Seminario Gratuito
"Information Security Management"

Roma, Giovedì 26 Marzo 2015
Personal Computing Studio – PCSNET Roma
Via Valadier 33 – 00193 Roma
Orario: 9.00 – 12.45

Argomenti del Seminario

Scopo del seminario è quello di fornire una panoramica sull' Information Security Management evidenziando gli standard di riferimento, i diversi approcci metodologici e le principali criticità di gestione.
Lo standard ISO/IEC 27001:2013 definisce le linee guida necessarie ad implementare, utilizzare, aggiornare e manutenere un sistema di gestione della sicurezza delle informazioni (Information Security Management System) il cui obiettivo è quello di preservare la riservatezza, l'integrità e la disponibilità dei dati mediante l'applicazione di un processo di gestione del rischio.
Esso dovrà integrarsi con tutti i processi dell'organizzazione ed essere considerato nella progettazione di nuovi processi e dei sistemi informativi.
La comprensione e l'utilizzo di un approccio metodologico di questo tipo nasce dalla necessità di rispondere a diversi interrogativi:

- Quali sono i rischi informatici significativi per l'organizzazione?
- Come può, la loro concretizzazione, impattare sui processi e sui servizi in termini di business?
- Come ridurre al minimo i rischi legati alla sicurezza dei dati?
- Quali asset possono essere definiti vitali e devono essere protetti per primi?
- Quali sono i passi da compiere al verificarsi di un "disastro"?

Durante il workshop cercheremo di rispondere a queste domande sviscerando i seguenti punti:

- Analisi della norma ISO/IEC 27005 (Information Security Risk Management) inserita nel più ampio contesto della ISO/IEC 27001 (Information Security Management System).
- Valutazione delle minacce e delle vulnerabilità più comuni dei sistemi informativi e del conseguente innalzamento dei livelli di rischio.
- Attuazione delle contromisure, necessarie a mitigare i rischi, attraverso l'utilizzo di Intrusion Detection Prevention Systems.
- Identificare i processi vitali per il business ed individuare gli impatti causati dagli eventi "disastrosi": la Business Impact Analysis (BIA).
- Reagire al disastro: comprensione dei processi di Business Continuity e di Disaster Recovery e la redazione dei Piani Operativi corrispondenti.
- Visione dell'attività intrapresa dall'Agenzia per l'Italia Digitale (AgID) sulle nuove "Linee Guida per il Disaster Recovery (DR) delle PA e le normative corrispondenti.
- Le peculiarità dello Studio di Fattibilità Tecnica, dei piani di Disaster Recovery e di Continuità Operativa della Pubblica Amministrazione.

Alla fine sarà data una panoramica tecnologica sui prodotti che possono servire per implementare il Disaster Recovery.

Ai partecipanti sarà offerto un **Voucher Formativo del valore di € 500,00** utilizzabile per l'iscrizione di una persona ad un **Corso a Calendario** di durata pari o maggiore a 3 giorni ed avente come destinatari Professionisti IT o Sviluppatori. Il Voucher Formativo avrà **validità fino al 31/12/2015**.

Agenda

Orario	Argomento
09.00 – 09.30	Welcome Coffee e Registrazione dei Partecipanti
09.30 – 10.15	Introduzione alla norma ISO/IEC 27001 e analisi dell'Information Security Risk Management Process (ISO/IEC 27005)
10.15 – 11.00	Sicurezza dei sistemi informativi: limitare le vulnerabilità attraverso l'utilizzo di Intrusion Detection Prevention Systems
11.00 – 11.15	Coffee Break
11.15 – 11.45	Business Continuity e Disaster Recovery: approcci metodologici
11.45– 12.30	Studio di Fattibilità Tecnica, Linee Guida per il Disaster Recovery e la Continuità Operativa nelle Pubbliche Amministrazioni
12.30 – 12.45	Domande e Risposte Offerta Corsi di PCS – PCSNET Roma