TRABAJANDO DESDE CASA

Ir a diapositiva siguiente

Módulo 3

Seguridad: laboral y física

En este tercer y último módulo, el foco será puesto sobre el autocuidado, para lo cual conoceremos los principales riesgos y cuidados informáticos a los cuales nos enfrentamos en el contexto de teletrabajo o trabajo a distancia. Además, pensando en nuestro lugar y hábitos de trabajo, identificaremos los riesgos ergonómicos y preocupaciones físicas que debemos tener al trabajar desde casa.

Ir a diapositiva anterior

Ir a diapositiva siguiente

Lección 1

Lección 2

Ir a diapositiva anterior

Lección 1

Navegación Segura

Ir a diapositiva anterior

Ir a diapositiva siguiente

Para acceder a internet, utilizamos programas llamados navegadores. Éstos nos permiten el ingreso fluido por Internet y ofrecen una serie de herramientas y funciones que facilitan la familiarización con la Web (o red).

Algunos de los navegadores más utilizados son Google Chrome, Safari, Opera, Internet Explorer y Mozilla Firefox.

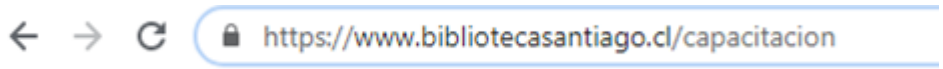
Ir a diapositiva anterior

Ir a diapositiva siguiente

Cuando gran parte de nuestro trabajo y/o de nuestra comunicación con otros, se realiza por medios electrónicos, desde varios dispositivos conectados a internet, debemos mantener un especial cuidado, para ello te dejamos aquí una serie de recomendaciones:

Por ejemplo: ¿Cómo comprobar si la navegación es segura?

Un antecedente que puede ayudarnos a saber si es una conexión segura o no, es HyperText Transfer Protocol Secre, es un Protocolo de comunicación de Internet que protege la integridad y la confidencialidad de los datos de los usuarios entre sus equipos y el sitio web. Para verificar esto, debemos fijarnos en la dirección de Internet que ponemos en el navegador, y que aparezca la figura del candado en su costado izquierdo:



