BOLETIN INFORMATIVO

20-noviembre-2020

Nº 15/2020

Servicios de Prevención Ajenos
ASPA-ANEPA

losa MED

SERLOMED

CHARTER DIVERSIDAD 2019 2021

Gracias, a todos los profesionales de Seguridad y Salud en el Trabajo.

ASPA-ANEPA. 25 aniversario de la Ley de Preveción de Riesgos Laborales.

Guía práctica. Protocolo de reincorporación de trabajadores/as tras una baja prolongada. ASPA-ANEPA-IRSST.

Las organizaciones empresariales ASPA-ANEPA dentro del marco de colaboración que mantenemos con el Instituto Regional de Seguridad y Salud en el Trabajo de la Comunidad de Madrid, hemos desarrollado una " **Guía de aplicación del Protocolo de reincorporación del puesto de trabajo tras una baja de larga duración "** , que servirá de herramienta para el seguimiento, valoración y adaptación de estos trabajadores a su puesto de trabajo. Al final de la misma se encuentran los anexos correspondientes y el procedimiento abreviado.

El objetivo con este proyecto es ofrecer a los Servicios de Prevención una herramienta estandarizada que garantice una gestión preventiva adecuada ante la reincorporación de trabajadores de larga duración en las empresas clientes.

Descargar Guía.

SPAjenos.

El Tribunal de Cuentas apunta a la Seguridad Social por especulación en la venta de servicios de las mutuas.

Según la publicación de Europapress del pasado 16 de noviembre, varias sociedades se vendieron a directivos de las mismas mutuas y algunas fueron revendidas meses después multiplicándose el precio.

El Tribunal de Cuentas ha detectado falta de control y especulación en el proceso de privatización de los servicios de prevención de las mutuas colaboradoras de la

Seguridad Social, apuntando a la responsabilidad de la Dirección General de Ordenación de la Seguridad Social como encargada de supervisar el proceso .

Leer noticia completa

Informe anual de accidentes de trabajo en España 2019

El Instituto Nacional de Seguridad y Salud en el Trabajo acaba de publicar el informe anual con los resultados generales de accidentes de trabajo. Este año incluye una novedad importante, debido a que en el año 2019 se han incorporado más de 2,5 millones de trabajadores autónomos en la población de referencia de esta estadística

como consecuencia de que, a partir de 1 de enero de 2019, la cobertura específica de accidentes de trabajo por la Seguridad Social para los afiliados al Régimen Especial de Trabajadores Autónomos (RETA) pasó a ser obligatoria con carácter general.

De esta forma se igualan los derechos y obligaciones de los trabajadores por cuenta propia con el resto de población laboral y, además, se espera que contribuya a un conocimiento mejor de su siniestralidad.

Esta circunstancia ha llevado a un conocimiento más exacto de la siniestralidad en los trabajadores por cuenta propia, ya que las contingencias profesionales ocurridas quedan reflejadas en los sistemas de notificación y registro correspondientes. Por este, los datos totales en valor absoluto motivo e índices de incidencia del año 2019 no son comparables con los datos reflejados en los informes anteriores.

En el presente informe se analizarán por separado los accidentes de trabajo de los trabajadores asalariados y los trabajadores por cuenta propia.

En España, durante el año 2019, se registraron 650.602 accidentes de trabajo con baja. La mayoría se produjeron durante la jornada laboral, en concreto 562.756 accidentes, que suponen el 86,5%.El resto, 87.846 accidentes, tuvieron lugar durante el trayecto del domicilio al centro de trabajo o viceversa; son los que se denominan accidentes de trabajo con baja en itínere.

Del total de los accidentes de trabajo con baja, 529.421 los sufrieron trabajadores asalariados, que suponen el 94,1% de estos accidentes. Los trabajadores por cuenta propia sumaron 33.335 accidentes con baja en jornada de trabajo, y representan el 5,9% de los mismos.

Descargar informe

Jornada AESAE-CEOE "Problemática alrededor del nuevo trabajo a distancia".

El trabajo a distancia, por vía telemática o teletrabajo, se ha convertido a lo largo de este año 2020 en una forma de trabajo habitual, tanto en España como en la mayoría de los países del mundo, debido a la pandemia que vivimos.

Las cifras de la implantación de esta modalidad de trabajo en nuestro país, son cada vez mayores, habiéndose aprobado, recientemente, la nueva normativa que regulará el Teletrabajo, lo que en el contexto actual obliga a considerar la problemática que todo ello conlleva.

