CPIFP HURTADO DE MENDOZA
ESCUELA DE HOSTELERÍA
Y TURISMO DE GRANADA

MANUAL DEL BUEN USO DEL EQUIPAMIENTO INFORMÁTICO

#TDE
TRANSFORMACIÓN DIGITAL EDUCATIVA

ÍNDICE

1. NORMAS Y RECOMENDACIONES PARA EL USO RESPONSABLE DEL EQUIPAMIENTO INFORMÁTICO DEL CENTRO

1.1 NORMAS Y RECOMENDACIONES PARA EL ALUMNADO

El objetivo de las siguientes normas generales es promover el uso responsable y seguro del equipamiento informático y digital del Centro. Además, tienen el objetivo de prolongar la vida útil de los equipos informáticos y que alumnado y profesorado lo pueda aprovechar y utilizar en las mejores condiciones:

- Los equipos informáticos son de uso exclusivamente educativo y solamente se pueden utilizar en horario lectivo y con la supervisión del profesorado.
- No se pueden utilizar los equipos informáticos del Centro para juegos, música, vídeos que no tengan relación con las clases, redes sociales o mensajería instantánea.
- Prohibido consultar, crear o compartir mensajes, imágenes, vídeos, páginas web o cualquier otro contenido de carácter ilegal o dañino.
- Se debe proteger la información propia y de los demás.
- No almacenar en los equipos información personal, imágenes, vídeos, ni permitir que éstos recuerden las contraseñas.
- No compartir las contraseñas con nadie (salvo con el profesorado para solventar incidencias técnicas, y una vez solventadas , volverlas a cambiar).
- Acordarse siempre de cerrar sesión.
- Proteger la documentación de trabajo.
- Guardar los documentos de trabajo sólo en el lugar indicado por los docentes (carpeta online de Google Classroom o similar, por lo general).
- Hacer copias de seguridad en dispositivos extraíbles (memoria USB, tarjeta de memoria) o en la nube (Dropbox, Google Drive, OneDrive, etc.).
- Protegerse de virus y malwares. Al conectar un dispositivo extraíble (pincho USB, tarjeta de memoria) o descargar un archivo de Internet analizarlo siempre con el antivirus.
- Desconfiar de mensajes y enlaces sospechosos, extender enlaces cortos y analizar URLs antes de abrirlas.
- Cuidar de los recursos informáticos como si fueran tuyos.
- Evitar golpes, transportar los equipos portátiles con seguridad, usar fundas protectoras…
- Evitar líquidos cerca del equipamiento informático ya que puede perjudicar gravemente a los equipos, teclados, etc. si se derrama sobre ellos.
- No desconectar los cables bruscamente ya que podría dañar el propio cable, las clavijas, etc.
- Evitar desconectar cables de proyectores, ordenadores de aula, etc.
- No personalizar configuraciones en equipos, ni instalar o desinstalar programas y aplicaciones.

- Si los equipos alertan sobre una posible amenaza, no hay que saltarse dichas restricciones de seguridad.
- Seguir las pautas de carga de batería y almacenamiento de dispositivos móviles.
- Apagar siempre los equipos informáticos después de su utilización. De esta forma, habrá ahorro energético y se evitará que los datos de navegación queden expuestos (los equipos están congelados y todos los datos se borran automáticamente con el apagado).
- Los equipos informáticos deben encenderse cuando vayan a usarse para prolongar su vida útil y ahorrar costes energéticos.
- Colaborar con el profesorado y apagar los equipos informáticos al finalizar la clase.
- Comprobar el estado del equipo al iniciar y terminar la clase. Ante cualquier problema informar al profesor para registrar la incidencia.

Imagen 1: Aula de nuestro Centro. Elaboración propia

1.2 NORMAS Y RECOMENDACIONES PARA EL PROFESORADO

Las normas para profesorado son muy similares a las anteriormente mencionadas para el alumnado, aunque su cumplimiento es aún más importante ya que el profesor es referencia y modelo del uso responsable de los equipos informáticos del Centro.

Además de todas las normas y recomendaciones anteriores, se añaden las siguientes normas específicas:

- Los equipos informáticos y proyectores solamente deben encenderse cuando vayan a usarse para prolongar su vida útil y ahorrar costes energéticos.
- El profesorado que se encuentre a última hora en un aula será el encargado de comprobar que todos los equipos informáticos y proyectores estén apagados.
- Los equipos de los despachos y departamentos también deben ser apagados por el profesorado que los use en las últimas horas o cuando no vayan a ser utilizados.

