Servicio de Informática y Comunicaciones
Universidad de Sevilla

PREGUNTAS FRECUENTES SOBRE SEGURIDAD DE LA INFORMACIÓN

SEGURIDAD EN EL PUESTO DE TRABAJO

PROTECCION DE LOS ESPACIOS FISICOS

P. ¿Deberíamos dejar cerrados todos los armarios que contengan información de los alumnos antes de abandonar nuestro puesto de trabajo?

R. Sí, se deben dejar cerrados los armarios para evitar que accedan a la información personas no autorizadas.

P. ¿En la Universidad de Sevilla existe alguna norma que regule el uso de llaves maestras?

R. La normativa de acceso físico de la Universidad de Sevilla establece que en cada área restringida debe haber una persona encargada del control y registro de accesos. Esta persona será responsable de identificación en primera instancia del personal autorizado y del seguimiento de los accesos. Para más información puede consultar dicha Normativa en el enlace http://sic.us.es/sites/default/files/seguridad/normativa_control_acceso_fisico_us.pdf .

CONFIGURACIÓN DE LOS ORDENADORES

P. ¿Cómo se qué servicios se pueden desactivar en el ordenador?

R. Los servicios mínimos necesarios que deben estar arrancados en un equipo dependen del uso que se le vaya a dar al equipo y del sistema operativo usado. Sin los conocimientos necesarios es una tarea difícil de realizar por el usuario por lo que recomendamos que para los puestos de trabajo se solicite ayuda al Servicio de Atención a Usuarios SOS. No obstante el SIC publicará en breve una Guía de bastionado seguro de equipos que pueda servir de orientación a los usuarios.

P. ¿Se ha planteado la Universidad homogeneizar plataformas, electrónica y sistemas operativos para simplificar la administración y reforzar las políticas de seguridad?

R. Actualmente se está haciendo un estudio para maquetar los puestos de trabajo en la Universidad de Sevilla.

P. La seguridad recomienda activar las actualizaciones automáticas ¿y si dejan de funcionar las aplicaciones corporativas?

R. Sólo en algunos casos puntuales puede ocurrir esto. Es estos caso recomendamos al usuario que acuda al Servicio de Atención a Usuarios SOS para estudiar la mejor solución.

P. ¿Qué ocurre si actualizo Java?

R. La actualización de Java puede afectar al uso de herramientas de UXXI que requieren una versión específica. La actualización automática del Sistema Operativo no implica la actualización automática de Java. No obstante, ante cualquier problema que surja, debe contactar con el Servicio de Atención a Usuarios SOS y seguir sus indicaciones.

P. ¿Por qué no funciona el Registro Electrónico de la US?

R. Por una incorrecta configuración del equipo desde el cual se accede al Registro. Cuando esto ocurra, la mejor opción es solicitar ayuda al Servicio de Atención a Usuarios SOS para la correcta configuración del puesto de trabajo.

RECURSOS COMPARTIDOS

P. Si personal de secretaría del decanato son varios usuarios ¿es correcto usar un mismo disco externo para copias de seguridad?

R. Si todos los usuarios están autorizados a acceder a la información, no habría problemas de confidencialidad. No obstante, la protección de las copias requiere que haya una persona responsable de que haya una política de copias de seguridad necesarias, que esta se cumpla y que custodie el disco externo de forma segura. Los discos externos no deben estar conectados permanentemente a los equipos ya que el compromiso de un equipo puede comprometer la copia de seguridad.

P. Para puestos técnicos temporales de alta rotación, ¿el responsable sería la persona usuaria de la máquina o el responsable del contrato a tal persona?

R. Lo recomendable es que hubiera una persona con estabilidad laboral que se hiciera responsable del puesto de trabajo, de su correcta configuración, su mantenimiento y su seguridad.

P. ¿A un PC compartido hay que ponerle clave de acceso?

R. Sí. Lo ideal, si el sistema operativo lo permite, es que se creen perfiles por usuario y cada trabajador tenga su usuario y contraseña. Si esto no es posible, una persona del servicio debe responsabilizarse de que siempre esté puesta la clave, de su cambio periódico y de que la conozcan sólo los autorizados, Cualquier compromiso de la clave debe comunicarse inmediatamente al responsable.

