INSTITUTO NACIONAL DE CIBERSEGURIDAD

Ciberseguridad

Teletrabajo Seguro

Marco A. Lozano Merino

Responsable de Servicios de Ciberseguridad para Empresas

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

017 TU AYUDA EN CIBERSEGURIDAD incibe_

INCIBE

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

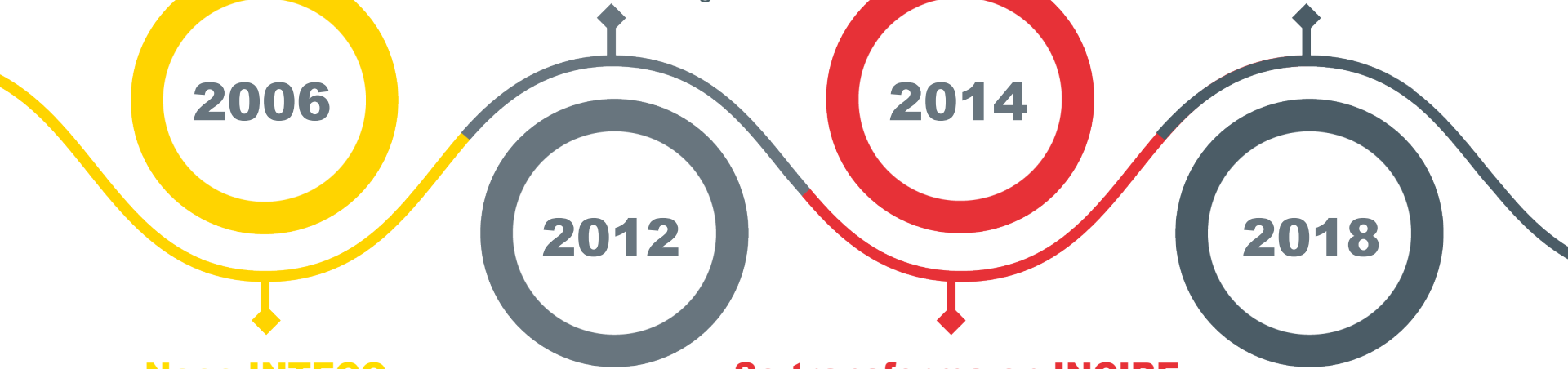
Secretaría de Estado de Digitalización e Inteligencia Artificial

