Ministero
per i Beni e le Attività Culturali
Direzione generale per l'Organizzazione, l'Innovazione,la Formazione, la Qualificazione professionale e le Relazioni sindacali
Servizio II

Circolare n. 53

Roma, 12 MAR. 2008

Ai Direttori degli Uffici e Istituti centrali e periferici

LORO SEDI

Prot. N° 6788
Class. 16.34.13|2

Allegati N° 1

Risposta al foglio del
N°

Oggetto: Progetto formazione e sensibilizzazione dei dipendenti della Pubblica Amministrazione in materia di sicurezza ICT

Per opportuna conoscenza e massima diffusione si comunica l'iniziativa organizzata dal Ministero delle Comunicazioni – Istituto Superiore C.T.I., relativa al progetto indicato in oggetto, di cui si allega il programma.

Le domande di partecipazione dovranno essere consegnate all'istituto di appartenenza, il quale farà pervenire a Questa Direzione Generale, entro e non oltre il 4 aprile 2008, al numero di fax 06-67232216, unicamente quelle per le quali potrà garantire copertura finanziaria relativa al trattamento di missione (si fa presente che l'iscrizione al corso non comporta spese); le istanze prive di tali indicazioni non saranno prese in considerazione.

Si fa presente che questa Direzione Generale non potrà sostenere le spese relative alla partecipazione al progetto in argomento.

Per ulteriori informazioni sui corsi, contattare l'Ing. Giuseppe Pierri dirigente responsabile del progetto presso l'Istituto, tel. 06-54442271.

Il Direttore del Servizio II
(Dr. Mauro Cotone)

00100 Roma

PROT.N.IST/5/2/FORM/SIC-ICT
Citare nella risposta tutti i dati compresi nel riquadro

MINISTERO DELLE COMUNICAZIONI

ISTITUTO SUPERIORE C.T.I
Ufficio 5°

ALLEGATI:.....
RISP.AL PROT.....
DEL.....

Alle Amministrazioni Pubbliche – Ufficio FORMAZIONE del PERSONALE

Oggetto: Progetto Formazione e Sensibilizzazione dei dipendenti della Pubblica Amministrazione in materia di **sicurezza ICT.**

Per incrementare la "Sensibilità" al tema della sicurezza ICT attraverso lo sviluppo di un'adeguata consapevolezza relativamente a minacce, vulnerabilità e rischi che possono gravare sul patrimonio informativo della P.A. Centrale, con DM 14 maggio 2003, il Comitato dei Ministri per la Società dell'Informazione ha dato mandato all'Istituto Superiore delle Comunicazioni di realizzare un piano di formazione e sensibilizzazione dei dipendenti della Pubblica Amministrazione in materia di sicurezza ICT.

Questo Istituto Superiore, per il prosieguo di tale progetto, ha in programma l'erogazione di un corso di formazione e sensibilizzazione in aula, rivolto agli addetti e/o tecnici amministratori ICT, appartenenti all'Amministrazione Pubblica Centrale.

Si prevede l'esecuzione di 40 sessioni di formazione, per un totale di circa 800 utenti. Ciascuna sessione di corso avrà una durata di 72 ore distribuite su 10 giornate lavorative.

I corsi si svolgeranno a Roma secondo un calendario in fase di definizione .

Il personale oggetto dell'intervento formativo dovrà possedere conoscenze informatiche di base, di natura teorico e/o pratica, in relazione ai seguenti argomenti:

- Principi di base del funzionamento di sistemi operativi e programmi;
- Reti locali: installazione e configurazione;
- Architetture e servizi di rete;
- Applicazioni web, applicazioni server;
- Propensione a trasferire i contenuti del corso all'interno dell'amministrazione;

L'elenco dei candidati dovrà essere comunicato, **in ordine di priorità**, indicando il nome di un referente con i relativi recapiti di ciascun partecipante.

Considerata l'importanza degli argomenti trattati, si confida nella massima partecipazione di tutti i tecnici interessati, dando maggiore rilievo al tipo di attività svolta.

Le risposte di adesione, dovranno essere comunicate al seguente indirizzo:

Istituto Superiore CTI - Uff.5° - Viale America 201 – 00144 – Roma – Fax: 065410904.