CONEXIÓN A LA RED WIFI

P. Al conectarnos con nuestro dispositivo a *Eduroam* (red *WiFi* de la Universidad) ¿la normativa, control y seguimiento que se ha explicado en materia de seguridad es la misma?

R. Sí. Aunque sea un dispositivo personal, se están usando servicios de la Universidad y hay que cumplir las mismas normativas de uso de los servicios.

P. ¿Cómo puedo cambiar la clave de wifi en mi móvil?

R. Dependiendo del terminal móvil las opciones de configuración pueden variar. Mi recomendación es que busque las opciones de configuración para su modelo en móvil en Internet y localice la forma de cambiar en el móvil la clave para acceder a una red wifi particular (la de casa, por ejemplo). En relación al acceso a Eduroam, para que la configuración sea segura, la mejor opción es acceder a la página web de Eduroam CAT para configurar su dispositivo. La página incluye un instalador.

CONEXIÓN REMOTA AL PUESTO DE TRABAJO

P. ¿El uso del programa de escritorio remoto *TeamViewer* está aceptado en la Universidad?

R. De momento, si la configuración es segura, sí. No obstante, cuando sea necesario acceder a recursos de la US desde fuera de nuestras instalaciones, se recomienda el uso de VPN (Red Privada Virtual) https://sic.us.es/servicios/infraestructuras-comunicaciones-hw-y-sw/acceso-externo-los-recursos-electronicos-de-la-us

P. ¿Se puede acceder por la herramienta de escritorio remoto de Microsoft?

R. De momento únicamente se permite el uso del programa *RDP* de Microsoft y de *TeamViewer* configurados de forma segura, pero se recomienda el uso de VPN (Red Privada Virtual) https://sic.us.es/servicios/infraestructuras-comunicaciones-hw-y-sw/acceso-externo-los-recursos-electronicos-de-la-us . El uso del programa VNC no está permitido por ser la conexión insegura.

P. ¿Hay que solicitar VPN para estar, se algún modo, autorizado, aunque ya nos conectemos por *TeamViewer* bien configurado habitualmente?

R. Es recomendable. Actualmente está abierto el acceso directo a los programas de escritorio remoto cifrados como *RDP* o *TeamViewer*, pero en algún momento se restringirá su uso al ámbito de la US para reducir la superficie de exposición y entonces el acceso sólo estará permitido por Red Privada virtual (VPN).

SEGURIDAD DE LA INFORMACIÓN

INFORMACIÓN CORPORATIVA

P. ¿Cómo se define “dato corporativo”? ¿Los apuntes que tomo de esta charla, es un dato corporativo?

R. Cualquier dato o información generada en el ejercicio de nuestras funciones es corporativo. Los apuntes de una charla también. Las medidas de protección de la información corporativa dependerán de la clasificación de dicha información. http://sic.us.es/sites/default/files/seguridad/normativa_clasificacion_tratamiento_informacion_us.pdf

P. ¿A quién hay que dirigirse para que se modifique el correo electrónico de un trabajador/a, del directorio público?

R. Los datos que aparecen en el directorio son datos personales que por ser corporativos pueden ser publicados sin el consentimiento del trabajador. No obstante, deben ser exactos y si no lo son, se deben actualizar. Los datos del directorio se obtienen de distintas fuentes de datos corporativas por lo que la mejor opción es comunicarlo al Servicios de Atención a Usuarios SOS mediante un parte en Remedy para que el dato incorrecto se actualice en la fuente correspondiente.

P. ¿Se contempla el correo corporativo y personal con la terminación us.es? Y si es así ¿existen protocolos de uso diferenciados?