2. AMENAZAS MÁS IMPORTANTES EN EL USO DE LAS TIC

2.1 PRINCIPALES AMENAZAS EN EL USO DE LAS NUEVAS TECNOLOGÍAS

2.1.1 Ciberacoso

El **ciberacoso o ciberbullying**, es el acoso entre iguales llevado a cabo a través de medios telemáticos como Internet, teléfonos móviles, videojuegos, etc. Por norma general, viene asociado con amenazas, insultos, vejaciones o de la creación de perfiles en redes sociales suplantando la identidad de la víctima y asociándola a contenidos vejatorios, del etiquetado de fotografías de otras personas o cosas con intención ofensiva hacia la víctima.

De acuerdo con el psicólogo José María Avilés[1], algunas de las manifestaciones más frecuentes del ciberbullying son:

- Envío repetido de mensajes ofensivos e insultantes hacia un determinado individuo
- Luchas online a través de mensajes electrónicos (chat, mensajería instantánea vía móvil, SMS, redes sociales…) con un lenguaje enfadado y soez.
- Envío de mensajes que incluyen amenazas de daños y que son altamente intimidatorios. Además, se acompañan de otras actividades (acecho, seguimiento) en la red que hacen que la persona tema por su propia seguridad.

[1] INTECO. Guía de actuación contra el ciberacoso
http://www.injuve.es/sites/default/files/Gu%C3%ADa%20de%20actuaci%C3%B3n%20contra%20el%20ciberacoso.pdf

- Enviar o propagar cotilleos crueles o rumores sobre alguien que dañan su reputación o la dañan ante sus amigos.
- Pretender ser alguien que no se es y enviar o difundir materiales e informaciones online que dejan mal a la persona en cuestión, la ponen en riesgo o causan daño a su reputación ante sus conocidos y/o amigos.
- Compartir online información secreta o embarazosa de alguien. Engañar a alguien para que revele información secreta o embarazosa que después se comparte online.
- Excluir intencionalmente a alguien de un grupo online, como una lista de amigos
- Enviar programas basura: virus, suscripción a listas de pornografía, colapsar el buzón del acosado etc.
- Grabar y colgar en Internet vídeos de peleas y asaltos a personas a quienes se agrede y que después quedan expuestas a todos.
- Grabar actividades sexuales en el móvil o con webcam y enviarlo a la pareja, quien lo comparte con sus amigos con la intención de molestar y denigrar intencionadamente.
- Utilizar un blog personal para denigrar y hablar mal de una persona.
- Manipular materiales digitales: fotos, conversaciones grabadas, correos electrónicos, cambiarlos, trucarlos y modificarlos para ridiculizar y dañar a personas.
- Robar contraseñas para suplantar su identidad

*Imagen 2: Foto de manos computadora creado por **rawpixel.com** - www.freepik.es*

2.1.2 Grooming

El grooming es "un acoso ejercido por un adulto y se refiere a acciones realizadas deliberadamente para establecer una relación y un control emocional sobre un niño o niña con el fin de preparar el terreno para el abuso sexual del menor. Se podría decir que son situaciones de acoso con un contenido sexual explícito o implícito".[2]

Se caracteriza por:

- Inicio en la fase de amistad. Hace referencia a la toma de contacto con el menor de edad para conocer sus gustos, preferencias y crear una relación de amistad con el objeto de alcanzar la confianza del posible afectado.

- Inicio de la fase de relación. La fase de formación de la relación incluye con frecuencia confesiones personales e íntimas entre el menor y el acosador. De esta forma se consolida la confianza obtenida del menor y se profundiza en información sobre su vida, sus gustos y costumbres.

- Componente sexual. Con frecuencia incluye la descripción de términos específicamente sexuales y la petición a los menores de su participación en actos de naturaleza sexual, grabación de imágenes o toma de fotografías.

2.1.3 Suplantación de identidad

Se produce cuando una persona se apropia indebidamente de otra identidad digital y la usa para conseguir información personal, para publicar y desprestigiar, extorsionar o chantajear… También se produce cuando una persona crea una cuenta o perfil con los datos de otra y se hace pasar por ella actuando en su nombre.

