Borrar datos Imprimir

REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN (CUESTIONARIO PREVIO A LA ADQUISICIÓN DE NUEVOS ACTIVOS)

El siguiente cuestionario de requisitos de seguridad debe cumplimentarse por el proveedor **CON CARÁCTER PREVIO A LA ADQUISICIÓN DEL ACTIVO**[1]. Unión de Mutuas podrá así valorar, con las respuestas a este cuestionario, si el activo cumple[2] en materia de:

- compatibilidad con los sistemas en funcionamiento en Unión de Mutuas,
- seguridad de la información[3],
- protección de los datos de carácter personal[4] y otra normativa de aplicación,

y trasladar al proveedor, si se considera necesario, cualquier aclaración o modificación sobre el activo, antes de ser aprobado por esta entidad.

SOBRE LA COMPATIBILIDAD DEL ACTIVO CON LOS SISTEMAS DE UNIÓN DE MUTUAS Y LA SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

REQUISITO	SÍ	NO	NO APLICA
Activo: Software/aplicaciones			
¿El funcionamiento del software es compatible con los sistemas operativos en Unión de Mutuas? (aquellas versiones de Citrix, Windows o Linux indicadas al proveedor en el momento de la consulta)	☐	☐	☐
Una vez instalado el software, ¿funciona por máquina y no solo por usuario instalador?	☐	☐	☐
Una vez instalado el software ¿funciona en modo multiusuario? (varios usuarios pueden tenerlo en ejecución sin necesidad de cerrar el programa al salir de la sesión abierta)	☐	☐	☐
¿La instalación del software puede realizarse en idioma castellano?	☐	☐	☐
¿El software dispone de una base de datos de información propia?	☐	☐	☐
Si el software dispone de base de datos con información propia ¿puede esta tratar datos de carácter personal?	☐	☐	☐
Si el software dispone de base de datos con información propia y puede tratar datos de carácter personal, ¿permitiría el registro de personas de forma pseudonimizada? (ejemplo: por código -alfanumérico de más de 10 caracteres- y no forzando introducción de DNI)	☐	☐	☐
Si el software dispone de base de datos con información ¿funciona correctamente externalizando la base de datos de información fuera del disco local del equipo? (por ejemplo, en una unidad de red indicada por Unión de Mutuas)	☐	☐	☐
Si el software dispone una base de datos de información, ¿el software realiza copia de seguridad de la base de datos de forma automatizada?	☐	☐	☐
Si el punto anterior es afirmativo, ¿el software permite hacer la copia de seguridad en una ruta en red (no localmente en el equipo)?	☐	☐	☐
Si el software dispone una base de datos de información, ¿el software guarda registro de logs de acceso de los usuarios (usuario, fecha y hora de acceso, intentos fallidos de acceso, etc.)?	☐	☐	☐
Si el software dispone una base de datos de información ¿el software guarda registro de logs de consulta/alta/modificación/borrado de registros de los usuarios (usuario, fecha y hora de acceso, registro accedido/modificado/etc.)?	☐	☐	☐

[1] Un activo podrá ser un equipo médico, una herramienta de seguridad, una aplicación informática, un servicio en la nube, un equipo IoT o, en definitiva, cualquier sistema que vaya a interactuar con los sistemas de información y servicios de Unión de Mutuas.

[2] El proveedor podrá contactar con Unión de Mutuas con cualquier consulta o duda que tenga relacionada con este cuestionario.

[3] Según requisitos de norma ISO27001 y Esquema Nacional de Seguridad en los que Unión de Mutuas se encuentra certificada.

[4] De conformidad con Reglamento General de Protección de Datos 2016/679 y Ley Orgánica 3/2018 de Protección de Datos Personales.