Entidad de referencia en **ciberseguridad**

Ciudadanos

Empresas y profesionales

INCIBE



Nace INTECO

Instituto Nacional de Tecnologías de la Comunicación

INTECO

Se focaliza en el mundo de la ciberseguridad

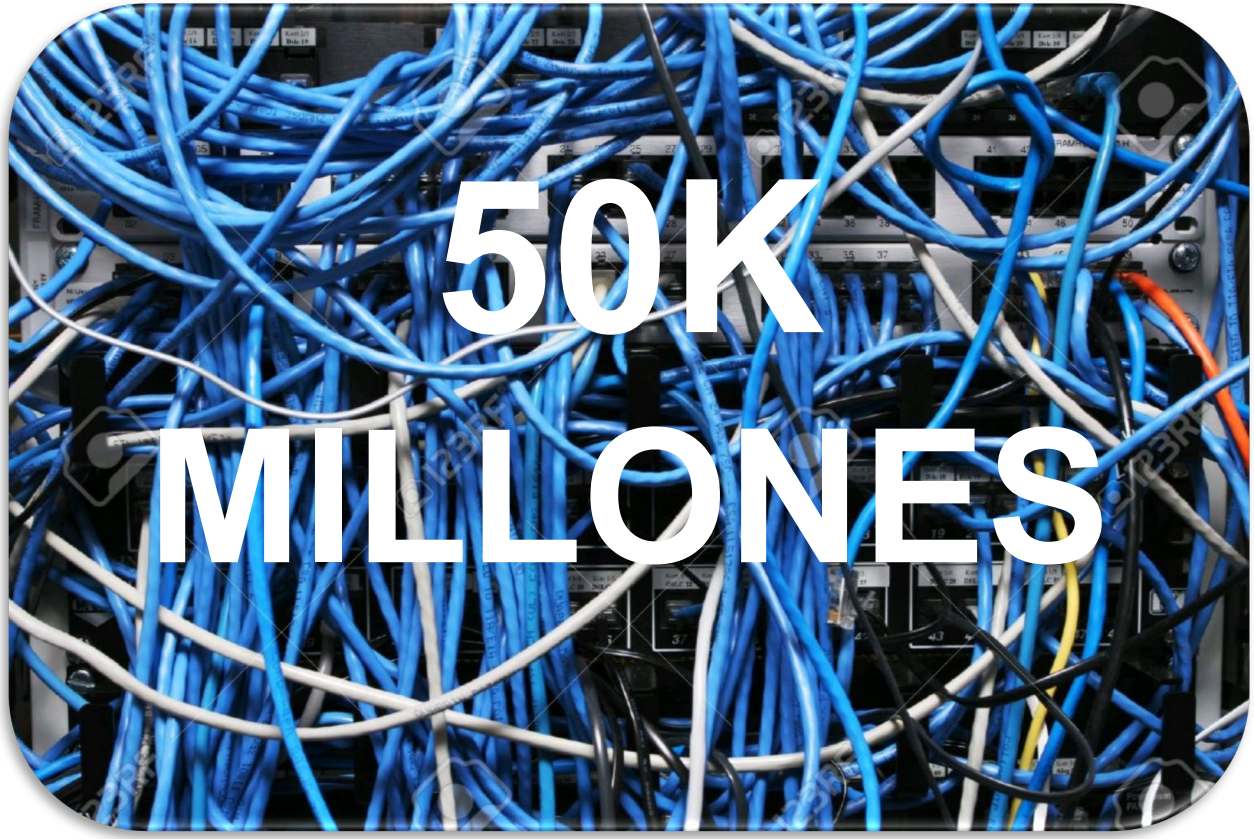
Se transforma en INCIBE

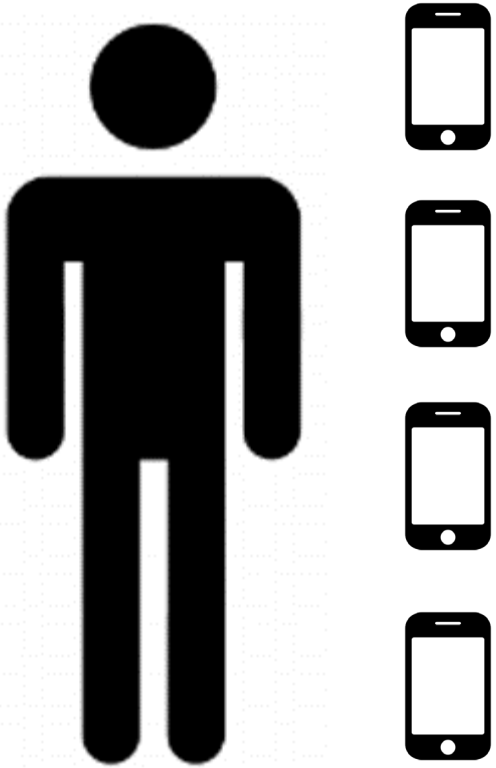
Instituto Nacional de Ciberseguridad de España