Inviare le risposte anche per E-MAIL all'indirizzo: aurelio.monti@comunicazioni.it

Per ogni ulteriore informazione, relativa al progetto, si può contattare l'Ing Giuseppe Pierri, Dirigente Responsabile del Progetto. Tel. 06/5444.2271-cell. 3349008527-fax 065410904 E-Mail: giuseppe.pierri@comunicazioni.it..

IL DIRETTORE
(Dott. Marcello Fiori)

Ministero delle Comunicazioni

CORSO di FORMAZIONE per i DIPENDENTI della PA in MATERIA DI SICUREZZA ICT

ELENCO dei MODULI

MODULO I
Tecniche di comunicazione

Obiettivo: fornire ai partecipanti le tecniche di comunicazione utili a relazionarsi con colleghi sia in aula, sia in attività di tutoraggio, sia nella normalità della vita lavorativa. Lo scopo primario del modulo formativo intende selezionare le diverse tipologie comunicative, le regole ed i criteri per ottimizzare la comunicazione .

Contenuti: Principi di comunicazione relazionale e comunicazione organizzativa.
La leadership: la leadership nel gruppo, il conflitto e la negoziazione come processo organizzativo e di cambiamento (gestione delle riunioni e del tempo).
Formazione e tutoraggio: come relazionarsi con uditori diversi. Il ruolo del facilitatore nel processo formativo.
Tecniche e strumenti di informazione e comunicazione diretta e mediata (tramite i media tradizionali e i new media).

MODULO II
Introduzione alla sicurezza informatica

Obiettivo: introdurre i partecipanti al tema della sicurezza ICT

Contenuti: Confidenzialità, autenticazione, integrità e non ripudio di documenti e comunicazioni.
Controllo di accesso ai sistemi e ai dati.
Disponibilità dei servizi e dei dati.

MODULO III
Sintesi delle vulnerabilità e delle minacce dei sistemi informatici

Obiettivo: Presentare una panoramica delle vulnerabilità più diffuse dei sistemi software e delle reti al fine di sensibilizzare i partecipanti circa esistenza e diffusione di minacce nei sistemi tipicamentre in uso nella PA.

Contenuti: Vulnerabilità del software: input fidato e non fidato, validazione dell'input. Attacchi di tipo buffer overflow. Ubiquità del problema a livello di applicazioni, server, librerie e applicazioni in linguaggi interpretati. Applicazioni via Web, application servers ed attacchi di tipo SQL injection.
Modalità di sfruttamento (exploitation) dei bug di tipo buffer overflow: priviledge excalation, intrusioni via rete tramite servizi aperti, intrusione via documenti non fidati (via email, via web o altro). Strumenti per la generazione automatica degli exploit (es. metasploit.com).
Script kiddies e software malevolo. Vari aspetti di software malevolo: virus, worm, cavalli di Troia, rootkit, backdoors, sniffer, spyware, adware, ecc.
Vulnerabilità delle reti locali (protocolli in chiaro, sniffing), delle reti locali switched e del protocollo ARP (ARP poisoning), vulnerabilità del DNS. Session hijecking, attacchi MitM. Attacchi MitM di protocolli criptati (ssh). L'importanza dell' autenticazione.
Vulnerabilità delle password: la potenza degli attacchi a compleanno sugli hash, vulnerabilità dei

protocolli di autenticazione in windows e dei sistemi di memorizzazione delle password nei sistemi operativi.
Statistiche sull'incidenza delle varie tipologie di attacco.

MODULO IV

Tecnologie per la sicurezza informatica

Obiettivo: fornire una panoramica delle tecnologie e delle metodologie di progetto usate per la mitigazione del rischio, sia nell'ambito delle reti che nell'ambito dei sistemi e delle applicazioni. I partecipanti dovranno essere messi in grado di comprendere documenti tecnici che descrivono soluzioni per la sicurezza informatica .