Programa

Tecnología

Principal tendencia de ciberseguridad para 2021

Check Point Softwre Techolologies Ltd., proveedor global de soluciones de seguridad de TI, ha anunciado sus previsiones en materia de ciberseguridad de cara al 2021, así hacer como los principales retos de seguridad a los que las empresas tendrán que frente durante el próximo año.

Durante el 2021 os efectos de los cambios introducidos durante la pandemia del COVID-19 continuarán siendo un punto clave para los equipos TI y de seguridad. De hecho, el 81% de las empresas han adoptado el teletrabajo, mientras que un 74%

planea que se establezca de forma permanente.

Por otra parte, la compañía apunta a las nuevas generaciones de amenazas ransomware y de botnets, así como de los retos de securizar las nuevas redes 5G y el consecuente aumento de dispositivos conectados como los principales peligros para las empresas.

“La pandemia ha supuesto un cambio radical para todas las empresas que se han visto obligados a dejar de lado sus planos estratégicos y comerciales para centrarse en proporcionar a sus empleados una conectividad en remoto rápido, seguro y escalable. Ante esta situación, los equipos de seguridad han tenido que hacer frente a un creciente número de amenazas en la migración a la nube, puesto que los ciberdelincuentesbuscaban sacar provecho de esta situación.De hecho, según datos de nuestra encuesta, el 71% de los profesionales de la seguridad informaron de un aumento de las ciberamenzas desde que comenzó el confinamiento "indica su Vicepresidenta, Doris Dor. " Una de las pocas cosas predecibles en ciberseguridad es que los delincuentessiempre están al acecho de nuevas oportunidades o grandes acontecimientos, como puede ser la crisis del COVID-19 o la llegada del 5G, para sacar provecho. Por este motivo, aconsejamos a las empresas adoptar seguridad proactiva y no dejar ningún punto desprotegido, puesto que de lo contrario se arriesgan a Convertirse en la Próxima Víctima” Las Tendencias en materia de ciberseguridad se dividen en tres Grandes **bloques** : **Amenazas relacionadas con la pandemia**

- **Proteger la “nueva normalidad”:** el COVID-19 seguirá muy presente en el 2021, aunque su impacto variará según el avance el año. Sin embargo, las empresas necesitarán seguir estando preparadas para una serie de 'próximos normales', para lo que proteger las redes, los entornos cloud, las aplicaciones y la información es crucial. Para ello, es clave reforzar la amenaza de amenazas en toda la red con el objetivo de evitar que los ataques avanzados se extiendan rápidamente por las infraestructuras corporativas y aprovechen las debilidades de seguridad. La automatización de la prevención será crítica, ya que el 78% de las empresas declara adolecer de conocimientos y recursos en estas áreas.
- **Sin cura para las amenazas relacionadas con la pandemia:** las noticias

sobre el desarrollo de vacunas, nuevas restricciones de movilidad, etc. seguirán copando los titulares de los medios y serán los ganchos que utilicen los ciberdelincuentes para lanzar campañas masivas de phishing. Asimismo, las compañías farmacéuticas involucradas en el desarrollo de vacunas se mantendrán como uno de los principales objetivos de los ataques por parte de cibercriminales o incluso grupos maliciosos relacionados con determinados países.

- **La formación a distancia, en el punto de mira:** al igual que las empresas, el sistema educativo ha tenido que migrar para poder continuar trabajando a distancia mediante el uso de plataformas online. Como consecuencia, este sector ha experimentado un aumento del 30% de ataques semanales durante el mes de agosto, coincidiendo con el periodo anterior al inicio del curso y seguiremos viendo altos niveles de riesgo durante los próximos 12 meses.

Malware, privacidad y ciberguerra

- **El ransomware de doble extorsión impulsa el auge de esta amenaza:** durante el tercer trimestre del año se ha producido un aumento en el uso de este tipo de virus. Cuando lanzan este tipo de ataques, los cibercriminales primero extraen grandes cantidades de datos sensibles antes de cifrar el equipo infectado. Tras esto, amenazan a su víctima con publicar esta información a no ser que se pague el rescate. Para demostrar que su amenaza es veraz, publican una pequeña cantidad de datos en la dark web, aumentando así el nivel de presión.
- **El ejército de botnets continuará creciendo:** los ciberdelincuentes están apostando por convertir muchas familias de malware en botnets con el objetivo de crear una red que permita lanzar ataques de forma masiva. Emotet, que el el malware más utilizado en 2020, comenzó como un troyano bancario, pero ha evolucionado hasta convertirse en una de las botnets más persistentes y versátiles, capaz de lanzar exploits dañinos, from ransomware hasta robo de datos.
- **Ciberataques entre países, el nuevo campo de batalla:** los ataques informáticos entre países en entornos virtuales, ya sea para espiar o para influir en determinados acontecimientos, seguirán al alza. De hecho, según datos de Microsoft, grupos de cibercriminales de 3 nacionalidades copan el 89% del total de hackeos entre estados durante todo el año pasado. En los