INCIBE-CERT

Trasposición Directiva NIS

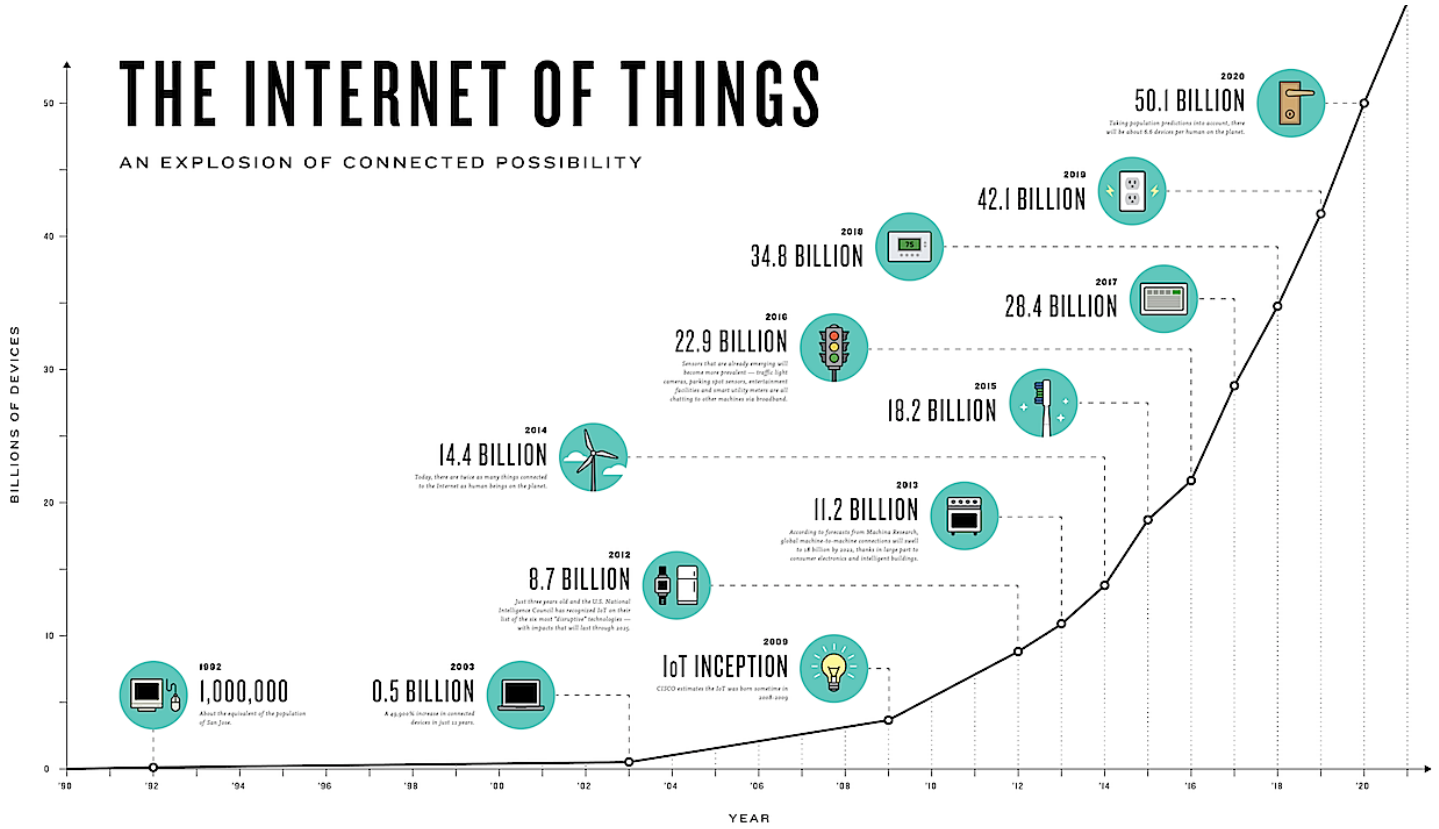
Estado y necesidad de la Ciberseguridad





Fuente: http://www.i-scoop.eu/internet-of-things/

Estado y necesidad de la Ciberseguridad

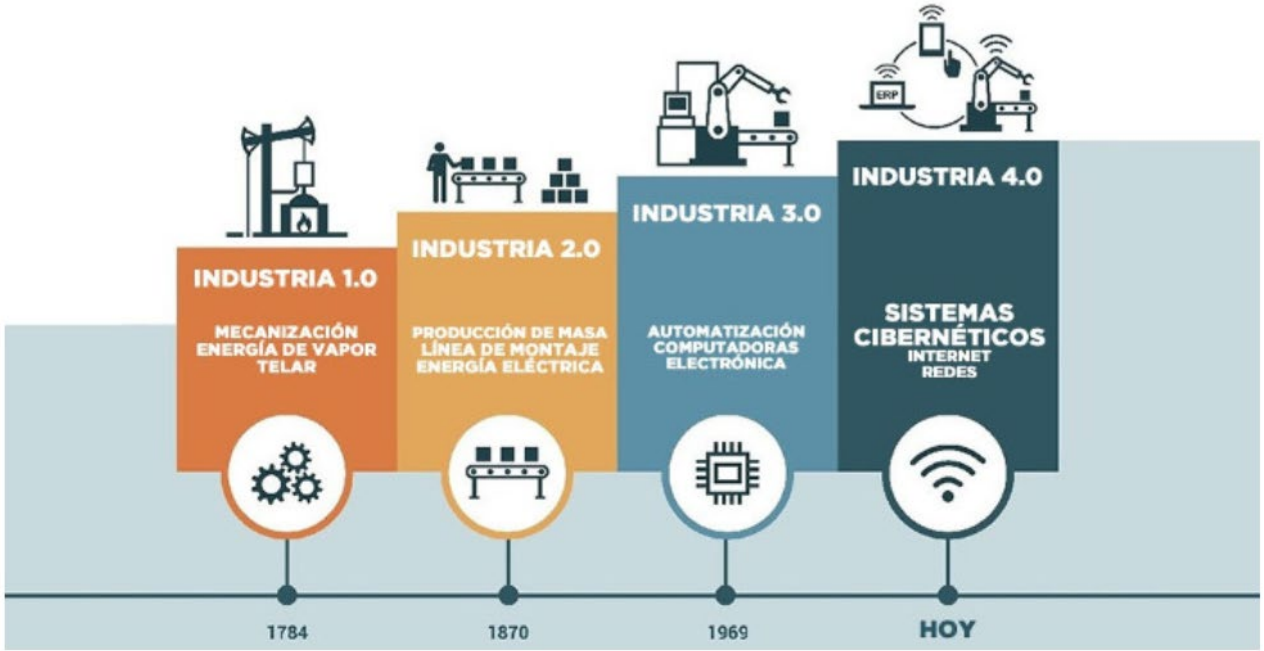


Fuente: http://www.i-scoop.eu/internet-of-things/

Estado y necesidad de la Ciberseguridad

Fuente: https://www.ins-digital.com/consultoria-iot/?lang=es

Estado y necesidad de la Ciberseguridad



La industria 4.0 pone en auge el uso de sistemas cibernéticos enfocados a la producción industrial

Fuente: https://blog.nivel4.com/noticias/tendencias-de-ciberseguridad-en-la-industria-agropecuari

Estado y necesidad de la Ciberseguridad

Redes 5G

Big Data

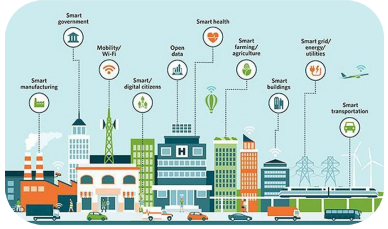
Cloud

Blockchain

IA

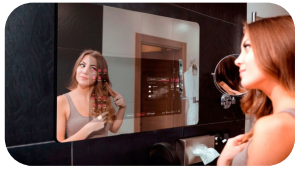
Vectores creados por katemangostar, stories, rawpixel.com, macrovector y freepik - www.freepik.es

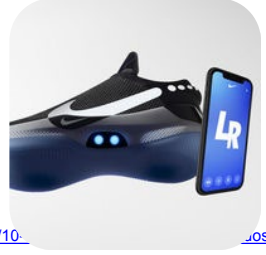
Estado y necesidad de la Ciberseguridad



Tr… …tal de la empresa

¡¡SEGURA!!





Fuente: https://www.prevencionintegral.com/actualidad/noticias/2019/05/23/10… …os-en-dia-c

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

¿Estamos preparados?

Estado y necesidad de la Ciberseguridad