Ir a diapositiva anterior

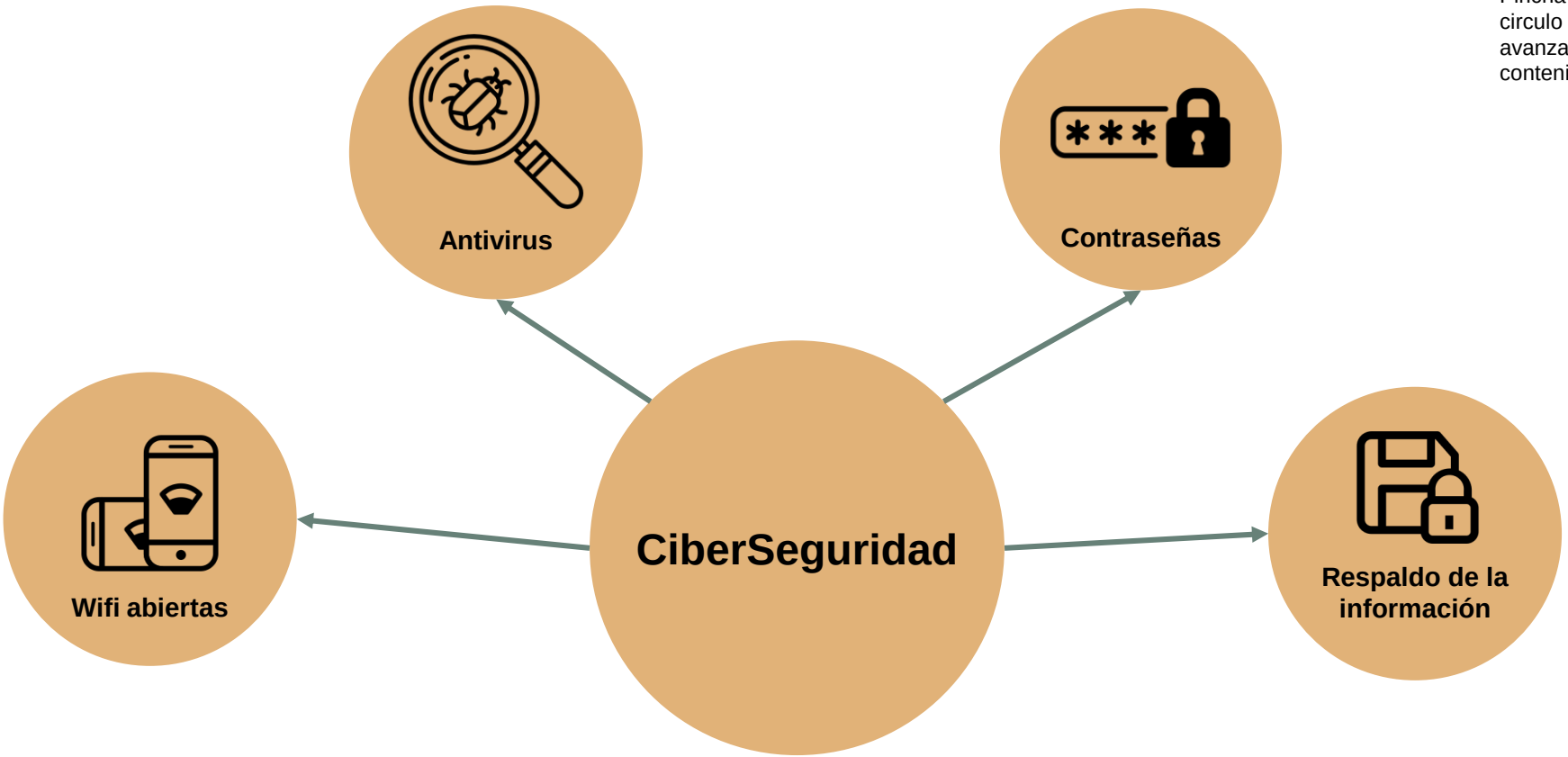
Ir a diapositiva siguiente

Con el símbolo de candado cerrado, el navegador confirma que es un sitio seguro. De todas maneras, aunque veas este símbolo, ten cuidado al compartir información personal, comprueba en la barra de direcciones que corresponda al sitio deseado.

Esto lo podemos revisar en la barra de direcciones: si es una red privada aparece al comienzo de la dirección https:// y no será privada cuando se vea así http:// (sin la letra ‘s’)

Te recomendamos no usar el sitio y/o no ingresar información personal o privada, si en el sitio que visitas te aparece un símbolo de advertencia, un mensaje de error o de acceso no seguro. Ya que puede poner en riesgo tu información o incluso tus dispositivos.

Pincha en cada circulo para avanzar en el contenido



Consejos de Ciberseguridad

Volver a Lección 1

Pincha en cada recuadro para avanzar en el contenido

Wifi Abiertas

¿Qué son las redes de Wifi abiertas?

¿Cuáles son los lugares donde habitualmente se encuentran disponibles?

¿Por qué es peligroso usar Wifi Abiertas?

¿Qué tipo de transacciones son más riesgosas realizar por este medio?

¿Principales amenazas que podrían afectar?

¿Cuál es la información que se podría exponer usando las redes de Wifi abiertas?

Ir a diapositiva Ciberseguridad

¿Qué son las redes de Wifi abiertas?

Las redes Wifi permiten conectar nuestro dispositivo tipo laptop, teléfono móvil e incluso tablet a una red de datos de forma inalámbrica. El término “wifi abiertas” quiere decir que son redes abiertas al público en general y, frecuentemente, ofrecen salida a internet de manera gratuita para la persona que se encuentra en ese recinto o lugar.

Ir a menú de preguntas Wifi

Ir a diapositiva siguiente

¿Cuáles son los lugares donde habitualmente se encuentran disponibles?

