DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Boletín protección de datos

Boletín del Departamento de protección de datos y Seguridad de la Información de la Diputación Provincial de Valencia

Boletín N.º 9| Marzo 2021

MEDIDAS DE SEGURIDAD EN EL PUESTO DE TRABAJO

Í N D I C E

MEDIDAS DE SEGURIDAD EN EL PUESTO DE TRABAJO

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdssi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

INTRODUCCIÓN

El buen funcionamiento de una organización depende, en gran medida, de sus sistemas de información y de la información que en ellos se almacena. La gestión de esta información se realiza desde el puesto de trabajo, ya sea desde dispositivos tecnológicos como no tecnológicos.

El concepto de puesto de trabajo va más allá de la ubicación física donde los usuarios de los sistemas de información de la organización desempeñan sus funciones diarias. El puesto de trabajo ha ido extendiéndose con la incorporación de los nuevos dispositivos tecnológicos como: ordenadores de sobremesa, portátiles, teléfonos móviles, tabletas, dispositivos de almacenamiento extraíbles, impresoras de red, escáneres, etc.

Gran parte de los incidentes de seguridad se suelen generar dentro de la propia organización y, en muchas ocasiones, de manera accidental. Por este motivo, un elemento vital para evitar incidentes relacionados con la seguridad de la información es la implantación de medidas de seguridad en el puesto de trabajo.

Mitigar los riesgos del puesto de trabajo de una forma significativa no siempre requiere de la implantación de complejas medidas técnicas, sino que se trata de establecer una cultura de la seguridad de la información y poner en marcha medidas técnicas y organizativas adaptadas a las necesidades del puesto de trabajo que son, en la mayoría de los casos, sencillas. La aplicación de estas medidas, junto a un adecuado plan de formación y concienciación de las personas trabajadoras que gestionan la información desde sus puestos de trabajo, nos ayudará a proteger de manera adecuada nuestra organización.

"MITIGAR LOS RIESGOS DEL PUESTO DE TRABAJO DE UNA FORMA SIGNIFICATIVA NO REQUIERE DE LA IMPLANTACIÓN DE COMPLEJAS MEDIDAS TÉCNICAS, SINO QUE SE TRATA DE ESTABLECER UNA CULTURA DE LA SEGURIDAD DE LA INFORMACIÓN Y PONER EN MARCHA MEDIDAS TÉCNICAS Y ORGANIZATIVAS ADAPTADAS A LAS NECESIDADES DEL PUESTO DE TRABAJO QUE SON, EN LA MAYORÍA DE LOS CASOS, SENCILLAS".

ESCENARIOS DE RIESGO

No siempre los incidentes de seguridad se producen por usuarios malintencionados. A menudo, se trata de usuarios que llevan a cabo prácticas no recomendables, que pueden ser aprovechadas por un atacante externo o interno, o simplemente llevar asociadas consecuencias indeseables.

Veamos, como ejemplo, algunos escenarios de riesgo que nos podemos encontrar, de forma habitual, en nuestro puesto de trabajo:

Un usuario detiene el antivirus corporativo porque le impide llevar a cabo alguna acción. Más tarde, ejecuta un archivo que le llega por correo electrónico, infectando su equipo y toda la red de la organización.

Un usuario tira a la papelera los exámenes del último proceso de selección, que acaban en un contenedor y son recogidos por una tercera persona.

Un usuario copia en un pendrive documentación para seguir trabajando desde casa. El pendrive se pierde en el autobús, alguien lo encuentra y la información termina publicándose.

Un usuario vende su portátil personal. Aunque no se trata de una herramienta profesional, era habitual que lo utilizase para gestionar y guardar información corporativa. Mediante un sencillo programa de recuperación, el comprador recupera la información y la hace pública.

Un usuario deja en la bandeja de la impresora documentos que contienen datos personales. Un ciudadano descontento aprovecha que no le ve nadie para coger los documentos.

Un usuario recibe un correo electrónico de un destinatario desconocido que le alienta a descargar un archivo adjunto que contiene un código malicioso, técnica a través de la cual logra obtener información confidencial de la organización.

“NO SIEMPRE LOS INCIDENTES DE SEGURIDAD SE PRODUCEN POR USUARIOS MALINTENCIONADOS. A MENUDO, SE TRATA DE USUARIOS QUE LLEVAN A CABO PRÁCTICAS NO RECOMENDABLES, QUE PUEDEN SER APROVECHADAS POR UN ATACANTE EXTERNO O INTERNO, O SIMPLEMENTE LLEVAR ASOCIADAS CONSECUENCIAS INDESEABLES”.