R. Todo el correo electrónico *us.es* es corporativo. Se puede distinguir entre cuentas nominales asociadas al UVUS, de uso personal e intransferible, ya que nos permite el acceso a las aplicaciones corporativas y a nuestros datos personales, y cuentas misceláneas asociadas a un puesto de trabajo, que tienen un único responsable pero que puede ser usarda por más de una persona en el tiempo para el ejercicio de sus funciones. Los procedimientos de solicitud, uso y custodia son diferentes y se encuentran descritos en el “Procedimiento de gestión de la Identidad Digital y acceso lógico de la Universidad de Sevilla”. https://sic.us.es/sites/default/files/seguridad/privado/procedimiento_gestion_identidad_digital_us.pdf

P. Hay muchas personas que usan el correo corporativo para fines personales. ¿Se puede controlar esto?

R. El uso personal de la cuentas de correo vienen justificado por el hecho de que hace años no existían proveedores de servicios en Internet que nos facilitaran cuentas de correo gratuitas y la Universidad era permisiva en este aspecto. Algo similar ocurria con las llamadas telefónicas personales cunado no había móviles y un trabajador tenía una emergencia personal o familiar. Esto ha cambiado y debemos concienciarnos de que los medios puestos a nuestra disposición por la Universidad no pueden ser utilizados para fines privados y así lo establecen las distintas normativas de uso de los servicios. De hecho, la ley permite a la Universidad el acceso a los buzones de correo de los usuarios si dan ciertas condiciones que deberán ser comunicadas previamiente a los interesados, poderando siempre el derecho a la intimidad y las expectativas de privacidad de los trabajadores tal como establece la nueva Ley de Orgánica de Protección de Datos y Grarantía de los Derechos Digitales.

DATOS PERSONALES

P. Las fotografías de eventos públicos que se suben a los servidores Web de la Universidad, a los que accede personal externo a la Universidad de Sevilla ¿sería una mala práctica? ¿se pueden publicar fotos externas en las RRSS corporativas?

R. Si no se cumplen los principios de protección de datos, sí es una mala práctica, incluso cuando se publican sólo para personal interno a la US. Dependiendo del evento puede ser necesario tener un consentimiento explícito de las personas que aparezcan en la fotografía pero en todo caso el obligatorio anunciar la grabación y dar información sobre el tratamiento y la finalidad que se va a dar a esas fotografías. Ante cualquier duda debemos consultar a la Delegada de Protección de Datos de la Universidad de Sevilla.

P. ¿Podemos dar información de las calificaciones por teléfono?

R. No se puede ya que no es posible identificar correctamente al solicitante. Las nuevas tecnologías ya permiten la consulta de las calificaciones de forma segura sin tener que acudir a esta vía.

P. Una hoja de cálculo con las notas de los alumnos nombre, DNI y calificación ¿de qué nivel es? ¿Se pueden publicar en tablón de anuncios y plataforma de enseñanza virtual, la calificación de los estudiantes con su nombre y apellidos?

R. Nombre, apellidos, DNI y calificaciones son datos personales y hay que cumplir la ley. La Universidad de Sevilla establece las directrices para la correcta publicación de las calificaciones en relación a la protección de datos

personales y la transparencia. Se pueden consultar en la página http://sic.us.es/sites/default/files/pd/1.2019publicacion_de_calificaciones.pdf

P. ¿Qué podemos hacer si se ponen en los cristales de nuestro centro los DNI o carnets extraviados a la vista de todos?

R. Pedir a los conserjes que los retiren y simplemente informen en una nota de que se ha encontrado un DNI o carné universitario.

P. Si hago una reunión familiar y publico una foto de todos en Facebook ¿tengo que pedirles permiso?

R. El Reglamento General de Protección de Datos no aplica al tratamiento de imágenes efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas, si bien la publicación de información de terceros en el ámbito doméstico nunca podrá lesionar los derechos e intereses de las personas. La Agencia Española de Protección de Datos ha publicado una Guía sobre el uso de videocámaras para seguridad y otras finalidades que aclara muchos puntos relacionados con la publicación de imágenes y vídeos, tanto en el ámbito profesional como en el personal. https://www.aepd.es/media/guias/guia-videovigilancia.pdf

P. En Google pongo mi nombre y apellidos y aparecen todos mis datos personales: domicilio, teléfono donde trabajo, etc. A mí ¿quién me protege?

R. Los datos profesionales se pueden publicar siempre que sean los mínimos imprescindibles para localizar al profesional. La finalidad debe ser la de entablar relaciones profesionales-empresariales. Cualquier dato que no sea necesario para este fin no podrá ser publicado y el trabajador podrá solicitar la retirada del mismo.