Las Wifi abiertas las podemos encontrar en hoteles, cafés, centros comerciales, aeropuertos, restaurantes, plazas y edificios con gran afluencia de público, incluso en estaciones de metro, bibliotecas y universidades entre otros.

Ir a menú de preguntas Wifi

Ir a diapositiva siguiente

¿Por qué es peligroso usar Wifi Abiertas?

Las Wifi abiertas son inherentemente inseguras. La mayoría de los dispositivos digitales como computadores y celulares, pueden estar en riesgo al conectarse debido a que estos lugares favorecen a cibercriminales para mezclarse entre la gente y utilizar los nombres identificadores de esas redes wifi para espiar a sus clientes.

Ir a menú de preguntas Wifi

Ir a diapositiva siguiente

¿Qué tipo de transacciones son más riesgosas realizar por este medio?

Se sugiere evitar los sitios web que para su uso requieren verificar la identidad del usuario. Esto se refiere a aquellos que utilizan sistemas de validación a través de un nombre de usuario y contraseña.

Ejemplo de estos sitios que requiere un usuario y contraseña son las redes sociales Facebook, Twitter, Instagram y casillas de correo electrónico. También es un riesgoso utilizar la banca en línea de tu institución financiera, y que por lo general utiliza datos como el RUT y una contraseña. También evita usarlas para realizar compras por internet donde tengas que ingresar los datos de tu tarjeta bancaria, así como otros servicios que puedan utilizar datos personales.

Ir a menú de preguntas Wifi

Ir a diapositiva siguiente

¿Principales amenazas que podrían afectar?

Principalmente el cibercriminal podría capturar los datos de usuario y contraseña para un servicio específico. Estos datos los puede utilizar para ingresar a esos servicios, obtener información adicional de cada uno de ellos, realizar accesos indebidos a la información personal del afectado e incluso eliminar datos relevantes

¿Cuál es la información que se podría exponer usando las redes de Wifi abiertas?

El cibercriminal, además de conocer las contraseñas de una persona, puede acceder a la información almacenada en sus correos electrónicos, conocer tu ubicación, saber que sitios Web visitas, fotografías y videos contenidos en redes sociales, y acceder a la banca en línea de una persona.

Ir a menú de preguntas Wifi

¿Qué son los programas Antivirus?

Los antivirus son programas informáticos, cuyo objetivo es detectar, controlar y eliminar virus del dispositivo en el cual esté activo. **Virus informático** serán aquellos programas que buscan alterar el funcionamiento normal del dispositivo, sin el permiso o conocimiento del usuario, principalmente para fines maliciosos sobre el dispositivo o sus programas.

Ir a diapositiva siguiente

¿Qué virus informáticos existen?

Existen muchos tipos de virus informáticos, revisemos algunos:

MALWARE

Un **malware** es un acrónimo del inglés malicious software, traducido al español como código malicioso. Es un programa informático cuya característica principal es que se ejecuta sin el conocimiento ni autorización del propietario o usuario del equipo infectado y realiza funciones en el sistema que son perjudiciales para el usuario y/o para el sistema; su fin es dañar o robar datos e información.

GUSANO

Un **gusano** informático es un malware que se replica para propagarse a otras computadoras. Este software malicioso suele utilizar una red informática para propagarse, aprovechando las fallas de seguridad en la computadora de destino para acceder a ella. Los gusanos casi siempre causan algún perjuicio a la red, aunque sea solo consumir ancho de banda.

Ir a diapositiva siguiente

SPYWARE

Un **spyware** o también denominado spybot, es un programa malicioso espía. Se trata de un malware, un tipo de software utilizado para recopilar información de un ordenador o dispositivo informático y transmitir la información a una entidad externa sin el permiso del dueño del ordenador o dispositivos móviles.

TROYANO

Un caballo de **Troya** o **troyano** es un tipo de malware que a menudo se disfraza de software legítimo. Es el más popular de los malware, diseñado para controlar de forma remota un computador. Los cibercriminales y hackers pueden utilizar troyanos para tratar de acceder a los sistemas de los usuarios, infiltrarse, dañar una computadora o el sistema de información, sin el consentimiento de su propietario.