GOBIERNO DE ESPAÑA · VICEPRESIDENCIA TERCERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

El Médico Interactivo

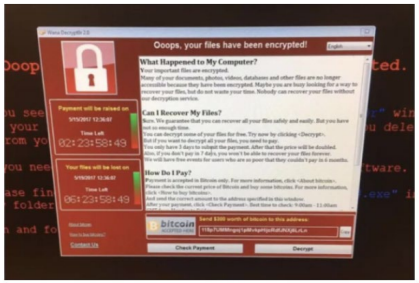
La ciberseguridad, un remedio sanitario

El modelo sanitario de nuestra sociedad se basa en un marco de "Salud Integral" con una historia clínica compartida por los diferentes actores sanitarios y que resulta accesible para el ciudadano. Actualmente, se demanda un acceso continuo a la prestación y asistencia sanitaria, incluso desde el móvil mediante APP sanitarias, buscando una atención eficaz e inmediata que requiere un alto nivel de integración de sistemas de información muy complejos. Esto implica que los sistemas y tecnologías necesarios en la asistencia sanitaria estén conectados, pero con un riesgo inherente de la propia conectividad que podría traicionar la seguridad de los pacientes, sometiéndolos a riesgos innecesarios y obligándolos a pagar costes personales inaceptables

El Médico Interactivo 22 de abril 2019, 12:00 pm

a3sec Nosotros Soluciones Sectores Blog

El Sector Sanitario está sufriendo los mayores ciberataques aprovechando la actual pandemia provocada por el Covid-19:



- Más de 150 Países
- Más de 230k endpoints implicados
- Impacto significativo en infraestructura sanitaria: ordenadores, MRI escáneres, refrigeradores, etc.