¿QUÉ PODEMOS HACER PARA EVITARLO? MEDIDAS DE SEGURIDAD

Vistos los escenarios anteriores, es lógico preguntarse cómo podemos evitar o mitigar los riesgos. Lo primero y fundamental es implantar una **Política de Seguridad** interna de la organización, que transmita a los usuarios de los sistemas de información de la organización las obligaciones y buenas prácticas en relación con la seguridad de la información. Y es que, la seguridad de la información es un esfuerzo conjunto, que requiere la implicación y participación de todas las personas usuarias que utilicen los sistemas de información para el desempeño de su trabajo, y en su caso, el personal externo vinculado a prestaciones de servicios.

En la Diputación de Valencia, contamos con el **Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal en la Diputación Provincial de Valencia**, aprobado por acuerdo del Pleno de la Corporación de fecha 18 de junio de 2013 -BOP 159, de 6 de julio-, cuyo artículo 37.1 establece que deberán elaborarse un conjunto de reglas y directrices de carácter obligatorio que desarrollen el contenido de dicha Política.

Por Decreto nº 6111, de 26 de junio de 2015, se aprobaron las **Normas de Seguridad para los Usuarios de los Sistemas de Información**, de aplicación a todos los sistemas de información TIC, así como a aquellos sistemas de información de cualquier naturaleza que traten datos de carácter personal, que sean de la titularidad de la Diputación de Valencia o cuya gestión o responsabilidad tenga encomendada, como es el caso de la información municipal. Estas son algunas de las medidas contempladas:

MEDIOS TECNOLÓGICOS

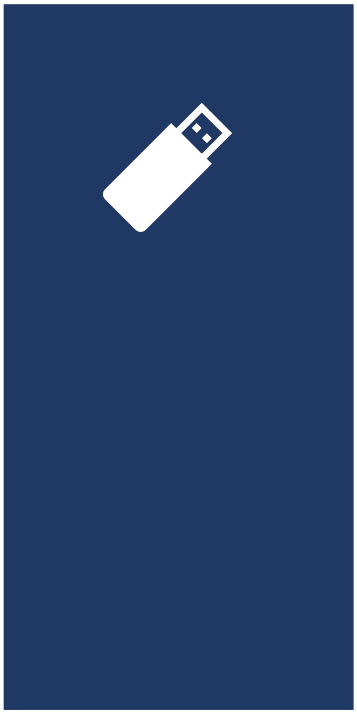
- El uso de los recursos facilitados a los usuarios por la organización para el desarrollo de la actividad, con fines distintos a los autorizados, está estrictamente prohibido.
- No está permitido alterar la configuración hardware de los equipos ni conectar otros dispositivos a estos a iniciativa del usuario, así como variar su ubicación.
- No está permitido alterar la configuración software de los equipos, desinstalar o instalar programas distintos a la configuración establecida por el Servicio de Informática.
- No está permitida la instalación, utilización o conexión a la red corporativa de cualquier medio tecnológico distinto de los admitidos, habilitados y configurados por el Servicio de Informática, sin contar con su autorización.
- No está permitido almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento compartidos.

DISPOSITIVOS PORTÁTILES Y MÓVILES

- Está prohibido utilizar dispositivos portátiles y móviles no proporcionados por la Corporación para almacenar, acceder, transmitir o tratar de cualquier otro modo información, salvo si se cuenta con autorización.
- En principio, los dispositivos portátiles y móviles deberán utilizarse únicamente para fines profesionales, no para fines privados.
- Este tipo de dispositivos estará bajo la custodia del usuario que los utilice, el cual deberá adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de personas no autorizadas.
- La pérdida o sustracción de estos dispositivos se deberá poner inmediatamente en conocimiento del Servicio de Informática de la Corporación, para la adopción de las medidas que correspondan y a efectos de baja en el inventario.
- Los usuarios de estos dispositivos deberán realizar conexiones periódicas a la red corporativa, según las instrucciones proporcionadas por el Servicio de Informática, para permitir la actualización de aplicaciones, sistema operativo, firmas de antivirus y demás medidas de seguridad.
- Cuando se modifiquen las circunstancias profesionales (término de una tarea, cambio de puesto o funciones, cese en el cargo, etc.) que originaron la entrega de un recurso informático móvil, el usuario lo devolverá al Servicio de Informática de la Corporación, al objeto de proceder al borrado seguro de la información almacenada y, en su caso, restaurar el equipo a su estado original para que pueda ser asignado a un nuevo usuario.

SOPORTES ELECTRÓNICOS DE INFORMACIÓN

- Está prohibido utilizar soportes electrónicos de información no proporcionados por la Corporación para almacenar información, salvo si se trata de información clasificada como PÚBLICA y se cuenta con la autorización correspondiente.

