

## **ACTIVIDAD 1**

- **RIESGO CONDICIONES SEGURIDAD**

**-Lugares de trabajo:** "Como el edificio está en obras es raro el día que no da un traspíe en los estrechos escalones que comunican con el sótano donde guardan el material". "Además la luz del pasillo es insuficiente y alguna vez ha tropezado con las cajas que se amontonan allí por todas partes".

- Daño: caídas a distinto nivel de personas.

**-Máquinas y equipos de trabajo: El orden y la limpieza:** "Uno de los oficiales tiene la mala costumbre de no guardar las herramientas que utiliza en la caja correspondiente, y casi siempre están todas esparcidas por el suelo durante toda la jornada"

- Daño: Choques con objetos móviles

**-Riesgos eléctricos:** "un trabajador sufriera una quemadura por contacto eléctrico"

-Daño: Quemaduras, pueden producir contracciones musculares dificultando la respiración, paradas del corazón.

- **RIESGOS AMBIENTALES**

**-Contaminantes / agentes físicos: Ruido:** "el ruido del tráfico es constante en esa zona y se oye en todo el edificio. Esto, unido al ruido que produce la maquinaria, hace que prácticamente haya que gritar para hacerse entender"

- Daño: Contracciones musculares, aumento de presión sanguínea, problemas cardiovasculares.

**-Contaminantes / agentes físicos: Temperatura:** "las trabajadoras y trabajadores están expuestos a frecuentes corrientes de aire"

- Daño: Enfriamiento, hipotermia, posibilidad de contraer enfermedades víricas respiratorias.

- **RIESGOS ERGONOMICOS**

**-Riesgo derivado de posturas indeseables y cuya prolongación provoca**

**fatiga. Posicion de pie:** "Durante la mayor parte de la jornada está de pie y en muchas ocasiones tiene que adoptar posturas muy incómodas por lo que al final de la jornada"

-Daño: dolor de pies, hinchazón de piernas, venas varicosas, fatiga muscular general, dolor en la parte baja de la espalda, rigidez de cuello y hombros entre otros.

- **Riesgos Psicosociales:**

**-Organización de la actividad: jornada laboral:** "Al finalizar la jornada, recogen las herramientas que están en el suelo y las colocan en sus respectivas cajas, entre recoger las herramientas y cambiarse de ropa

acaba saliendo a las 18.30 o 19.00 horas, aunque su jornada acaba a las 18.00 horas"

**-Organización de la actividad: un clima de comunicación adecuado, un estilo de mando democrático:** "Su jefe se muestra especialmente exigente con él" "desde que ascendió a jefe de instalaciones eléctricas no parece confiar en su capacidad y constantemente pone en tela de juicio sus decisiones y su trabajo. En una ocasión llegó incluso a amonestarlo verbalmente por tener iniciativas sin consultarlas antes con la dirección"

**- La organización de la actividad: la organización de la empresa:** "la sobrecarga de trabajo que tiene, ya que debe desarrollar un determinado volumen de trabajo para cobrar el plus de productividad"

-Daños: insatisfacción laboral, estrés, mobbing, ansiedad, irritabilidad, falta de sueño que pueden derivar en depresión.

## ACTIVIDAD 2 punto 1.-

### NUEVOS DELITOS INFORMÁTICOS

De la nueva cultura TIC se han generado los "delitos Informáticos".  
Por ello el ordenamiento jurídico se ha debido adecuar con la **reforma del Código Penal, tras la ley Orgánica 1/2005 de 30 de Marzo.**

Impulsada por la normativa europea "Decisión Marco 2005/222" del consejo de 24 de Febrero  
Posteriormente sustituida por la Directiva 2013/40 UE del Parlamento Europeo de 12 de Agosto.

#### 1. DELITO DE INTRUSIÓN INFORMÁTICA (ARTÍCULO 197 BIS APARTADO PRIMERO)

"el que por cualquier medio o procedimiento vulnerando las medidas de seguridad establecidas para impedirlo y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años".

#### 2. INTERCEPTACIÓN DE TRANSMISIONES DE DATOS INFORMÁTICOS (ARTÍCULO 197 BIS APARTADO SEGUNDO)

"el que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses".

El **artículo 197 ter** castiga las conductas relacionadas con la producción o facilitación a terceros de instrumentos para la realización de los delitos previsto en los dos apartados primeros del artículo 197.

#### 3. DELITOS INFORMÁTICOS RELACIONADOS CON LA PROPIEDAD INTELECTUAL E INDUSTRIAL ARTÍCULOS 270 Y SS CP

Se castiga no sólo la reproducción, el plagio, la distribución, la comunicación pública o cualesquiera otras prácticas de obras literarias, artísticas o científicas, sin la autorización de los titulares de tales derechos, sino también la facilitación del acceso a esos contenidos mediante links o enlaces de descarga con fines lucrativos, así como la fabricación, distribución, producción, importación, almacenamiento, ofrecimiento, comercialización y cualesquiera otras prácticas similares de productos que incorporen algún signo distintivo idéntico al original.