Contenuti: Crittografia a chiave pubblica e a chiave simmetrica. Firma digitale. Certificati. Infrastrutture a chiave pubblica. Esempi di tecnologie di rete basate su metodi crittografici (PGP, S/MIME, SSL, IPSEC e VPN). La posta elettronica certificata.
La sicurezza delle reti: VLAN, screening router, firewall, firewall applicativi, proxy, intrusion detection system su rete. Continuità del servizio: ridondanza della rete e delle apparecchiature. Colli di bottiglia tipici (es. firewall). Load balancing. Autenticazione degli utenti tramite 802.1X e Radius e sue vulnerabilità.
La sicurezza dei sistemi: autenticazione, autorizzazione, (discretionary) access control, logging, log auditing, host based intrusion detection systems e intrusion prevention systems. L'antivirus come sistema integrato di protezione. Mandatory access control. Ridondanza e configurazioni high availability.
Progetto di reti "compartimentate" ed esempi di architetture di reti sicure con DMZ. Importanza della protezione fisica degli apparati. Politica di hardening dei calcolatori, mantenimento, tracking dei security alert, applicazione delle patch di sicurezza, ecc.
Controllo dei sistemi e delle reti mediante IDS e analisi dei log, contrasto automatico degli attacchi di rete mediante architetture firewall-IDS. Cenni alle tecniche di analisi forense dopo l'attacco. Politiche di backup e problematiche correlate.

MODULO V

Normativa sulla sicurezza informatica nella pubblica amministrazione

Durata orientativa: 7,20 ore

Obiettivo: fornire una panoramica sulla normativa che vincola le pubbliche amministrazioni in materia di sicurezza informatica e sulle responsabilità delle amministrazioni e degli individui.

Contenuti: Normative circa il trattamento dei dati (Codice della Privacy). Responsabilità della PA e del personale dipendente.
Vincoli normativi rispetto al monitoraggio dei sistemi e delle reti (privacy dei dipendenti). Uso dei disclaimer e delle note informative.
Diritto d'autore (detenzione di materiale piratato nei sistemi della pubblica amministrazione, pubblicazione di materiale su web), responsabilità dei dipendenti e della pubblica amministrazione.
Quadro normativo per la firma digitale.
Cenni al codice per l'amministrazione digitale, alle norme circa il protocollo informatico e alla gestione elettronica dei documenti

MODULO VI

Gestione della sicurezza

Obiettivo: introdurre i principali aspetti organizzativi legati alla sicurezza informatica; e degli obblighi di legge connessi tra cui la redazione del documento programmatico sulla sicurezza; mettere in grado i partecipanti di curare gli aspetti tecnici e contrattuali legati alla sicurezza informatica con particolare riguardo alla la redazione dei capitolati di gara

Contenuti: Vantaggi organizzativi dalla redazione di un piano di sicurezza: diffusione

dell'informazione, tracciamento del processo, verifica dei risultati, ecc.
Analisi e valutazione del rischio. Metodologie quantitative e qualitative: pro e contro, linee guida per la scelta. Casi di studio. Vulnerabilità legate alle risorse umane: statistiche. Gestione password e meccanismi alternativi di autenticazione (pro e contro). Social engineering: centralini, call center, ecc. Trattamento dei rischi. Probabilità dell'evento avverso, entità del rischio e proattività/reattività delle contromisure. Processi di bussiness con vari livelli di criticità: tempi e costi delle soluzioni. Procedure di risposta agli incidenti. Business continuity. Disaster recovery.
Criteri per gestire i rapporti con i fornitori riguardo la sicurezza: verificabilità e collaudabilità dei requisiti, contrattualizzazione delle verifiche. Certificazione dei prodotti secondo lo standard Common Criteria. Qualità e continuità dei servizi informatici: legami con la qualità del software e la tolleranza ai guasti. Applicazione alla preparazione dei capitolati di gara.
Linee guida per la preparazione del documento programmatico sulla sicurezza e obblighi normativi. Esempi di Documento Programmatico sulla Sicurezza.
Valutazione della sicurezza di una organizzazione. Il principio della separazione dei compiti ("chi esegue non verifica"). BS7799 parte 1. Certificazione BS7799 parte 2.
Comitato Tecnico Nazionale per la Sicurezza ICT: proposte strategiche.
Organizzazione locale della sicurezza (CERT-AM): obiettivi, organizzazione, ruoli e responsabilità. Figure professionali coinvolte: aspetti tecnici e di comunicazione con gli utenti. govCERT.it: early warning, supporto e coordinamento di risposta agli incidenti, coordinamento della risposta alla gestione dei codici pericolosi. Osservatorio tecnologico. Raccolta e condivisione di informazioni. Disseminazione di informazioni. Interazione con i CERT-AM.
Il codice dell'amministrazione digitale.

Ministero delle Comunicazioni

ISTITUTO SUPERIORE C.T.I
Ufficio 5°

Ing.Giuseppe Pierri
dirigente responsabile del progetto
tel.: 06 5444.2271 - E-Mail: giuseppe.pierri@comunicazioni.it..