2.1.4 Sexting

Consiste en enviar mensajes, fotos o videos de contenido erótico, sexual y pornográfico, mediante aplicaciones de mensajería en tiempo real. Los riesgos se encuentran en la exposición y divulgación de este contenido íntimo.

[2] https://www.eicyc.es/que-es-grooming/

2.1.5 Phishing

El phishing es un tipo de estafa que intenta obtener datos, contraseñas, cuentas bancarias, números de tarjetas de crédito o del documento nacional de identidad de la víctima mediante engaño para utilizarlos en el robo o sustracción de fondos de sus cuentas. Generalmente se obtienen estos datos solicitando al usuario datos personales haciéndose pasar por una empresa o entidad pública con la excusa de comprobarlos o actualizarlos. Esta petición de datos se suele realizar a través de un SMS, whatsapp, una llamada telefónica, un correo electrónico o una ventana emergente durante la navegación por Internet.

*Imagen 3: Vector de web móvil creado por **storyset** - www.freepik.es*

2.1.6 Ciberadicción

Consiste en la «conexión compulsiva» y en la necesidad de tener que conectarse con frecuencia muchas veces al día. Esto tiene consecuencias como la dispersión de la atención, la búsqueda constante de contenidos relacionados con ciertos gustos o adicciones, la creación de distintas identidades, la sustitución de lo real por lo vivido en entornos virtuales, la pérdida de la noción del tiempo, mal humor o nerviosismo cuando no se puede conectar o la conexión es lenta, o dedicar menos horas de sueño y comida.

2.1.7 Otros riesgos

- **Contenidos violentos y pornográficos**: Los menores de edad cada vez están más expuestos a contenidos violentos y cada vez tienen más acceso a la pornografía.

- **Compras de juegos en línea**: Son una actividad recurrente entre los jóvenes. Los riesgos se encuentran en las estafas o robos cuando se adquieren estos juegos en plataformas de dudosa procedencia.

- **Apuestas en línea**: Son una serie de actividades virtuales que generan adicción en adultos, como adolescentes. Estas están relacionadas con los juegos de azar.

2.2 VIRUS Y SOFTWARE MALICIOSO

Alumnado y profesorado utilizan a diario los equipos informáticos de nuestro Centro para desarrollar diferentes tareas, ya sean académicas, evaluativas o administrativas. Por ello, es esencial llevar a cabo una serie de consejos para garantizar la seguridad de los datos y la protección frente a los virus.

Un virus es "un software informático malicioso o un archivo ejecutable o código que se reproduce cuando un usuario accede a este de distintas formas"[3]. Antes de ahondar en los consejos para evitar virus y brechas de seguridad, es necesario definir una serie de conceptos para entender la diferencia entre los diversos tipos de ataques informáticos:

- **Troyanos**: Este tipo de virus se suele presentar en forma de ejecutable. Al ejecutarlo permite al delincuente un acceso remoto al equipo infectado.

- **Gusanos**: Tiene la capacidad para replicarse en tu sistema, por lo que el dispositivo puede llegar a enviar cientos o miles de copias de sí mismo, con el problema que eso supone.

- **Spyware**: Es un software que recopila información de un dispositivo, como la navegación del usuario, datos personales, bancarios. El software monitoriza y rastrea nuestra actividad para luego enviarla al delincuente.

- **Malware**: Se trata de códigos diseñados para alterar el normal funcionamiento del ordenador, sin el permiso o el conocimiento del usuario. Este tipo de virus pueden destruir o corromper los archivos del disco duro.

[3] https://informatix.es/los-tipos-de-virus-informaticos-mas-comunes/

- **Adware**: Se trata de anuncios que aparecen en el navegador con pop-ups o ventanas con gran contenido visual, e incluso audios. Es aquel software que ofrece publicidad no deseada o engañosa con el fin de generar ganancias económicas a los creadores

- **Ransomware**: El ciberdelincuente bloquea el dispositivo con un mensaje solicitando un rescate para liberarlo.

- **Apps maliciosas**: Se trata de aplicaciones que instalamos en nuestro dispositivo móvil y que lo infecta para robar información almacenada como contactos, imágenes, contraseñas, datos de navegación, etc. Es muy importante leer bien los permisos que se conceden al instalar una nueva app, ya que muchos pueden no tener relación alguna con la funcionalidad que dicha app nos ofrece.

