Recomendaciones de seguridad informática

Castellano / Català

Hola a tod@s:

Va pasando el tiempo y hay ciertas costumbres de buen uso informático que conviene ir recordando de vez en cuando:

- **Piratería informática**

  UPC de vez en cuando nos avisa de descargas de ficheros desde la red RMEECIMNE con programas como el emule, jdownloader o torrent, entre otros, que además de saturar la red pueden facilitar la entrada de virus. Por ello, informamos que queda terminantemente prohibida la utilización de este tipo de aplicaciones.

  No debemos olvidar que la red RMEE-CIMNE, así como el equipamiento que se utiliza es de trabajo y ha sido financiado en su mayoría con fondos públicos. Ejemplos de esta situación son problemas de conexión con servidores de correo, servidores de disco, impresoras y con el exterior. Os ruego que utilicéis los recursos informáticos con prudencia y de la forma más adecuada para alcanzar los objetivos propios de vuestro trabajo, sin perjudicar al resto de usuarios.

  Si tenéis que realizar una transferencia masiva os sugiero que utilicéis discos duros portátiles, pues si un usuario copia un archivo de 1GByte este usuario está bloqueando la red durante 2 minutos, en el mejor de los casos.

  Si la actividad del CIMNE o del departamento se sigue viendo afectada por estos problemas, no quedará más remedio que tomar otras medidas para evitarlos.

- **Contraseñas**

  Para los departamentos que utilizan muchas contraseñas volvemos a recomendar el uso de una aplicación de gestión de contraseñas: keepassx . Esta aplicación te facilita la organización y memorización de tus contraseñas protegiéndolas bajo una única contraseña maestra. Para más información consulta los manuales en https://web.cimne.upc.edu/groups/sistemes/index.php?dir=.%2FManuales%2FGestor_Passwords

Remarcamos también que el password es PERSONAL y se debe ir cambiando cada cierto tiempo, pues la auditoria obliga, aunque sistemas solo aconseja.

- **Phishing**

Aunque el correo CIMNE pase por los filtros de UPC y nuestros servidores suele ocurrir de vez en cuando el phishing o suplantación de identidad. Es decir, correos caracterizados por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). Por eso desde sistemas pedimos verificar la fuente de información y no contestar automáticamente a ningún correo que solicite información personal o financiera. No olvidéis que las entidades bancarias no solicitan información confidencial a través de canales no seguros, como el correo electrónico.

- **Antivirus**

Aunque se tenga siempre activado el antivirus aconsejamos ir pasando el antivirus al menos un par de veces al mes. Se hace accediendo a la consola del antivirus con el botón derecho en el icono inferior a la derecha de la pantalla y pulsando en exploración completa. Para más información consulta los manuales en https://web.cimne.upc.edu/groups/sistemes/index.php?dir=.%2FManuales%2FTutorial_AntiVirus

Aunque tengáis antivirus, firewall y aunque los correos pasen por el filtro de UPC y de sistemas CIMNE siempre el pirata va por delante. Recalcamos que **vosotros mismos sois el último nivel de seguridad y el más importante "antivirus" que hay** y por tanto sería bueno aplicar un poco de sentido común para abrir o no ciertos correos desconocidos y no meteros en páginas no adecuadas o desconocidas. Recordaros que el uso de pendrives de orígenes desconocidos tiene que ir asociado al escaneo mediante antivirus.

- **Mejora y uso outlook y PST**

A medida que pasa el tiempo, nuestro cliente de correo OUTLOOK se va llenando de correo, con lo que la carpeta personal que contiene todos los datos (mails y direcciones) se va haciendo cada vez más grande pudiendo colapsar el PC. Si sucede esto se puede llegar a perder todo el correo, por tanto, es necesario saber cómo organizar el Outlook para que no pase.

Como casi todo el personal de PAS utiliza el cliente de correo OUTLOOK hemos confeccionado un manual sobre el buen uso de Outlook 2010. Lo podréis encontrar tanto en catalán como castellano en nuestra documentación, es decir en la siguiente dirección:

https://web.cimne.upc.edu/groups/sistemes/index.php?dir=.%2FManuales%2FCorreo%2FMejora%20de%20uso%20del%20correo%20Outlook%20y%20PSTs
Os aconsejamos que utilicéis dicho manual.