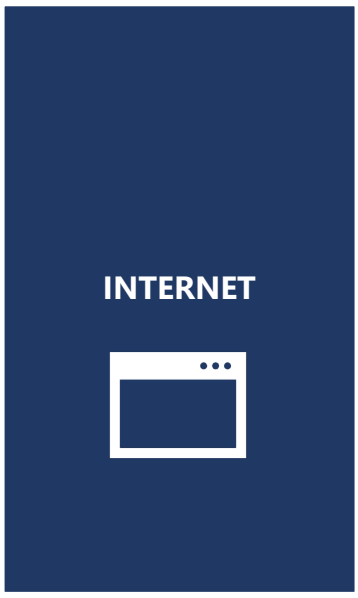


- Si se produjese la sustracción, pérdida o acceso indebido a los soportes de información deberá ponerse en conocimiento del Responsable de Seguridad de los Sistemas de Información, a través del sistema de notificación de incidencias de seguridad.

- En el traslado de soportes de información se adoptarán las pertinentes medidas para evitar la sustracción, pérdida o acceso indebido a la información durante su transporte, especialmente cuando la información contenida en el soporte no haya sido objeto de cifrado. Se dispondrá de un procedimiento rutinario que coteje las salidas con las llegadas y levante las alarmas pertinentes cuando se detecte algún incidente. En caso de sustracción, pérdida o acceso indebido a la información durante su transporte deberá ponerse en conocimiento del Responsable de Seguridad de los Sistemas de Información, a través del sistema de notificación de incidencias de seguridad.

- Únicamente podrán utilizarse las herramientas y programas de correo electrónico suministrados, instalados y configurados por el Servicio de Informática de la Diputación de Valencia.

- El correo corporativo deberá utilizarse, única y exclusivamente, para la realización de las funciones encomendadas al personal, evitando el uso privado del mismo.



- Sólo se podrá acceder a Internet mediante los navegadores suministrados y configurados por el Servicio de Informática en los puestos de usuario. No podrá alterarse la configuración del mismo ni utilizar un navegador alternativo sin la debida autorización del Servicio de Informática.

- La utilización de Internet debe obedecer a fines profesionales, teniendo siempre en cuenta que se están utilizando recursos informáticos restringidos y escasos. El acceso a Internet para fines personales tendrá carácter extraordinario, debiéndose limitar su utilización dentro de un tiempo razonable que no interfiera en el rendimiento profesional ni en la eficiencia de los recursos informáticos corporativos.

IMPRESORAS, FOTOCOPIADORAS, ESCÁNERES Y FAXES

- Con carácter general deberán utilizarse las impresoras en red y las fotocopiadoras corporativas. Excepcionalmente podrán instalarse impresoras locales, gestionadas por un puesto de trabajo de usuario. En este caso, la instalación irá precedida de la autorización pertinente por parte del responsable del peticionario.

- Cuando se imprima, fotocopie, digitalice o se remita por fax documentación, deberá permanecer el menor tiempo posible en las bandejas de salida de los equipos implicados, para evitar que terceras personas puedan acceder a la misma.

- Conviene no olvidar retirar los originales de la fotocopiadora, impresora, escáner o fax una vez finalizado el proceso correspondiente.

- Si se encontrase documentación abandonada en una fotocopiadora, impresora, escáner o fax, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente. En caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento del superior jerárquico.

- Con carácter general, cuando se digitalicen documentos el usuario deberá ser especialmente cuidadoso con la selección del directorio compartido donde habrán de almacenarse las imágenes obtenidas, especialmente si contienen información no clasificada como PÚBLICA.

CONTROL DE ACCESOS A LOS SISTEMAS DE INFORMACIÓN

- Los mecanismos que se pongan a disposición de los usuarios para su debida identificación y autenticación en los sistemas de información (claves concertadas, contraseñas, tarjetas de identificación, etc.) serán personales e intransferibles.

- Los usuarios son responsables de la custodia de los mismos y de toda actividad relacionada con el uso de su acceso autorizado, por lo que no deberán en ningún caso revelar o entregar, bajo ningún concepto, sus mecanismos de credenciales de acceso a terceras personas, ni siquiera a otros usuarios o personal al servicio de la Diputación de Valencia, ni

mantenerlas por escrito a la vista o al alcance de terceros. Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización de su titular.

- Si un usuario tiene sospechas de que sus credenciales están siendo utilizadas por otra persona, debe proceder inmediatamente a comunicar la correspondiente incidencia de seguridad. Del mismo modo deberá actuarse cuando se produzca la pérdida o extravío del mecanismo, un mal funcionamiento o cualquier otro comportamiento anómalo del mismo.

SEGURIDAD EN EL ENTORNO DE TRABAJO

- Los puestos de trabajo permanecerán despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento. Aquella documentación que no se vaya a utilizar en el momento deberá guardarse en cajones bajo llave o en los armarios o archivadores correspondientes.