#### 4. OTRO TIPO DE DELITOS INFORMÁTICOS

- Amenazas (artículo 169 y ss del CP) realizadas o difundidas a través de cualquier medio de comunicación.
- Calumnias e injurias (artículo 205 y ss CP) realizadas o difundidas a través de cualquier medio de comunicación.
- Fraudes informáticos (artículo 248 del CP)
- Sabotaje informático (artículo 263 del CP).
- Inducción a la prostitución de menores (artículo 187).
- producción, venta, distribución, exhibición o posesión de material pornográfico en cuya elaboración hayan intervenido o sido utilizados menores de edad o incapaces (artículo 189 CP).
- Posesión de software informático destinado a cometer delitos de falsedad

## **ACTIVIDAD 2 punto 2.-**

- Actualizar regularmente sus sistema para solucionar posibles fallos que pueden aprovechar los delincuentes.
- Actualizar antivirus y actualizarlo con frecuencia.
- Instalar un firewall para restringir accesos no autorizados de internet.
- Instalar software anti-spyware para evitar que se introduzcan en el equipo programas espías que recopilan información confidencial del usuario.
- Utilizar contraseñas seguras y modificarlas con frecuencia.
- Navegar por webs seguras y de confianza identificando sellos o certificados digitales o que empiecen por "https://" no "http://".
- Tener cuidado al utilizar programas de acceso remoto. Por ejemplo cambiando el puerto de escucha por defecto "389".
- Tomar precauciones en la utilización del correo electrónico:
  - No abrir correos de remitentes desconocidos.
  - Desconfiar de e-mails que solicitan contraseñas, información confidencial...
  - No propagar mensajes de contenido dudoso que piden ser reenviados a todos los contactos.
  - Utilizar software anti-spam que protege la cuenta de correos no deseados.

## **ACTIVIDAD 3 punto 1.-**

### **Empresa1**

#### **MELCHOR MASCARÓ**

Empresa dedicada a obra civil y servicios (mantenimientos, limpieza viaria, jardinería....)

Dispone de un servicio de prevención mancomunado de 7 técnicos

Tiene 122 mandos intermedios con formación de nivel básico de PRL (60H)

#### **Buenas prácticas:**

- Sistema OHSAS 18001 (2005) de gestión ética.
- Grupo de estudio para la mejora de la calidad técnica de los planes de seguridad y salud.
- Se adoptan medidas que favorezcan la asistencia de los trabajadores al reconocimiento médico.
- Tienen equipos de medición propios para la evaluación de riesgos.
- Celebran la Semana Europea de la Seguridad y Salud en el Trabajo desde 2004.
- Se realizan encuestas de clima laboral.
- Se ha ofrecido formación en dirección de equipos de trabajo.
- Dispone de un sistema informático para el control de las obligaciones de subcontratistas y autónomos.
- Se ha implantado una tarjeta identificativa para el personal para asegurar el cumplimiento de sus obligaciones en PRL.

- El Servicio de Prevención Propio ha evolucionado ha departamento de gestión integral.
- Hay una coordinación constante entre el departamento de compras, el departamento de estudios y contratación y el departamento de recursos humanos.
- Cuentan con una línea gráfica de cartelería con la creación del personaje Segurito Prevencio.
- Tienen una revista "De tu a tu" que fomenta la implicación y la sensibilización de todos los trabajadores con la seguridad y salud laboral.
- Han elaborado un procedimiento específico de evaluación de la maquinaria.
- En el manual de bienvenida se potencia la información gráfica para cubrir las necesidades de los inmigrantes.
- Tienen una línea creciente de inversión directa en el departamento de seguridad y salud.

## **Empresa 2**

### ETEL

Empresa de 66 trabajadores dedicada a instalaciones eléctricas, domótica, sistemas contra incendios, telecomunicaciones, fontanería y climatización.

#### Buenas prácticas:

- Tiene un sistema de gestión integral de prevención, calidad y medioambiente con los siguientes procedimientos:

Identificación y evaluación de requisitos legales y otros

- Evaluación de riesgos laborales
- Planificación de la actividad preventiva
- Objetivos preventivos
- Integración de la PRL
- Formación
- Gestión de No Conformidades
- Adquisición de equipos de trabajo y productos
- Gestión de EPIS
- Información a los trabajadores
- Comunicación de riesgos detectados
- Actuación ante emergencias
- Actuación ante riesgo grave e inminente
- Coordinación de actividades empresariales
- Permiso para trabajos especiales
- Comunicación, gestión e investigación de A.T.
- Consulta y participación de los trabajadores
- Cuenta con un técnico superior en PRL.
- Coordinación entre el departamento de seguridad y salud y el de recursos humanos.
- Han desarrollado un procedimiento específico de evaluación de maquinaria.