- **Denegación de servicio**: Provoca ataques a plataformas conectadas para que sus servicios queden inaccesibles e inutilizados por sus administradores y usuarios.

Imagen 4: Vector de ataque cibernético creado por freepik - www.freepik.es

2.2.1 Consejos para evitar virus y software malicioso

- Instalar un antivirus de confianza en nuestros dispositivos. Se debe utilizar el antivirus para escanear los archivos descargados antes de ejecutarlos.

- Realizar actualizaciones regularmente. Debemos mantener el software de nuestros equipos actualizado ya que estas ayudan a eliminar posibles brechas de seguridad. Es recomendable activar la función automática de actualización periódica del software.

- No conectar ningún dispositivo extraño a tu equipo, ya que puede contener virus o software malicioso. En el caso de que sea necesario, realizar un escaneo completo del dispositivo USB con nuestro antivirus antes de ejecutarlo.

- Antes de abrir los archivos adjuntos, hay que estar 100% seguros de que se trata de correo fiable. Es importante detectar la fiabilidad de los correos electrónicos que recibimos. Debemos tener en cuenta que muchos *hackers* suelen utilizar correos falsos de empresas conocidas para que confiemos. Hay que utilizar la lógica, analizar bien estos correos y evitar abrir adjuntos o proporcionar información personal (datos bancarios, contraseñas, etc.).

- No instalar software de procedencia desconocida.

- No hacer clic en anuncios o ventanas emergentes.

- Es muy recomendable contar siempre con una copia de seguridad de los datos más importantes en un disco duro o USB. De esta forma, si el equipo sufre un ataque de virus o de software malicioso, nuestra copia desconectada de dicho equipo estará a salvo.

Imagen 5: Vector de malware creado por rawpixel.com - www.freepik.es

2.3 RECOMENDACIONES BÁSICAS DIRIGIDAS A PADRES Y MADRES PARA EVITAR RIESGOS DE LAS TIC

A continuación, se detallan algunas recomendaciones para que los padres / madres / tutores legales de los menores de edad puedan evitar los riesgos asociados a las nuevas tecnologías que se han ido describiendo anteriormente:

1. Establecer horarios. Se recomienda el uso máximo de dos horas al día para realizar actividades en entornos digitales. El tiempo para entretenimiento debe ser menor.

2. Promover el uso de pantallas en espacios abiertos. El objetivo es observar claramente las actividades que los menores realizan online.

3. Hablar con los hijos sobre medidas de seguridad online. Debemos concienciar a los menores de los riesgos online y de que solo tengan acceso a páginas seguras.

4. Restringir los ajustes de privacidad en diversas aplicaciones, como son los videojuegos. Una forma de protección es tener acceso a sus cuentas y revisarlas periódicamente.

5. Restringir el uso de la cámara web para proteger la identidad del menor.

6. Deshabilitar el GPS o los permisos de localización. De esta forma, nadie podrá conocer la ubicación del menor y el peligro será menor.

7. Enseñar a crear contraseñas seguras y a no compartirlas con extraños. Las contraseñas deben contar con números y letras.

3. CONSEJOS PARA CREAR CONTRASEÑAS SEGURAS

1. Debe tener como mínimo 10-12 caracteres. Si es más larga, será más segura.

2. Evitar secuencias del tipo “123456” o “111111”, o “qwerty”, así como palabras comunes como “contraseña1”.

3. Usar caracteres variados: minúsculas, mayúsculas, símbolos y números deben formar parte de la contraseña. A mayor variedad, más impredecible y segura es la contraseña.

4. Usar palabras poco comunes o inesperadas.

5. Si la contraseña es una secuencia de palabras, desordenarlas para que sea poco predecible.

6. Evitar los sustitutos obvios de los caracteres (0 en lugar de O).

7. No reutilices contraseñas. Repetir contraseñas puede comprometer la seguridad de varias cuentas.

8. Lo importante es que tú recuerdes la contraseña. Usa algo que tenga sentido para ti pero que sea muy difícil de adivinar tanto por otras personas como por métodos de hackeo que utilizan combinaciones predecibles.

Para garantizar la seguridad, debemos también seguir las siguientes recomendaciones:

- No escribir las contraseñas en hojas de papel.