Ir a diapositiva Ciberseguridad

Pincha en cada recuadro para avanzar en el contenido

Contraseñas

¿Cuándo una contraseña es segura?

¿Es posible usar contraseñas compartidas?

¿Existe algún método adicional de seguridad?

¿Es recomendable utilizar la misma contraseña en varios sistemas o sitios web?

¿Existe alguna aplicación que almacene mis contraseñas?

Ir a diapositiva Ciberseguridad

¿Cuándo una contraseña es segura?

Las contraseñas son un mecanismo de seguridad que permiten el acceso a un sistema exclusivamente a la persona que las conoce. Es segura cuando utiliza más de 8 o 10 caracteres, pero también debe incluir mayúsculas, minúsculas y caracteres especiales como la barra, coma, punto y coma, signo gato u otros símbolos. Hoy en día el paradigma de las contraseñas complejas ha cambiado ya que son muy difíciles de recordar. Por ello, se sugiere utilizar frases sencillas de tener presente como letras de canciones, poemas o similares, eso sí, siempre utilizando caracteres especiales alfa-numéricos.

Ir a diapositiva Contraseñas

¿Es posible usar contraseñas compartidas?

Es necesario considerar que la mayoría de las veces los sistemas y plataformas son de uso personal. Incluso algunas empresas establecen en sus contratos explícitamente la no divulgación de las contraseñas hacia terceros, por lo que entregar la contraseña podría constituir una falta.

Ir a diapositiva Contraseñas

¿Existe algún método adicional de seguridad?

Sí. Hoy en día la mayoría de los sistemas y sitios web utilizan el método de autentificación de doble factor. Esto quiere decir que además de la contraseña que conoce el usuario, el sistema envía un código de verificación hacía algún dispositivo del usuario, el que puede llegar a través de un mensaje de texto o correo electrónico, y dentro de un lapso de tiempo se debe ingresar el valor de verificación. En la actualidad los sistemas de verificación están utilizando biometría, como por ejemplo huella digital.

Ir a diapositiva Contraseñas

¿Es recomendable utilizar la misma contraseña en varios sistemas o sitios web?

No. Se recomienda utilizar una contraseña diferente en cada sitio Web y cambiarla frecuentemente, ya que, si alguno de ellos es vulnerado, los cibercriminales pueden intentar ocupar esas contraseñas en las redes sociales, banca en línea y/o correo electrónico de las personas, logrando acceder fácilmente a su información privada.

Ir a diapositiva Contraseñas

¿Existe alguna aplicación que almacene mis contraseñas?

Existen varias soluciones en el mercado que permiten guardar de forma segura las contraseñas de diferentes sistemas y sitios web. La ventaja principal es que esta información queda cifrada y protegida. Algunos navegadores web también guardan las contraseñas, pero no todos cifran la información, por lo que los datos podrían estar en peligro en caso de existir una vulnerabilidad, por tanto se recomienda no guardarlas en dicho caso. Estas aplicaciones se llaman “gestores de contraseñas”.

Pincha en cada recuadro para avanzar en el contenido

Respaldo de la Información

Ir a diapositiva Ciberseguridad

¿Qué riesgos tiene descargar archivos?

¿Todos los enlaces de descarga son maliciosos?

¿Qué puedo hacer si descargue archivos sospechosos?

¿Los teléfonos móviles también se infectan?

Generalmente recibo correos electrónicos de instituciones importantes, ¿Son confiables?

¿Qué recomiendan para descargar archivos confiables?

¿Qué riesgos tiene descargar archivos?

Una forma de entrada recurrente de virus a los dispositivos, es el envío de correos, mensajes de textos o incluso whatsapp maliciosos, disfrazados de promociones, de ayudas estatales, promesas de devoluciones de dinero o falsos avisos desde bancos, casas comerciales u otros.

Archivos provenientes de fuentes desconocidas **pueden contener virus o malware.** Esta es la llave de entrada para que cibercriminales ingresen al computador de una persona y puedan acceder a su información personal.