P. ¿Cómo podemos evitar que Google nos indexe?

R. Se puede limitar la indexación de nuestra web, no solo por parte de Google, sino por cualquier otro buscador (Yahoo, Bing…) utilizando el archivo de texto plano **robots.txt.** Hay que crearlo en la raíz del sitio web, por lo que debe hacerlo el administrador de la página. En dicho archivo se establecen las indicaciones que deben cumplir los *robots spiders* cuando visiten y rastreen nuestro sitio web.

P. ¿Cómo se protege el derecho a la intimidad de las personas discapacitadas en los procesos de concurrencia competitiva?

R. Las convocatorias deben ser acordes al Reglamento General de Protección de Datos. El registro online permite mantener la privacidad si las convocatorías se ajustan a la ley. No obstante, cualquier consulta relacionada con protección de datos debe hacerse a través del Delegado de Protección de Datos de la Universidad de Sevilla (dpd@us.es).

P. ¿Por qué ultimamente pregunta SEVIUS si queremos que se pubique nuestra foto?¿Con que fin?

R. El Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales, establecen el principio de minimización de los datos, que significa que estos deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. La Universidad de Sevilla trata los datos imprescindibles para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos que tiene conferidos sin necesidad de tener un consentimiento explícito del usuario. Pero una fotografía puede no ser un dato mínimo y en este caso, sí pide, a través de Sevius, el consentimiento para publicarla en el nuevo Portal de la Universidad www.us.es. La publicación es voluntaria.

P. Hay algunos alumnos que graban clases ¿se puede hacer?

No. Debería tener el consentimineto explícito de los asistentes a la clase. No obstante, cualquier consulta relacionada con protección de datos debe hacerse a través del Delegado de Protección de Datos de la Universidad de Sevilla (dpd@us.es).

USO DE ANTIVIRUS Y CORTAFUEGO

P. Soy usuario Mac y no uso antivirus pero hago un uso siempre responsable. ¿Es correcto?

R. El uso responsable no es suficiente para proteger el equipo. Debemos usar siempre un antivirus independientemente del sistema operativo que tengamos.

P. ¿Qué ocurre con los que tenemos equipos con Windows XP y ya no tenemos la licencia del TrendMicro?

R. Debido a la finalización de las licencias de antivirus de *TrendMicro* para los equipos con XP el Servicio de Informática y Comunicaciones recomienda el uso del antivirus AVIRA para los equipos que quedan con XP: https://www.avira.com/es/free-antivirus-windows. Toda la información relativa a antivirus se va a ir publicando en http://sic.us.es/servicios/infraestructuras-comunicaciones-hw-y-sw/antivirus.

P. ¿El cortafuegos detecta los archivos adjuntos al correo potencialmente peligrosos?

R. No siempre. Tendría que ser un cortafuego muy avanzado con un módulo específico de protección del correo electrónico. No obstante, la Universidad de Sevilla, en su servidor de Correo, dispone de un sistema de detección de mensajes con adjuntos potencialmente peligrosos. Estos sistemas nunca tiene un 100% de eficacia pero constituyen una buena barrera de protección.

P. A veces nos sale un aviso de seguridad desaconsejándonos conectar con páginas que son de la propia universidad, ¿a qué se debe?

R. En principio, no debe ocurrir cuando la página es de la propia Universidad. El cortafuego perimetral actúa cuando intentamos conectarnos a una página externa a la US que está catalogada como maliciosa. El motivo del mensaje es que la página remota contiene código que puede ser dañino para nuestros equipos y por eso se bloquea. Sólo en el caso de que el usuario esté seguro de que la página es buena, debe seguir las instrucciones de la propia página de aviso para pedir la revisión de la misma al fabricante del cortafuego. Ante la duda, mejor preguntar al SOS.

P. ¿La base de datos del cortafuego de la US actualiza las reglas de forma dinámica o se realiza de forma manual?

R. La actualización es dinámica. La base de datos de firmas de virus y direcciones IPs maliciosas en listas negras se actualiza cada hora.

P. Diariamente se puede ver en los registros de *logs* de mi sistema muchos intentos de ataque ¿hay alguna forma de reportar o evitar estos ataques en el cortafuego corporativo?