últimos años, la atención se ha centrado en la seguridad de infraestructuras críticas, aunque cada vez diversifican más y atacan a otros sectores como el sanitario o diversos departamentos gubernamentales, tal y como se pudo comprobar con la campaña Vicious Panda contra Mongolia que Check Point descubrió en marzo.

- **Utilizar deepfakes como arma:** las técnicas digitales para falsificar vídeo o audios están lo suficientemente avanzados como para convertirse en armas y utilizarlas para crear contenido malicioso destinado a influir sobre la opinión pública o sobreprecios de acciones de empresas, por poner sólo dos ejemplos. A principios de año, un grupo político belga difundió un video falso del Primer Ministro de Bélgica en el que se habla sobre el efecto medioambiental del COVID-19 y hacía un llamamiento a actuar contra el cambio climático.
- **Sin noticias de la privacidad:** los dispositivos móviles contienen una gran cantidad de información personal que está en aplicaciones que piden permiso de acceso a los contactos, mensajes y otros servicios. Un paso más allá, las aplicaciones de rastreo de contactos COVID-19 tienen problemas de privacidad de las personas. Y esto no ocurre sólo en / con aplicaciones legítimas: el adware movil para robar credenciales bancarias de los usuarios es una importante amenaza al alza.

5G y plataformas IoT

- **Beneficios y retos de 5G:** la llegada de la nueva generación de redes de telecomunicaciones trae consigo un nuevo entorno de alta velocidad e hiperconectividad, pero, por el contrario, supone también la oportunidad para lanzar ataques con el objetivo de bloquear las conexiones entre dispositivos . Los equipos con funciones de bienestar recogerán información sobre el usuario (ritmo cardiaco, etc.), los coches incluirán funciones para controlar el movimiento de otros vehículos o peatones y las ciudades inteligentes podrán recabar información sobre los hábitos de sus ciudadanos. Este volumen de datos tan masivo necesita altos niveles de seguridad para evitar robos o filtraciones
- **IoT (Interet of Threats):** las siglas IoT, además de Internet de las Cosas (en su traducción al castellano), también hacen referencia a las amenazas que nos podemos encontrar en el mundo virtual. A medida que se implantan las redes 5G, el número de dispositivos interconectados crece

exponencialmente, aumenta así los riesgos de vulnerabilidad frente a ciberataques multivectoriales a gran escala. Los equipos IoT y los entornos cloud se mantienen como un eslabón débil en ciberseguridad, puesto que es difícil obtener una visibilidad completa de estos elementos.

Durante el próximo año el escenario de ciberriesgos pre-pandemia continuará, puesto que las empresas siguen enfrentándose al mismo tipo de amenazas, como el phishing o el ransomware, que ha crecido un 50% en los últimos tiempos. Sin embargo, las compañías tienen ante sí un nuevo reto: securizar las infraestructuras y el acceso remoto a su información. Estamos atravesando un cambio de paradigma, y la llegada de nuevas tecnologías como el 5G suponen un esfuerzo adicional para las empresas debido a la hiperconectividad que potencia este tipo de redes. Por tanto, la ciberseguridad de los endpoints y estructuras corporativas será capital de cara al próximo año, un reto mayúsculo si se tiene en cuenta que el 40% de las empresas no cuenta con seguridad básica.

Cepymenews

Jurisprudencia

Los representantes de los trabajadores conservan la preferencia a quedarse en la empresa también en los ERTES por Covid-19

El Tribunal Superior de Justicia de Madrid ha emitido una sentencia en la que declara que el derecho preferenciante a quedarse en la empresa reconocido a los miembros del Comité de Empresa por el artículo 51.5 del Estatuto de los Trabajadores para determinados supuestos de despido colectivo debe entenderse que es aplicable también en el caso de los ERTEs por fuerza mayor que se han tramitado como consecuencia de la emergencia sanitaria de la Covid-19.

La empresa recurrió la sentencia en suplicación, y sostuvo que en la normativa reguladora de los ERTEs específicamente aprobada durante la pandemia, en concreto el Real Decreto-ley 8/2020, de 17 de marzo, de medidas urgentes extraordinarias para hacer frente al impacto económico y social del COVID-19, no se menciona la existencia de ese derecho de permanencia, por lo que no existe la prohibición de incluir a los representantes legales de los trabajadores en la lista de personas afectadas por un ERTE.