Ir a diapositiva Respaldo de la Información

Ir a diapositiva siguiente

¿Todos los enlaces de descarga son maliciosos?

No necesariamente. Sin embargo, hoy en día la mayoría de los organismos comerciales, financieros y públicos, no mantienen enlaces dentro de sus correos electrónicos, sino más bien son informativos e invitan a que el usuario visite directamente el sitio web.

Ir a diapositiva Respaldo de la Información

Ir a diapositiva siguiente

¿Qué puedo hacer si descargue archivos sospechosos?

Lo mejor es tener un antivirus actualizado y completo, u otro sistema de protección, el cual pueda prevenir estas descargas. Si la persona ya ha ejecutado el archivo y no generó el resultado esperado, se sugiere tomar contacto con un especialista que pueda analizar el computador en búsqueda de elementos maliciosos.

Ir a diapositiva Respaldo de la Información

Ir a diapositiva siguiente

¿Los teléfonos móviles también se infectan?

Efectivamente, los dispositivos móviles, como tablets y celulares, también pueden ser víctima de malware y lograr los mismos resultados que obtiene un cibercriminal al infectar un computador normal. Es más, puede acceder al historial de llamados, mensajes, correos electrónicos y mensajería instantánea.

Ir a diapositiva Respaldo de la Información

Ir a diapositiva siguiente

Generalmente recibo correos electrónicos de instituciones importantes, ¿Son confiables?

Lamentablemente inescrupulosos utilizan los procesos habituales de las organizaciones tales como declaración de impuestos, notificaciones judiciales y promociones (en el caso de retail), y mediante el engaño intentan conseguir que los receptores de esos correos electrónicos falsos descarguen archivos maliciosos. Esto se denomina comúnmente como Phishing, y consiste básicamente en que el cibercriminal envía de forma masiva, correos electrónicos que simulan provenir de una institución a espera que las personas caigan en el engaño.

Ir a diapositiva Respaldo de la Información

Ir a diapositiva siguiente

¿Qué recomiendan para descargar archivos confiables?

Utiliza elementos de seguridad para dispositivos como antivirus o, los más modernos, EDR Protección y Respuesta de Endpoints.

Visita directamente los sitios web de interés, preocupándose que cuenten con certificados de seguridad y no llegar a ellos a través de enlaces sospechosos.

Ir a diapositiva Ciberseguridad

Ir a diapositiva consejos

Consejos wifi

- Debemos ver estas redes con responsabilidad ya que los cibercriminales pueden utilizar esta tecnología inalámbrica para capturar datos importantes e información personal de usuarios descuidados.

Ir a diapositiva siguiente

Consejos wifi

- En ocasiones los delincuentes se aprovechan del nombre del recinto que se está visitando para crear redes wifi falsas. Por ello, si es muy necesario conectarse a internet, se sugiere preguntar al encargado del lugar sí disponen de wifi pública y cuáles son los datos de la conexión.

Ir a diapositiva siguiente

Consejos wifi

- Si estás usando sistema operativo Windows, indícale que te conectaras a una red pública, para mayor información contáctate con tu operador de servicio.

Ir a diapositiva siguiente

Consejos wifi

- Considera utilizar tu teléfono móvil (con plan de datos) para realizar transacciones que requieran el uso de datos sensibles, en vez de utilizar redes wifi públicas.

Ir a diapositiva siguiente

Consejos wifi

- Protege tus dispositivos, especialmente los móviles y computador con alguna solución anti-virus, manteniendo sus actualizaciones al día.

Ir a diapositiva siguiente

Consejos contraseñas

- No olvides proteger tus dispositivos móviles. Establece como primera medida de seguridad el bloqueo de tu móvil a través de una contraseña o con el lector biométrico de huella dactilar. Esta característica hace que sea mucho más difícil acceder a tu información personal en caso de robo o pérdida del dispositivo.

Ir a diapositiva siguiente

Consejos contraseñas

- Utiliza siempre contraseñas seguras, alfa-numérica.