R. Es más operativo realizar el filtrado de ataques a un servidor concreto de la Universidad en el cortafuego del propio servidor, a no ser que se detecte que el ataque se realiza de forma masiva a múltiples equipos de la Universidad de Sevilla. Hay que estudiar el por qué de los ataques: a veces es porque tenemos expuesto un puerto o servicio al mundo, que debería estar restringido a la US.

NAVEGACIÓN SEGURA

P. ¿La “s” de https es importante?

R. Importantísima. Significa que la conexión es segura y la información va cifrada. Siempre que nos conectemos a una página que tenga información confidencial o registro por usuario debemos asegurarnos de que el protocolo usado es https y no http.

P. ¿Todas las direcciones que tienen candado son seguras?

R. No todas. Dependiendo del navegador, a veces, en una conexión segura https, en vez del candado aparece un signo de advertencia en lugar del candado o una página que dice que la conexión es insegura. Esto significa que el certificado digital que usa el servidor al que intentamos conectarnos está caducado o no es de confianza. En ese caso debemos valorar si nos conectamos o no.

P. ¿Por qué aparece el molesto mensaje de las *cookies* al entrar en cada nueva web?

R. Es obligatorio avisar al usuario de que el sitio utiliza *cookies*. Antes de que se aprobara el Reglamento General Europeo de Protección de Datos bastaba con informar y que el usuario aceptara haber sido informado. Después del 25 de mayo de 2018 las webs que utilizan cookies deben dar una información más detallada sobre las *cookies* que utilizan, ofrecer al usuario la posibilidad de aceptar o no las que no sean obligatorias para navegar y guardar la aceptación explícita de las condiciones por parte del usuario.

P. ¿Las web de los Centros están controladas por la US o son independientes?

R. Algunos Centros tienen sus webs integradas en un gestor de contenidos mantenido por el SIC. Otros tienen webs independientes alojadas en servidores que están en las infraestructuras del SIC y el resto tienen sus propios servidores con sus páginas Web fuera del CPD del SIC. Lo ideal es que todos los Centros tuvieran sus páginas Web alojadas en infraestructura del SIC ya que el CPD reúne las condiciones de seguridad físicas y lógicas requeridas.

USUARIOS Y CONTRASEÑAS

¿Tiene la universidad algún gestor de contraseña?

R. No. Cada usuario debe gestionar sus contraseñas de forma segura. El uso de gestores de contraseñas tiene ventas y desventajas por lo que es conveniente evaluarlos correctamente y elegir el más adecuado a nuestra situación.

P. ¿Es aconsejable tener la misma contraseña para todos los dispositivos y cuentas, sean personales o laborales, que uno utilice?

R. No. Se recomienda usar distintas claves para no comprometer la seguridad de todos los dispositivos si se compromete uno de ellos. Especial cuidado hay que tener de no usar las mismas claves en cuentas personales y laborales. Sólo en las aplicaciones de la US integradas con Single Sign On o con LDAP utilizaremos el mismo identificador y la misma clave, que son las del UVUS.

P. ¿Es válido usar el gestor de contraseñas de Google Chrome?

R. No para claves de la Universidad. El gestor de contraseñas de Google mejora cada vez más, pero las claves están protegidas solo por la contraseña de la cuenta de Google. Si nos roban las credenciales de esta cuenta, tendrán el acceso a todas nuestras claves.

P. ¿Es válido almacenar las contraseñas en un gestor de contraseñas encriptadas en la nube?

R. Si están encriptadas y protegidas con un doble factor de autenticación para acceder a ellas, sería una buena opción.

P. Hay sistemas que permiten recordar contraseñas automáticamente ¿hay algún problema con esta opción?

R. Estos sistemas lo que hacen es guardar la clave en el navegador, por ejemplo, en el gestor de contraseñas de Google. Es mejor usar un programa específico para gestión de contraseñas con doble factor de autenticación.

P. ¿Hay información en la web de la US sobre la elección y uso de contraseñas?

R. La Política de contraseñas de la US establece limitaciones a la elección de la clave de forma que esta sea segura. La plataforma de cambio de claves identidad.us.es no permite usar en el UVUS una contraseña que no cumpla con la política. Podemos aplicar esas mismas reglas a cualquier otra contraseña que necesitemos crear, como por ejemplo, la de bloqueo de los puestos de trabajo.