- **VPN**

Desde sistemas remarcamos que es de uso PERSONAL y que se bloquea automáticamente por el uso abusivo y por razones de seguridad. Para más información consulta los manuales en
https://web.cimne.upc.edu/groups/sistemes/index.php?dir=.%2FManuales%2FAcceso%20remoto%20-%20VPN

- **Almacenamiento en la nube / FTP / Web**

El uso de almacenamiento externo en la nube (Dropbox, Google drive, Onedrive, icloud…) tiene que ir asociado a las mismas precauciones que para el correo y pendrives. Recientemente hemos detectado problemas de virus por compartir archivos en Dropbox.

La reciente sentencia del 6 de octubre del Tribunal de Justicia de la Unión Europea (TJUE) sobre el asunto C-362/14, conocido popularmente como “Decisión Schrems”, ha convertido la transferencia internacional de datos basada en el Safe Harbor Agreement en una opción ilegal.

Eso supone que en nuestro país (y en toda la Unión Europea) cualquier transferencia internacional de datos a EEUU es susceptible de ser considerada inválida y no amparada por la ley. Esto constituye una infracción grave, sancionable en España con hasta 600.000 euros por la Agencia Española de Protección de Datos.

A día de hoy, la Agencia Española de Protección de Datos, en un ejercicio de prudencia, no se ha posicionado sobre cuál será la mejor opción y manifiesta que se está trabajando con el Grupo 29, para actuar de forma conjunta en la aplicación de la sentencia.”

Es por ello que os aconsejamos utilizar los servicios FTP y web que Sistemas os proporciona y que está explicado en:

https://web.cimne.upc.edu/groups/sistemes/index.php?dir=.%2FManuales%2FFTP-Web y
https://web.cimne.upc.edu/groups/sistemes/index.php?dir=.%2FManuales%2FUso_de_la_red_y_dominio_RMEECIMNE

- **Pcs encendidos 24h/7x7 y uso de servidores de cálculo**

Se ha verificado que cierta cantidad de PCs se quedan encendidos las 24 horas del día y los 7 días de la semana.

- Si es personal administrativo (PAS): Los ordenadores de usuarios no están hechos para aguantar encendidos todo el rato. Estando mucho tiempo encendido el registro de Windows tiende al caos, por lo que es necesario reiniciar cada día; aparte de que los PCs se estropean mucho más rápidamente, envejecen prematuramente, con el consiguiente gasto para la empresa en PCs y electricidad…y el gasto para el planeta. Tened en cuenta que a nivel de seguridad hay que aplicar las actualizaciones que van surgiendo y reiniciando.
- Si es personal investigador, aparte que sigue siendo válido lo anterior tened en cuenta que contamos con un servicio de cálculo con 31 nodos de cálculo y que podéis calcular en él. Toda la documentación sobre el tema , de cómo utilizarlo está en https://hpc.cimne.upc.edu/ . Los servidores de cálculo serían la mejor forma y segura de realizar vuestros proyectos de cálculo. Dichos servidores están constantemente monitoreados, en un espacio refrigerado y con energía constate y fija.
- Si no tenéis otra alternativa **bloqueéis vuestros PCs con contraseña** antes de iros, aunque solo sea por una hora. El hecho de exponer datos potencialmente comprometidos para la CIMNE hace que corramos riesgo de infracción por parte de la autoridad RPGD y se debe reportar obligatoriamente.
- De todos modos, sería **mejor que cerraseis el ordenador cada día**, puesto que los ordenadores de usuarios no están hechos para aguantar encendidos todo el rato. Estando mucho tiempo encendido el registro del PC tiende al caos, por lo que es necesario reiniciar cada día; aparte de que los PCs se estropean mucho más rápidamente, envejecen prematuramente, con el consiguiente gasto para la empresa en PCs y electricidad…y el gasto para el planeta.