- No almacenar contraseñas en aplicaciones como “Notas” en el teléfono móvil.

- No guardar las contraseñas en el autocompletado del navegador.

*Imagen 6: Vector de seguridad internet creado por **jcomp** - www.freepik.es*

4. RECOMENDACIONES PARA TRABAJAR Y ESTUDIAR DE FORMA SALUDABLE

La información de esta sección se ha adaptado del manual publicado por la Consejería de Empleo, Formación y Trabajo Autónomo de la Junta en Andalucía denominado **Recomendaciones para teletrabajar de forma segura y saludable[4].**

Alumnado y profesorado emplean muchas horas a la semana utilizando dispositivos informáticos. Es por ello por lo que es esencial seleccionar adecuadamente el lugar de estudio y trabajo, el mobiliario, la ergonomía y la postura mientras se trabaja y estudia, así como otras condiciones como pueden ser la iluminación, rutinas saludables, etc. A continuación, se detallan recomendaciones de dicho manual.

4.1 SELECCIÓN DEL LUGAR DE ESTUDIO / TRABAJO

- El puesto de trabajo debe ubicarse en una estancia donde no se desarrollen otras tareas familiares o domésticas, para evitar interrupciones que dificulten la concentración.
- Se recomienda delimitar el lugar elegido para trabajar, para distinguirlo así de otros contextos propios de la vida doméstica. Si no se dispone de una habitación independiente, puede habilitarse una zona con los elementos y accesorios que se hagan necesarios para llevar a cabo las tareas.
- La habitación elegida debe contar con un buen nivel de iluminación, preferentemente natural, y con una buena ventilación.
- En el campo visual del estudiante / trabajador no debe haber fuentes de luz brillante que produzcan deslumbramiento directo (focos en el techo, ventanas, lámparas, etc.) o indirecto (reflejos en la pantalla, la mesa o el suelo, por ejemplo). Se recomienda que la fuente de iluminación natural incida de manera lateral al puesto de trabajo y al equipo informático.
- Debe haber enchufes en las proximidades para conectar el equipo informático y una lámpara de apoyo si es necesaria. En caso de utilizar regletas no hay que sobrecargarlas, especialmente si se utilizan calefactores. La ubicación de estas debe escogerse minimizando el riesgo de tropezar con los cables.

4.2 ORGANIZACIÓN DEL TRABAJO

Hay que proponerse no dedicar tiempo a otras acciones improductivas para el desempeño de las tareas o el estudio, tales como el uso por inercia del teléfono móvil o las redes sociales. Estas acciones pueden desarrollarse en los períodos que se dispongan de descanso.

[4] https://www.juntadeandalucia.es/export/drupaljda/guia-teletrabajo-cefta-covid19.pdf

Resulta de gran utilidad y efectividad establecer cada cierto tiempo un plan con tareas pendientes, así como fijar plazos y objetivos en un calendario.
Es recomendable seguir un horario preestablecido para aumentar la eficacia del tiempo dedicado al estudio o trabajo. De esta forma, resulta más sencillo compatibilizar con las tareas domésticas, familiares y sociales.

4.3 SELECCIÓN DEL MOBILIARIO

4.3.1 Selección de la mesa de trabajo

- La mesa utilizada debe tener la superficie necesaria para colocar el ordenador portátil o la pantalla y el teclado alineados frente al puesto de trabajo y asegurar una cierta libertad de movimientos.
- Es importante que la altura de la mesa esté aproximadamente a la altura de los codos del usuario cuando está sentado, ya que la postura ideal para evitar posturas forzadas o sobretensiones es tener los codos en descanso y flexionados 90º.