P. Si sólo conozco yo la contraseña y me pasa algo ¿nadie puede acceder?

R. Todos los sistemas tienen una opción de reinicio por consola que permite cambiar la clave en caso de emergencia. Sólo se puede hacer si se tiene acceso físico al ordenador.

CERTIFICADOS DIGITALES

P. ¿Por qué no se permite el acceso al correo de la US con un Certificado Digital?

R. Actualmente no todos los servicios de Tecnología de la Infomración de la US tienen integrado el acceso mediante certificado digital. Es necesario modificar las aplicaciones. Poco a poco se van integrando con los distintos métodos de acceso.

COPIAS DE SEGURIDAD Y CIFRADO DE LA INFORMACION

P. ¿Puedo llevarme el disco duro externo con la copia de seguridad a mi casa?

R. Si el disco contiene información corporativa es necesario disponer de una autorización del responsable de la información Si el responsable es uno mismo, en función del tipo de información del disco duro o de cualquier otro soporte, podría ser necesario cifrar la información.

P. ¿Cómo ciframos la información?

R. Consulte la siguiente Guía que le orientará sobre cuándo y cómo cifrar la información: https://sic.us.es/sites/default/files/seguridad/privado/guia_cifrado_informacion.pdf (acceso restringido por UVUS)

P. ¿Los portátiles corporativos llevan los discos cifrados para evitar comprometer los datos críticos si son robados o extraviados?

R. No. Es responsabilidad del usuario cifrar la información en un portátil cuando los datos sean confidenciales.

SEGURIDAD EN EL USO DE LOS SERVICIOS CORPORATIVOS

Redes

P. ¿Qué es el CICA?

R. El Centro Informático Científico de Andalucía (CICA) es un centro de la Junta de Andalucia concebido para prestar servicios a la comunidad científica andaluza. Es nuestro punto de acceso a Internet. Todas las Universidades Andaluzas y centros de investigación accedemos a Internet a través del CICA.

Aplicaciones

P. ¿Es segura la aplicación Etempo? ¿Podría articularse de forma más segura la forma de justificar frente a los responsables las incidencias en Etempo?

R. Es difícil decir que una aplicación es segura 100%. En el caso de Etempo ya se han solicitado por parte de Seguridad ciertas modificaciones relativas a la propia aplicación y a la protección de los datos personales.

RECURSOS HUMANOS EN SEGURIDAD

P. ¿Existe un responsable informático en cada centro o servicio de la US, con una plantilla de más de 20 personas? Y si no es así, ¿lo consideraría necesario?

R. Ojalá! Se trata de un tema que excede las competencias de la Seguridad de la Información. A día de hoy no existe. Existen modelos distintos de gestión y soporte de las tecnologías y es tan válido disponer de atención por centros o servicios, como establecer un modelo de atención centralizado correctamente dimensionado.

P. ¿Se ha realizado una auditoría por parte de los responsables de seguridad de la US, por Centro y Servicio para determinar las necesidades físicas y humanas?

R. Se realizan análisis de riesgos y auditorías de Seguridad de los Sistemas de Información Corporativos centralizados en el Servicio de Informática y Comunicaciones. De este análisis resulta un Plan de mejora que incluye las necesidades físicas y humanas que se presenta a a Comisión de Seguridad. Las necesidades de personal en Centros y Servicios es competencia de los propios Centros o Servicios y en última instancia de Recursos Humanos, que es a donde deben llegar las necesidades.

P. La línea que separa la protección de datos del tratamiento de la información es muy fina. ¿Hay colaboración entre el Responsable de Seguridad y la Delegada de Protección de Datos?

R. Completamente. Ambos pertenecen al nivel de supervisión de la Comisión de Seguridad de la Información y trabajan de forma coordinada.

NOTA: esta FAQ es la segunda versión del documento de PREGUNTAS FRECUENTES SOBRE SEGURIDAD DE LA INFORMACIÓN que se irá ampliando poco a poco con las consultas anonimizadas que se van recibiendo a través de cursos y charlas sobre Seguridad de la Información.