Hola a tots i totes:

Va passant el temps i hi ha certs costums de bon ús informàtic que convé anar recordant de tant en tant:

- **Pirateria informàtica**

  UPC de tant en tant ens avisa de descàrregues de fitxers des de la xarxa RMEECIMNE amb programes com l'emule, JDownloader o torrent, entre d'altres, que a més de saturar la xarxa poden facilitar l'entrada de virus. Per això, informem que queda terminantment prohibida la utilització d'aquest tipus d'aplicacions.

  No hem d'oblidar que la xarxa RMEE-CIMNE, així com l'equipament que s'utilitza és de treball i ha estat finançat majoritàriament amb fons públics. Exemples d'aquesta situació són problemes de connexió amb servidors de correu, servidors de disc, impressores i amb l'exterior. Us prego que feu servir els recursos informàtics amb prudència i de la forma més adequada per assolir els objectius propis del vostre treball, sense perjudicar la resta d'usuaris.

  Si heu de fer una transferència massiva us suggereixo que utilitzeu discs durs portàtils, ja que si un usuari copia un arxiu d'1Gbyte aquest usuari està bloquejant la xarxa durant 2 minuts, en el millor dels casos.

  Si l'activitat del CIMNE o del departament se segueix veient afectada per aquests problemes, no quedarà més remei que prendre altres mesures per evitar-los.

- **Contrasenyes**

  Per als departaments que utilitzen moltes contrasenyes tornem a recomanar l'ús d'una aplicació de gestió de contrasenyes: keepassx. Aquesta aplicació et facilita l'organització i memorització de les contrasenyes protegint sota una única contrasenya mestra. Per a més informació consulta els manuals en https://web.cimne.upc.edu/groups/sistemes/index.php?dir=.%2FManuales%2FGestor_Passwords

Remarquem també que el password és PERSONAL i s'ha d'anar canviant cada cert temps, ja que l'auditoria obliga encara que sistemes només aconsella.

- **Phishing**

Tot i que el correu CIMNE passi pels filtres d'UPC i els nostres servidors acostuma a passar de tant en tant el phishing o suplantació d'identitat. És a dir correus caracteritzats per intentar adquirir informació confidencial de forma fraudulenta (com pot ser una contrasenya o informació detallada sobre targetes de crèdit o altra informació bancària). Per això des de sistemes demanem verificar la font d'informació i no contestar automàticament a cap correu que sol·liciti informació personal o financera. No oblideu que les entitats bancàries no sol·liciten informació confidencial a través de canals no segurs, com el correu electrònic.

- **Antivirus**

Encara que es tingui sempre activat l'antivirus cal anar passant l'antivirus almenys un parell de vegades al mes. Es fa accedint a la consola del antivirus amb el botó dret a la icona inferior a la dreta de la pantalla i prement en exploració completa. Per a més informació consulta els manuals en
https://web.cimne.upc.edu/groups/sistemes/index.php?dir=.%2FManuales%2FTutorial_AntiVirus
Encara que tingueu antivirus, firewall i tot i que els correus passin pel filtre de UPC i de sistemes CIMNE sempre el pirata va per davant. Recalquem que **vosaltres mateixos sou l'últim nivell de seguretat i el més important "antivirus" que hi ha** i per tant seria bo aplicar una mica de seny per obrir o no certs correus desconeguts i no ficar-vos en pàgines no adequades o desconegudes. Recordar-vos que l'ús de pendrives d'orígens desconeguts ha d'anar associat al escaneig mitjançant antivirus.

- **Millora i ús outlook i PST**

A mesura que passa el temps, el nostre client de correu OUTLOOK es va omplint de correu, de manera que la carpeta que conté totes les dades (mails i adreces) es va fent cada vegada més gran pot col·lapsar el PC. Si succeeix això es pot arribar a perdre tot el correu, per tant cal saber com organitzar el Outlook perquè no passi.
Com gairebé tot el personal de PAS utilitza el client de correu OUTLOOK hem confeccionat un manual sobre el bon ús d'Outlook 2010. El podreu trobar tant en català com castellà a la nostra documentació, és a dir en la següent adreça:

https://web.cimne.upc.edu/groups/sistemes/index.php?dir=.%2FManuales%2FCorreo%2FMejora%20de%20uso%20del%20correo%20Outlook%20y%20PSTs
Us aconsellem que feu servir aquest manual.