REQUISITO	SÍ	NO	NO APLICA
Si alguno de los dos puntos anteriores es afirmativo ¿el acceso al registro de logs se encuentra restringido a usuarios específicos? (solo accesible por usuario admin., etc.)	☐	☐	☐
¿El software funciona correctamente con el equipo integrado en el dominio corporativo (LDAP), e independientemente del usuario del LDAP con el que se acceda al equipo?	☐	☐	☐
¿El acceso al software requiere usuario y contraseña o mecanismo de autenticación que aporte la misma o mayor seguridad?	☐	☐	☐
¿El acceso (login/passw) al software se puede hacer mediante integración con los usuarios del LDAP? (sin necesidad de base de datos local de usuarios)	☐	☐	☐
Si el software no se integra con el LDAP corporativo, ¿el software pide cambio de contraseña periódicamente al usuario?	☐	☐	☐
Si el software no se integra con el LDAP corporativo, ¿el software requiere contraseña robusta (mínimo 12 caracteres, alfanumérica, etc.)	☐	☐	☐
Si el software no se integra con el LDAP corporativo ¿el software bloquea la cuenta del usuario tras varios intentos reiterados fallidos?	☐	☐	☐
¿La ejecución del software requiere permisos de usuario administrador local para funcionar?	☐	☐	☐
¿El software suministrado cumple requisitos demostrables de seguridad conforme a normas o estándares reconocidos? (si afirmativo, indicar en observaciones)	☐	☐	☐
¿Cumple el software o desarrollo del proveedor con el **Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público**? (cumplimentar solo si es desarrollo web o de app) NOTA: resulta de aplicación a Unión de Mutuas este real decreto por ser sector público institucional.	☐	☐	☐
En cumplimiento del Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público, **se encuentra el proveedor en disposición de proporcionar la declaración de aplicabilidad e informe de cumplimiento sobre accesibilidad web o de app** del desarrollo solicitado y a la entrega del producto (cumplimentar solo si es desarrollo web o de app)	☐	☐	☐
Activo: hardware, equipo físico (PC, router, etc.)			
En la adquisición de equipos físicos con sistema operativo, ¿el sistema operativo permite la integración del equipo en el dominio corporativo?	☐	☐	☐
¿Los manuales de uso del equipo/software pueden proporcionarse y se encuentran en castellano?	☐	☐	☐
¿El equipo suministrado cumple requisitos demostrables de seguridad conforme a normas o estándares reconocidos? (si afirmativo, indicar en observaciones)	☐	☐	☐
Productos de seguridad informática: certificación de la funcionalidad de seguridad relacionada con el objeto de adquisición			
Las funcionalidades de seguridad de la información del equipo físico, software o servicio, ¿han sido evaluadas conforme a normas europeas o internacionales, o reconocidas por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información? tendrán la consideración de normas europeas o internacionales, Common Criteria ISO/IEC 15408 u otras de naturaleza y calidad análogas, o cuando se trate de productos incluidos en el catálogo de productos y servicios de seguridad de las tecnologías de la información y comunicación del CCN (CPSTIC). Indicar, en su defecto, si se emplean otros mecanismos de certificación de la seguridad o si se han seguido las taxonomías de referencia indicadas por el CCN	☐	☐	☐
Otras consideraciones			
¿El producto (equipo físico o software) puede certificar su exclusividad en el mercado?	☐	☐	☐

REQUISITO	SÍ	SÍ	NO APLICA
¿El producto (equipo físico o software) puede aportar medidas compensatorias de seguridad en relación con los requisitos que no cumple? (deberán ser revisadas por el responsable de seguridad de Unión de Mutuas para su aprobación)	☐	☐	☐
Servicios Cloud (modalidad SaaS, PaaS o IaaS)			
Arquitecturas de seguridad: ¿cumple o sigue el proveedor la Guía de Seguridad de las TIC CCN-STIC 499 de Arquitecturas de seguridad para servicios en la nube?	☐	☐	☐
En caso de servicios de seguridad, ¿cumple el proveedor con la Guía de Seguridad de las TIC: CCN-STIC 140 Taxonomía de productos de STIC – Anexo G: "Servicios en la nube" del Centro Criptológico Nacional. (Configuración específica de seguridad)?	☐	☐	☐
¿Son los sistemas de información que soportan el servicio conformes con el ENS o cumplen medidas y requisitos de seguridad en relación con: auditorías de pruebas de penetración, transparencia, cifrado y gestión de claves, jurisdicción de los datos, etc.? Indicar:	☐	☐	☐
¿Se encuentra el servicio certificado bajo una metodología de certificación reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.? Si el servicio en la nube es un servicio de seguridad deberá cumplir con los requisitos establecidos en [op.pl.5]	☐	☐	☐

SOBRE EL CUMPLIMIENTO DEL PROVEEDOR CON LAS NORMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Si el proveedor es de servicios de seguridad de la información o si la prestación del servicio por parte del proveedor (instalación, mantenimiento, reparaciones, etc.) implica acceso (presencialmente o en remoto) a datos de carácter personal o a información confidencial, o existe la posibilidad de retirada del equipo de nuestras instalaciones (ante fallos, mantenimientos específicos, etc.), se tendrán en cuenta las siguientes consideraciones, que podrán requerirse de forma obligatoria según cada caso:

REQUISITO	SÍ	NO	NO APLICA
¿El proveedor se encuentra certificado en normas de gestión de seguridad de la información conforme a estándares reconocidos (ISO 27001, ISO 20000, ENS, etc.)?	☐	☐	☐
¿El proveedor se encuentra adherido a códigos de conducta/códigos tipo de conformidad con el Reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales?	☐	☐	☐
¿El proveedor pasa auditorías de protección de datos de carácter personal por tercero independiente y tiene disponible el informe de resultados de auditoría de conformidad con la normativa de protección de datos vigente?	☐	☐	☐
¿Se requiere de subcontratación por parte del proveedor para determinados servicios que suponen tratamiento de datos de carácter personal?	☐	☐	☐

Si el proveedor no cumple algún requisito de este cuestionario, se estudiará y valorará por parte de Unión de Mutuas. Se podrá tener en cuenta la posibilidad de implementación de medidas compensatorias de seguridad tanto a propuesta del proveedor como por parte de Unión de Mutuas (pseudonimización, medidas alternativas que mitiguen riesgos de seguridad no contempladas en este catálogo, etc.).

Indicar, si procede, medidas compensatorias:

.....

.....

.....

.....

Nombre proveedor: .....

CIF: .....

FIRMA:

FECHA: .....

F040-00-056-ES/02