Sin embargo, el Tribunal Superior de Justicia de Madrid ha acabado por confirmar la sentencia de instancia, fundamentando su fallo en que la prerrogativa de permanencia que el Estatuto de los Trabajadores reconoce a los miembros del Comité de Empresa constituye un derecho fundamental, el derecho a la libertad sindical, y por tanto no puede entenderse que, por simple omisión o silencio, ese derecho puede ser eliminado por una norma que regula una situación específica ligada a una emergencia sanitaria.

Dice la sentencia que, dado que la norma que regula las suspensiones colectivas de contratos por fuerza mayor -es decir el art. 47.3 del Estatuto de los Trabajadores- contiene una remisión expresa, en cuanto a la tramitación del procedimiento, al art.51.7 de dicho Estatuto (sobre despidos colectivos), resulta que el derecho preferencial contemplado en el apartado 5 de ese mismo artículo es de aplicación también a las suspensiones.

Fuente: CEPYME

Descargar sentencia completa

DOCUMENTOS DE INTERÉS

- Real Decreto-ley 34/2020, de 17 de noviembre, de medidas urgentes de apoyo a la solvencia empresarial y al sector energético, y en materia tributaria.

- Evaluación del riesgo de transmisión de SARS-CoV-2 mediante aerosoles. Medidas de prevención y recomendaciones. Ministerio de Sanidad. 18/11/2020

- Estadística de Accidentes de Trabajo, avance enero-septiembre'20. Ministerio de Trabajo y Economía Social.

- Guía Práctica. Protocolo de reincorporación de trabajadores / as tras una baja prolongada

- Estrategia de detección precoz, vigilancia y control de Covid-1-

Actualización 12.11.20

Servicios de Prevención Ajenos
ASPA-ANEPA

03.11.20 - Subgrupo “Análisis de la Legislación en PRL” CEOE.

06.11.20 - Mesa Negociadora del III Convenio Colectivo nacional de los SPA.

11.11.20 - Junta Directiva de la Federación ASPA.

11.11.20 - GT Seguridad Vial Laboral de la CNSST.

12.11.20 - Mesa negociadora del III Convenio Colectivo de los SPA.

13.11.20 - Comisión de Sanidad y Asuntos Sociales CEOE.

13.11.20 - GT Plataformas Digitales. CEOE.

16.11.20 - Comisiones de Unión Europea y Sociedad digital CEOE.

16.11.20 - Dirección General de Salud Pública de la Comunidad de Madrid.
17.11.20 - Comisión de Responsabilidad Social Empresarial CEOE.
19.11.20 - Comisión Paritaria de Formación de los SPA.
19.11.20 - Patronato de la Fundación Estatal para la PRL.
20.11.20 - Reunión Mesa Negociadora del Convenio Colectivo de los SPA.
26.11.20 - Grupo de Trabajo ANEPA-ASPA Teletrabajo.
30.11.20 - Comisión de Desarrollo Sostenible y Medio Ambiente CEOE.
02.12.20 - Comisión Unión Europea CEOE

Sumario de #MICRONEWS

04.11.20 - ERGA on-line de julio a septiembre'20 del INSST.
05.11.2020 - Observatorio del Mercado Laboral nov'20. CEOE
06.11.20 - Boletín informativo nº 14/2020
11.11.20 - Campaña test de antígenos Serlomed.
12.11.20 - Webinar AESAE-CEOE "Problemática alrededor del nuevo trabajo a distancia".
13.11.20 - Actualización 12 de noviembre 2020 del documento “Estrategia de Detección Precoz, Vigilancia y Control de Covid-19”.
13.11.20 - Guía práctica. Protocolo de reincorporación de trabajadores / as tras una baja prolongada.
16.11.20 - Estadística de Accidentes de Trabajo, avance enero-septiembre'20. Ministerio de Trabajo y Economía Social.
17.11.20 - Europapress*: El Tribunal de Cuentas apunta a la Seguridad Social por especulación en la venta de servicios de las mutuas.*

19.11.20 - Documento técnico Evaluación del riesgo de la transmisión de SARS-CoV-2 mediante aerosoles. Medidas de prevención y recomendaciones. Ministerio Sanidad 18.11.20.

19.11.20 - Informe Panorama económico noviembre'2020. CEOE.

20.11.20 - Informe del Mercado Laboral y Negociación Colectiva nov'20. CEOE