- Cualquier usuario que se ausente temporalmente de su puesto de trabajo deberá bloquear la sesión de su ordenador (salvapantallas con contraseña, etc.) para impedir el acceso de otras personas a la información y al equipo informático. Se establecerán bloqueos de sesión automáticos por tiempo de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.

- Al final de la jornada de trabajo los usuarios deberán asegurarse de que el equipo está apagado y que no se deja accesible documentación ni soportes de información de ningún tipo.

- Cuando se utilicen pizarras y *flipcharts* los usuarios deberán asegurarse de que se limpian adecuadamente, para que no quede ningún tipo de información a la vista, antes de abandonar las salas o despachos donde se ubiquen o permitir que alguien ajeno entre.

- La comida y bebida pueden dañar tanto los componentes electrónicos como los soportes de información, por lo que no deberán realizarse estas acciones en el puesto de trabajo, salvo que se adopten todas las garantías que impidan el riesgo de daño mencionado.

ARCHIVADORES Y RECINTOS DEDICADOS AL ALMACENAMIENTO DE INFORMACIÓN

- Los armarios, archivadores u otros elementos en los que se ubiquen los soportes de información deberán disponer de mecanismos de cierre que impidan el acceso a personas no autorizadas.
- Siempre que sea posible, dichos armarios o archivadores deben encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los soportes de información que contienen.
- Deberá evitarse el almacenamiento, depósito o archivo de soportes de información en recintos o armarios de uso común, salvo que se garantice la existencia de mecanismos que hagan posible el acceso a la información únicamente al personal autorizado en cada caso.
- Las dependencias destinadas al archivo de información no se utilizarán para otros usos, como el de almacén de papelería, de utensilios informáticos, material de limpieza, taquillas y vestidores o cualquier otra utilidad que suponga el acceso a dichos recintos de personal distinto al autorizado para acceder a la información almacenada.

INFORMACIÓN EN SOPORTES NO AUTOMATIZADOS

- Mientras la documentación no se encuentre archivada, por estar en proceso de revisión o tramitación, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir que pueda ser accedida por persona no autorizada.
- La destrucción de los documentos se realizará mediante máquinas destructoras, de forma que se evite la recuperación o reconstrucción de la información con posterioridad.
- Siempre que se proceda al traslado físico de documentos que contengan información no clasificada como PÚBLICA, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

"LA SEGURIDAD DE LA INFORMACIÓN ES UN ESFUERZO CONJUNTO, QUE REQUIERE LA IMPLICACIÓN Y PARTICIPACIÓN DE TODAS LAS PERSONAS USUARIAS QUE UTILICEN LOS SISTEMAS DE INFORMACIÓN".

MATERIAL COMPLEMENTARIO

- "Protección del puesto de trabajo", del Instituto Nacional de Ciberseguridad (INCIBE). Consulta el documento en este enlace.
- "Evitando riesgos de ciberseguridad en el puesto de trabajo" de INCIBE. Consulta la publicación en este enlace.
- "Checklist básico para la protección del puesto de trabajo", de INCIBE. Consulta el checklist en este enlace.
- Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal en la Diputación Provincial de Valencia, aprobado por acuerdo del Pleno de la Corporación de fecha 18 de junio de 2013 -BOP 159, de 6 de julio-.
- Decreto nº 6111, de 26 de junio de 2015, Normas de Seguridad para los Usuarios de los Sistemas de Información. Diputación Provincial de Valencia.

NOTICIAS

- **La Agencia Española de Protección de Datos (AEPD) nos habla de la privacidad en las reuniones online.** Las reuniones virtuales online mediante voz, vídeo o a través de servicios web son una constante del trabajo actual y del teletrabajo, que se ha visto enormemente potenciado por motivo de la pandemia de la COVID-19. Si bien cada vez somos más conscientes de la necesidad de proteger nuestra privacidad y seguridad en el mundo online, con las reuniones virtuales debemos adoptar medidas específicas.

  Consulta el artículo de la AEPD en este enlace.

- **El Centro Criptológico Nacional (CCN) emite unas recomendaciones para métodos de evaluación y exámenes en remoto de forma segura.** El CCN recoge las principales medidas a adoptar para asegurar y preservar la integridad de los métodos de evaluación y examen en remoto.

  Consulta el documento en este enlace.

- **El Instituto Nacional de Ciberseguridad (INCIBE) nos habla de "Buenas prácticas en redes sociales".** Aunque las redes sociales pueden ser unas herramientas de gran valor, no podemos obviar que muchas veces son un blanco fácil para los ciberdelincuentes, aprovechando en muchas ocasiones el desconocimiento de los peligros asociados a su uso por parte de sus administradores. INCIBE nos habla de los riesgos que conlleva el uso de las mismas, para evitar ser víctimas de incidentes de seguridad.

  Consulta el artículo en este enlace.