Ir a diapositiva siguiente

Consejos contraseñas

- Evita repetir las contraseñas.

Ir a diapositiva siguiente

Consejos contraseñas

- No utilices datos predecibles, como fechas de nacimiento propias o familiares, dirección, etc.

Ir a diapositiva siguiente

Consejos contraseñas

- No compartas tus contraseñas con terceros.

Ir a Lección 2

Lección 2

Seguridad física, Ergonomía y otros temas de seguridad.

Ir a menú de lecciones

Ir a diapositiva siguiente

La actual emergencia sanitaria nos obligó a cambiar aspectos fundamentales de nuestras vidas como nuestro hábitos y relaciones de trabajo. En este contexto, nuestros hogares no han estado ajenos a esta serie de rápidas e imprevistas alteraciones, pasaron de ser el lugar de habitación al espacio donde también debemos desarrollar nuestras actividades laborales.

Como es esperable, las condiciones materiales con que nos encontramos no eran las ideales con los esperables efectos en nuestro cuerpo y en la calidad de nuestro trabajo.

Revisemos algunos temas, pensados en tu seguridad:

Ir a diapositiva siguiente

Pincha en cada circulo para avanzar en el contenido

Seguridad física

Condiciones ambientales

Estación de trabajo segura

Ley 16744

Ir a diapositiva anterior

Estación de trabajo segura

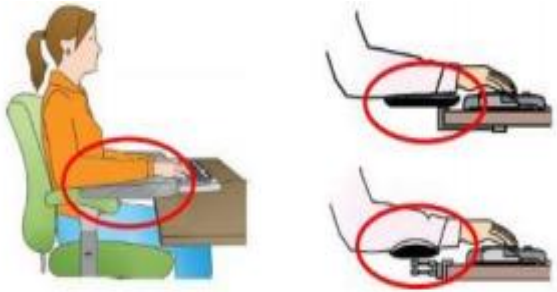
En este contexto existe una serie de recomendaciones para adaptar nuestras estaciones de trabajo de la mejor manera respetando los principios de la ergonomía.

Silla y escritorio: Como vimos anteriormente, muchas de las medidas que debemos tomar dentro de nuestros hogares se relacionan con adaptar las condiciones materiales ya existentes. En este sentido la recomendación es siempre trabajar en una mesa y silla, por ejemplo en los comedores de nuestras casas. En caso de contar con una silla de oficina y un escritorio especialmente destinados para fines laborales, se recomienda utilizarlos.

Ir a diapositiva siguiente

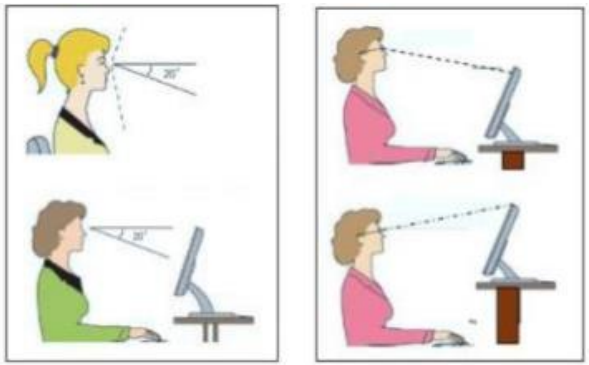
Estación de trabajo segura

Es necesario regular la silla para que los codos, en posición de relajo, puedan alcanzar el teclado sin que esto signifique un esfuerzo, tal como indica la ilustración:



Ir a diapositiva siguiente

Estación de trabajo segura



Como gran parte del teletrabajo lo realizaremos frente a un computador, este también debe ser parte de las medidas que tomemos pensando en un espacio de trabajo seguro.

El monitor debe estar siempre ubicado de frente, evitando posturas forzadas del cuello y espalda como las que ocurren cuando este se encuentra muy arriba o muy abajo. Debe quedar a un nivel ligeramente bajo la línea de los ojos, en un ángulo que varía entre 10° y 60° a una distancia cercana a los 50 cms, atendiendo siempre a las particularidades de cada persona.

