GESTIÓ DE LA CIBERSEGURETAT EN L'ENTORN DEL TELETREBALL

Temario (**20 HORAS**):

1. Cyberespai, cyberseguretat i seguretat de la informació
2. Situació actual del cyberespai i factors d'amenaça
3. Els 4 cyberatacs més habituals contra PIMES
4. Defensa d'una Pime en el cyberespai
5. Entenent i gestionant el risc
6. Salvaguardant la seva informació
7. Treballar de forma segura, també en remot
8. Exemples d'atacs actuals i com actuaríem ara

15 HORAS PRESENCIALES. 5 HORAS ON LINE

Objectius:
- Coneix les diferències existents entre cyberespai, cyberseguretat i seguretat de la informació.
- Aprèn a identificar els diferents actors d'amenaça presents en el cyberespai i la seva situació actual.
- Ser conscient dels quatre cyberatacs més habituals contra PIMES i aprèn a defensar-te contra ells.
- Aprèn a treballar de forma segura en remot gestionant el risc i salvaguardant la seva informació.

CALENDARIO:

Lunes 25/4	Martes 26	Miérc. 27	Jueves 28	Viernes 29	Sábado 30	
Grupo A 1ª SESIÓN 25/30 alumnos 17.30 a 22.30 Total 5h.	Grupo B 1ª SESIÓN 25/30 alumnos 17.30 a 22.30 Total 5h.	Grupo A 2ª SESIÓN 25/30 alumnos 17.30 a 22.30 Total 5h.	Grupo B 2ª SESIÓN 25/30 alumnos 17.30 a 22.30 Total 5h.		Grupo A 3ª SESIÓN 25/30 alumnos 9.30 a 14.30 Total 5h.	

Lunes	Mares	Miércoles	Jueves	Viernes	Sábado 7 de mayo
					Grupo B 3ª SESIÓN 25/30 alumnos 9.30 a 14.30 Total 5h.

La plataforma ON LINE ESTARÁ ABIERTA Y COLGADOS LOS CONTENIDOS DESDE **EL 25 DE (Inicio 25/26)** **HASTA EL 10 de mayo**. Examen final on line.

SEGURETAT A INTERNET I DISPOSITIUS MÒBILS

Temario (**30 HORAS**):

1. Amenaces i riscos: terminologia, amenaces a la seguretat informàtica, riscos
2. Autenticació: control d'accés, contrasenyes, autenticació de dos factors
3. Virus informàtics: tipus de virus, vectors d'atac, prevenció de la infecció
4. Xarxes i comunicacions: fonaments, desafiaments de seguretat, estàndards
5. Seguretat de xarxa: firewalls, xarxes privades virtuals, detecció / prevenció d'intrusions
6. Aspectes legals: les lleis de seguretat cibernètica, la recuperació dels ataquis
7. Gestió de riscos de seguretat: anàlisi i gestió de riscos

22 HORAS PRESENCIALES. 8 HORAS ON LINE

Objectius:
- Conèixer les amenaces presents a Internet.
- Transaccions per Internet.
- Configurar adequadament la seguretat i privadesa en xarxes socials.
- Configurar adequadament les polítiques de seguretat de l'equip.
- Mantenir i protegir adequadament l'equip i la seva connexió a les xarxes.
- Utilitzar eines de seguretat i mètodes específics per a diferents dispositius amb accés a Internet.
- Sensibilitzar davant els riscos d'Internet.

MAYO 2022

LUN 16	Mart 17	Mierc 18	Jueves 19	Viernes 20	Sábado 21
Grupo A 1ªSesión 25/30 Alumnos 18 A 22.30 4.30 H	Grupo B 1ªSesión 25/30 Alumnos 18 A 22.30 4.30 H.	Grupo A 2ªSesión 25/30 Alumnos 18 A 22.30 4.30 H.	Grupo B 2ªSesión 25/30 Alumnos 18 A 22.30 4.30 H.	Grupo A 3ªSesión 25/30 Alumnos 18 A 22.30 4.30 H.	Grupo B 3ªSesión 25/30 Alumnos 9.30 A 14.00 4.30 H.

Lun 23	Mart 24	Mierc 25	Jueves 26	Viernes 27	Sábado 28
Grupo A 4ªSesión 25/30 Alumnos 18 A 22.30 4.30 H.	Grupo B 4ªSesión 25/30 Alumnos 18 A 22.30 4.30 H.			Grupo A 5ª Sesión 25/30 Alumnos 18 A 22.00 4 H.	Grupo B 5ª Sesión 25/30 Alumnos 9.30 A 13.30 4 H.

Inicio del curso el **16/17 de mayo**. Finalización **31 de mayo**, fecha hasta la que estará abierta la plataforma on line del curso.

INTRODUCCIÓ A CIBERSEGURETAT

Temario (**25 HORAS**):

1. Fonaments
1.1. Fonaments de Seguretat.
1.2. Riscos.
1.3. Amenaces.

2. Polítiques de Seguretat Informàtica
2.1. Gestió de la ciber Seguretat.
2.2. Polítiques de Seguretat.
2.3. Mesures de protecció.

3. Seguretat física i seguretat lògica
3.1. Dispositius tamper-proof.
3.2. Side channel anàlisi.
3.3. Software Defined Radio i Cognitive Radio Networks.
3.4. Control d'accés.

4. Accés remot
4.1. Interconnexió remota de seus.
4.2. Demostració pràctica de diferents xarxes privades virtuals.

5. Control d'accés a aplicacions
5.1. Autenticació i autorització en serveis WEB.
5.2. OAuth, OAuth2 i tokens.

6. Aspectes legals
6.1. Aspectes jurídics en entorns tecnològics.
6.2. Protecció de dades.
6.3. Protecció intel·lectual i Llicències

18 HORAS PRESENCIALES. 7 HORAS ON LINE

Objectiu:

- El curs ofereix de manera concisa una útil introducció al disseny de polítiques de seguretat informàtica i a la implantació pràctica de mesures tant tecnològiques com metodològiques que previndran accidents en relació a l'ús de tecnologies informàtiques, o amb les dades que amb elles es manegen, en el nostre negoci , empresa o institució.

CALENDARIO:

JUNIO 2022

LUN 6	Mart 7	Mierc 8	Jueves 9	Viernes 10	Sábado 11
Grupo A 1ªSesión 25/30 Alumnos 18 A 22.30 4.30 H.	Grupo B 1ªSesión 25/30 Alumnos 18 A 22.30 4.30 H.	Grupo A 2ªSesión 25/30 Alumnos 18 A 22.30 4.30 H.	Grupo B 2ªSesión 25/30 Alumnos 18 A 22.30 4.30 H.	Grupo A 3ªSesión 25/30 Alumnos 18 A 22.30 4.30 H.	Grupo B 3ªSesión 25/30 Alumnos 9 A 14.30 4.30 H.

Lun 13	Mart 14	Mierc 15	Jueves 16	Viernes 17	Sábado 18
Grupo A 4ªSesión 25/30 Alumnos 18 A 22.30 4.30 H.	Grupo B 4ªSesión 25/30 Alumnos 18 A 22.30 4.30 H.				

Inicio del curso el **6/7 de JUNIO**. Finalización **17 de JUNIO**, fecha hasta la que estará abierta la plataformA on line del curso.

_____

Las clases presenciales se impartirán en la sede de BALMORE SOLUTIONS “BMS”, Calle BORRELL, 6 BAJOS DE SANT CUGAT DEL VALLES