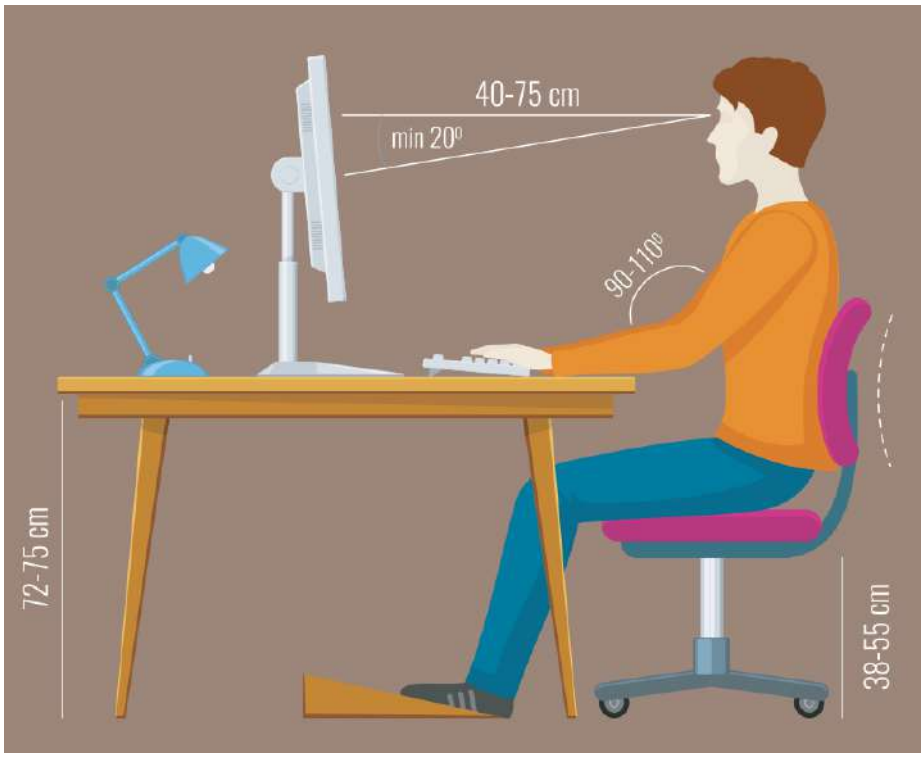

Imagen 7. Disposición de la mesa y silla de trabajo. Consejería de Empleo, Formación y Trabajo Autónomo. Junta de Andalucía

- Para posibilitar el apoyo de los antebrazos o de las muñecas en la mesa, la distancia horizontal entre el teclado y el borde frontal del tablero debe superar los 10 centímetros.

- Es importante que el borde superior de la pantalla quede a la altura de la horizontal de los ojos o ligeramente por debajo, a fin de asegurar una postura natural en el cuello.
- El espacio libre debajo de la mesa debe ser suficiente para que las piernas puedan moverse.
- Es conveniente utilizar mesitas y apoyos auxiliares para tener cerca los materiales que se usen de forma frecuente sin que ocupen un espacio extra.
- En caso de que deban emplearse tablets durante un tiempo prolongado, es importante colocarlas sobre la mesa utilizando atriles o fundas con función soporte. De lo contrario, pueden adoptarse posturas en las que el cuello se encuentre excesivamente flexionado.

4.3.2 Selección de la silla de trabajo

- Se recomienda utilizar sillas de escritorio con base giratoria y regulable en altura, así como aquellas otras opciones de adaptación complementarias para, desde un punto de vista de ergonomía y antropometría, proporcionar una posición postural y un ajuste lumbar correctos.
- En caso de que no sea posible, se aconseja optar por una silla estable sin salientes o rebordes que, asimismo, esté tapizada con un tejido que facilite la transpiración.
- El respaldo tiene que permitir apoyar la espalda correctamente con fijación de la zona lumbar y cobertura suficiente.
- Debe evitarse que el borde del asiento presione la parte posterior de las piernas, para evitar así que la presión ejercida dificulte la circulación sanguínea.
- Debe ser posible apoyar ambos pies en el suelo, con las piernas dobladas 90º. Si el ajuste correcto de la silla no lo permite, tendremos que utilizar un apoyo a modo de reposapiés para mantener la postura indicada.