Ir a diapositiva Seguridad Física

Condiciones Ambientales

A los factores materiales también debemos agregarle aquellos que son ambientales, principalmente los relacionados con iluminación y ruidos.
Si nuestro espacio de trabajo cuenta con una luz deficiente obligamos a nuestro sistema nervioso a realizar un esfuerzo adicional para poder trabajar en esas condiciones generando con esto una aceleración en la fatiga producida por la actividad laboral. Esto lo podemos experimentar cuando por ejemplo, intentamos leer con una luz que no es la ideal. Por otra parte, se produce un esfuerzo muscular mayor pues debemos adoptar posturas corporales que nos ayuden a compensar esta falta de luz.

Ir a diapositiva siguiente

Condiciones Ambientales

Dentro de los factores ambientales que afectan la calidad de nuestro trabajo se encuentra los ruidos que pueden llegar a constituir desde una molestia hasta un riesgo de daño auditivo, dependiendo del contexto de trabajo.

Como es evidente, en nuestros hogares no podemos hacer un control tan estricto respecto a los niveles de ruido ambiental, sin embargo, podemos tomar medidas tendientes a regular nuestra exposición a ellos. Por ejemplo, evitar que nuestro lugar de trabajo esté cerca de fuentes de emisión constantes de sonido como una televisión. El caso de la música ofrece atenuantes pues a niveles moderados puede incluso contribuir a nuestra concentración y creación de un ambiente más grato.

Ir a diapositiva Seguridad Física

Ley 16.744 en contexto de teletrabajo

En nuestro país, la Ley 16.744 es aquella que establece normas sobre accidentes de trabajo y enfermedades profesionales. Promulgada en 1968 bajo el gobierno de Eduardo Frei Montalva es reconocida como uno de los pilares del sistema de seguridad social en Chile. En ella, se declara obligatorio la existencia de un seguro para todos los y las trabajadoras que sufran accidentes y enfermedades consideradas laborales. Establece una serie de normativas que deben ser cumplidas por las instituciones y personas empleadoras, orientadas a la protección de la salud física y mental de trabajadores y estudiantes.

Ir a diapositiva siguiente

Ley 16744 en contexto de teletrabajo

Esta ley protege a trabajadores y trabajadoras, tanto del sector público como del privado, incluyendo aquellos que son independientes y cotizan previsionalmente. Ellas y ellos tienen derecho a tener acceso a “actividades preventivas que realizan los Organismos Administradores en las empresas adheridas o afiliadas”como capacitaciones o asistencia técnica cuando ésta sea considerada necesaria. Quizás la parte más conocida de esta ley es aquella que otorga a derecho a prestaciones médicas una vez ocurrido un accidente laboral.

Ir a diapositiva siguiente

Ley 16.744 en contexto de teletrabajo

Todo el detalle de la Ley 16.744, puedes revisarlo pinchando aquí

¿Qué ocurre con la Ley 16.744 en contexto de teletrabajo? Como nuestro lugar de trabajo y habitación pueden ser el mismo, es necesario distinguir entre aquellos accidentes laborales, como los anteriormente descritos y los domésticos. Estos últimos se producen en la vivienda mientras se desarrollan actividades propias del hogar y no a causa o con ocasión del trabajo. Así por ejemplo aquellos siniestros ocurridos en labores de limpieza, cocina o reparación de nuestro hogar no quedan bajo el amparo de la ley 16.744.

Finalmente es de vital importancia tener claro que el teletrabajo no exime a los empleadores de su obligación de adoptar todas las medidas de higiene y seguridad necesarias para proteger la vida y salud de trabajadores y trabajadoras.

Mapa de navegación Módulo 2:
“Herramientas de trabajo online”

Lección 1

Navegación Segura

Ciberseguridad

Wifi abiertas

Contraseñas

Antivirus

Respaldo de la Información

Consejos de Ciberseguridad

Lección 2

Seguridad Física, Ergonomía y otros temas

Seguridad Física

Estación de Trabajo Segura

Condiciones ambientales

Ley 16.744