimovibile la relativa chiave di crittografia e consegnandone una copia al Responsabile.
Tale chiave, collegata alla USERID e al PC su cui risiedono i dati crittografati, è infatti necessaria per garantirne il recupero in caso di problemi tecnici o di indisponibilità dell'utente assegnatario della USERID.
Le istruzioni da seguire per il salvataggio e il ripristino di tale chiave sono riportate nella guida utente "Crittografia EFS sul posto di lavoro Windows XP", disponibile sulla Intranet aziendale.

ALLEGATO "S/0"

[Intestazione della Organizzazione Sindacale]

AL CAPO DEL SERVIZIO
ELABORAZIONI E SISTEMI INFORMATIVI
e p.c.
AL CAPO DEL SERVIZIO PERSONALE
INQUADRAMENTO NORMATIVO ED ECONOMICO

Oggetto: Segnalazione del Responsabile della sicurezza informatica.

Nominativo: .....

USERID di UTENZE: .....

Data: .....

Firma per accettazione del Responsabile della sicurezza informatica

[Nominativo]

(firma leggibile)

.....

Il Presidente / Il Segretario Nazionale dell'Organizzazione Sindacale

[Nominativo]

(firma leggibile)

.....

ALLEGATO "S/1"

[Intestazione della Organizzazione Sindacale]

AL CAPO DEL SERVIZIO
ELABORAZIONI E SISTEMI INFORMATIVI
e p.c.
AL CAPO DEL SERVIZIO PERSONALE
INQUADRAMENTO NORMATIVO ED ECONOMICO

Oggetto: richiesta di creazione / revoca / cancellazione di un'utenza sindacale.

Nominativo: .....

USERID di UTENZE: .....

Nome Logico del PC e Serial Number: .....

Nome Logico del PC e Serial Number: .....

Si richiede per il nominativo sopra indicato (barrare la casella che interessa):

- ☐ Creazione della USERID sindacale e prima assegnazione della password
- ☐ Revoca della USERID sindacale ..... (indicare la USERID)
- ☐ Cancellazione della USERID sindacale ..... (indicare la USERID)

Data: .....

Il Responsabile della sicurezza informatica

[Nominativo]

(firma leggibile)

.....

ALLEGATO "S/2"

[Intestazione della Organizzazione Sindacale]

AL CAPO DEL SERVIZIO
ELABORAZIONI E SISTEMI INFORMATIVI
e p.c.
AL CAPO DEL SERVIZIO PERSONALE
INQUADRAMENTO NORMATIVO ED ECONOMICO

Oggetto: richiesta di riattivazione / riassegnazione della password.

Nominativo: .....

USERID sindacale: .....

Si richiede per la USERID sindacale sopra indicata (barrare la casella che interessa):

- ☐ Riattivazione (RESUME) della password
- ☐ Riassegnazione della password

per i seguenti motivi (barrare la casella che interessa):

- ☐ Dimenticanza
- ☐ Revoca, a seguito di reiterati tentativi di accesso con password errata
- ☐ Altre motivazioni:.....

.....

Data: .....

L'utente assegnatario della USERID sindacale

[Nominativo]

(firma leggibile)

.....

Il Responsabile della sicurezza informatica

[Nominativo]

(firma leggibile)

.....

ALLEGATO "S/3"

[Intestazione della Organizzazione Sindacale]

VERBALE DI VERIFICA PRESENZA VIRUS INFORMATICI

A) Data di individuazione del virus: .....

B) Occasione nella quale il virus è stato rilevato: .....

C) Tipo di virus rilevato: .....

D) Numero di supporti infetti: .....

E) Numero di P.C. infetti: .....

F) Nome Logico del PC e Serial Number: .....

.....

G) Causa presunta dell'insediamento del virus: .....
.....

H) Eventuali conseguenze derivanti dall'infezione:.....
.....

I) Descrizione delle azioni intraprese:.....
.....

J) Nominativo del Tecnico del S.E.S.I. presente all'intervento.....

Allegare al presente verbale la stampa dei messaggi relativi
all'esito delle operazioni di verifica e successiva bonifica

Data: .....

Il Responsabile della sicurezza informatica

[Nominativo]

(firma leggibile)

.....

Il Tecnico del S.E.S.I. presente all'intervento

[Nominativo]

(firma leggibile)

.....

Le Organizzazioni Sindacali firmano il presente accordo con riserva di ratifica definitiva entro il 4 luglio 2008.

La Delegazione dell'Amministrazione stipula il presente accordo per conto del Direttore Generale con riserva di sottoporlo al Governatore, il quale lo valuterà in sede di Consiglio Superiore affinché l'accordo stesso sia approvato o respinto nel suo complesso.

PER L'AMMINISTRAZIONE

PER LA FISAC-CGIL

PER IL SINDIRETTIVO-CIDA

PER IL SIBC-CISAL

PER LA FABI

PER LA FIBA-CISL

PER LA UILCA-UIL