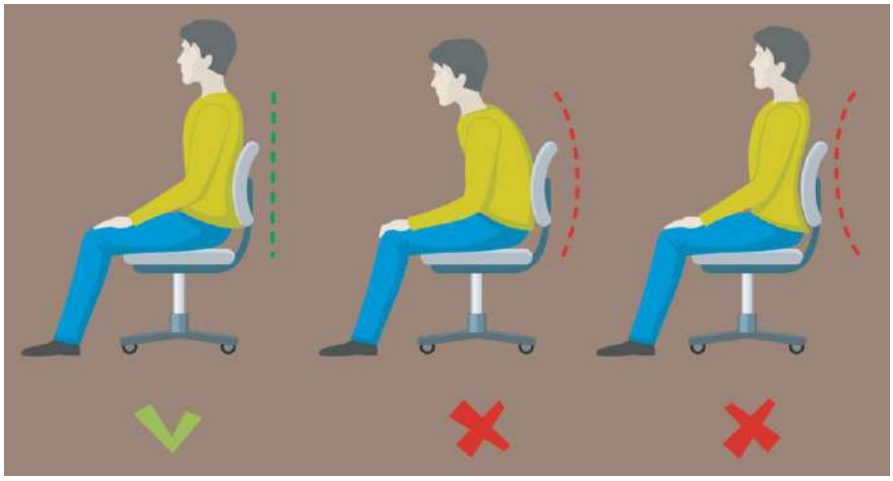

Imagen 8. Ergonomía en la silla de trabajo. Consejería de Empleo, Formación y Trabajo Autónomo. Junta de Andalucía

4.4 PREVENCIÓN DE RIESGOS

4.4.1 Prevención de la fatiga visual

- Para evitar problemas de visión, la distancia entre los ojos y la pantalla utilizada debe estar comprendida entre 40 y 55 centímetros.
- La pantalla, el teclado y los documentos que se consulten en papel deben situarse a una distancia similar y estar cercanos, para minimizar adicionalmente los giros de cuello y cabeza.
- El acabado de la mesa debe ser mate y, a ser posible, de un color suave.
- La pantalla del ordenador debe situarse de forma perpendicular a las ventanas para evitar deslumbramientos y reflejos y que la luz natural incida en el espacio de trabajo de manera transversal.
- Para evitar destellos o deslumbramiento, la entrada de luz natural debe regularse utilizando cortinas, estores o persianas.
- Los caracteres de la pantalla deben ser fácilmente distinguibles, por lo que es necesario seleccionar un tamaño adecuado y ajustar el brillo y el contraste del monitor a las condiciones lumínicas de la estancia.
- Se descansará la vista periódicamente mirando hacia lugares alejados: el cambio de enfoque ayuda a relajar los músculos oculares.

Imagen 9. Foto de exceso de trabajo creado por wayhomestudio - www.freepik.es

4.4.2 Prevención de la fatiga física y mental

- Se recomienda establecer pausas de 5 o 10 minutos por cada hora de trabajo, que pueden dedicarse a realizar ejercicios para relajar la musculatura de la columna vertebral, de la espalda y de los brazos, así como los ejercicios de relajación de músculos oculares con los pertinentes cambios de enfoque visual.
- Una opción es ponerse en pie y realizar algunos movimientos rotatorios de cabeza, lentamente, y después levantar los brazos y doblar suavemente el tronco a izquierda y derecha.
- La relajación de los músculos oculares se realizará a través de cambiar el enfoque de visión, desde las posiciones próximas hacia las más lejanas que puedan alcanzarse.

WEBGRAFÍA

Dirección General de Trabajo y Bienestar Laboral. Consejería de Empleo, Formación y Trabajo Autónomo. Junta de Andalucía (2020). *Recomendaciones para teletrabajar de forma segura y saludable.* Recuperado de https://www.juntadeandalucia.es/export/drupaljda/guia-teletrabajo-cefta-covid19.pdf

Escuela Internacional de Criminalística y Criminología (2018). *¿Qué es el «Grooming»?* Recuperado de https://www.eicyc.es/que-es-grooming/

Informatix Servicios Informáticos (2021). *¿Cuáles son los tipos de virus informáticos más comunes?* Recuperado de https://informatix.es/los-tipos-de-virus-informaticos-mas-comunes/

Instituto Nacional de Tecnologías de la Comunicación - INTECO. *Guía de actuación contra el ciberacoso.* Recuperado de http://www.injuve.es/sites/default/files/Gu%C3%ADa%20de%20actuaci%C3%B3n%20contra%20el%20ciberacoso.pdf

ENLACES DE INTERÉS

Brigada Central de Investigación Tecnológica de la Policía Nacional: https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php

Grupo de Delitos Telemáticos de la Guardia Civil: https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

INTECO: http://www.inteco.es

Oficina de Seguridad del Internauta: http://www.osi.es

Pantallas Amigas: http://www.pantallasamigas.net