- **VPN**

Des sistemes remarquem que és d'ús PERSONAL i que es bloqueja automàticament per l'ús abusiu i per raons de seguretat. Per a més informació consulta els manuals en https://web.cimne.upc.edu/groups/sistemes/index.php?dir=.%2FManuales%2FAcceso%20remoto%20-%20VPN

- **Emmagatzematge en el núvol / FTP / web**

L'ús d'emmagatzematge extern en el núvol (Dropbox, Google drive, Onedrive, icloud ...) ha d'anar associat a les mateixes precaucions que per al correu i pendrives. Recentment hem detectat problemes de virus per compartir arxius en Dropbox.

La recent sentència del 6 d'octubre del Tribunal de Justícia de la Unió Europea (TJUE) sobre l'assumpte C-362/14, conegut popularment com "Decisió Schrems", ha convertit la transferència internacional de dades basada en el Safe Harbor Agreement en una opció il·legal.

Això suposa que al nostre país (i en tota la Unió Europea) qualsevol transferència internacional de dades als EUA és susceptible de ser considerada invàlida i no emparada per la llei. Això constitueix una infracció greu, sancionable a Espanya amb fins a 600.000 euros per l'Agència Espanyola de Protecció de Dades.

A dia d'avui, l'Agència Espanyola de Protecció de Dades, en un exercici de prudència, no s'ha posicionat sobre quina serà la millor opció i manifesta que s'està treballant amb el Grup 29, per actuar de manera conjunta en l'aplicació de la sentència. "

És per això que us aconsellem utilitzar els serveis FTP i web que Sistemes us proporciona i que està explicat en:

https://web.cimne.upc.edu/groups/sistemes/index.php?dir=.%2FManuales%2FFTP-Web y https://web.cimne.upc.edu/groups/sistemes/index.php?dir=.%2FManuales%2FUso_de_la_red_y_dominio_RMEECIMNE

- **PC encesos 24h / 7x7 i ús de servidors de càlcul**

S'ha verificat que certa quantitat de PCs es queden encesos les 24 hores del dia i els 7 dies de la setmana.

- Si és personal administratiu (PAS): Els ordinadors d'usuaris no estan fets per aguantar encesos tota l'estona. Estant molt temps encès el registre de Windows tendeix al caos, pel que és necessari reiniciar cada dia; a part que els PC es fan malbé molt més ràpidament, envelleixen prematurament, amb la conseqüent despesa per a l'empresa en PCs i electricitat ... i la despesa per al planeta. Tingueu en compte que a nivell de seguretat cal aplicar les actualitzacions que van sorgint i reiniciant.

- Si és personal investigador, a part que segueix sent vàlid l'anterior tingueu en compte que comptem amb un servei de càlcul amb 31 nodes de càlcul i que podeu calcular en ell. Tota la documentació sobre el tema, de com utilitzar-lo està en https://hpc.cimne.upc.edu/ . Els servidors de càlcul serien la millor forma i segura de realitzar els vostres projectes de càlcul. Aquests servidors estan constantment monitoritzats, en un espai refrigerat i amb energia constati i fixa.

- Si no teniu una altra alternativa **bloquegeu el vostres PCs amb contrasenya** abans de marxar encara que només sigui per una hora. El fet d'exposar dades potencialment compromesos per a CIMNE fa que correm risc d'infracció per part de l'autoritat RPGD i s'ha de reportar obligatòriament.
- De totes maneres, seria **millor que tanquéssiu l'ordinador** cada dia, ja que els ordinadors d'usuaris no estan fets per a aguantar encesos tota l'estona. Estant molt temps encès el registre del PC tendeix al caos, per la qual cosa és necessari reiniciar cada dia; a part de que els PCs s'espatllen molt més ràpidament, envelleixen prematurament, amb la conseqüent despesa per a l'empresa en PCs i electricitat…i la despesa per al planeta.