Sin ir más lejos, el 23 de marzo se publicó la existencia de un ciberataque considerado muy peligroso contra hospitales españoles en plena crisis del Covid-19, se trata del programa "NetWalker", un ransomware (tipo de ciberataque que bloquea los sistemas informáticos de la víctima y pide un rescate a cambio de la clave para liberarlos) que, según han informado fuentes policiales, sería la base de una ofensiva cuyos "objetivos serían principalmente trabajadores y organismos sanitarios".

COMPUTERWORLD UNIVERSITY

Informe 2020 de brechas de datos en el sector sanitario

20 FEB 2020

Las infracciones de seguridad en la información médica afectaron a más de 27 millones de usuarios el año pasado

ABC SOCIEDAD

España · Internacional · Economía · Sociedad · Madrid · Familia · Opinión · Deportes · Gente · Cultura · Ciencia · Historia · Viajar · Play · Summum · Más

Sanidad advierte de fallos de ciberseguridad detectados en bombas de insulina

Laa alerta afecta a varios productos fabricados por Medtronic MiniMed

Bomba de insulina

Sophos **News**

El impacto de COVID-19 en la ciberseguridad del sector sanitario

Actualidad · Coronavirus · Corporate · coronavirus

16 OCTOBER 2020

El informe de mitad de año de Fortified descubrió que el 60% de las infracciones de atención médica de la primera mitad de 2020 fueron causadas por un ciberatque o incidente de TI, en lugar del personal sanitario. Los compromisos de correo electrónico han sido el vector de ataque más común para obtener acceso a las redes de atención médica y robar datos de pacientes durante la pandemia. Fortified explicó que estos ataques a menudo se ejecutan mediante campañas de phishing que se utilizan para instalar malware o ransomware.

Fuentes: https://blog.a3sec.com/ciberseguridad-en-el-sector-sanitario.-parte-1%C2%AA
https://news.sophos.com/es-es/2020/10/16/el-impacto-de-covid-19-en-la-ciberseguridad-del-sector-sanitario/
https://elmedicointeractivo.com/la-ciberseguridad-un-remedio-sanitario/
https://www.computerworlduniversity.es/ciberseguridad/informe-2020-de-brechas-de-datos-en-el-sector-sanitario
https://www.abc.es/sociedad/abci-sanidad-advierte-fallos-ciberseguridad-detectados-bombas-insulina-201907261335_noticia.html

Estado y necesidad de la Ciberseguridad

Los ciberataques al deporte ya causan pérdidas

Y es que, como ocurre en cualquier otro sector de actividad, a la creciente digitalización de los deportes se suma el dinero que mueve el sector dentro y fuera de los estadios. Los millones de americanos que asisten a eventos deportivos en los estadios de EE.UU y otros grandes recintos para espectáculos aportan unos 40.000 millones de dólares a la actividad económica anual. En el Reino Unido la industria del deporte supone unos 37.000 millones de libras a la economía. No es de extrañar, que como ocurre en otras actividades, en el deporte la mayoría de los ataques también tengan una motivación económica. Según el informe **The Cyber Threat to Sports Organisations** elaborado por el National Cyber Security Centre, casi un tercio (el 30%) de los incidentes analizados causaron daños financieros directos a la organización víctima del ataque. Con un coste medio de unas 10.000 libras por cada brecha de seguridad, aunque alguna entidad deportiva reconoce pérdidas de más de 4 millones de libras.

> El informe señala que el 70% de las entidades deportivas encuestadas reconoce al menos un ciberataque al año

El informe señala que el 70% de las entidades deportivas encuestadas reconoce al menos un ciberataque al año (más que el doble de la media sufrida por los negocios británicos) y que el 41% de los casos de ataques o brechas de seguridad, sirvieron para incorporar nuevas medidas de protección para evitar futuros incidentes. Entre los casos más llamativos recogidos en el informe destacan el de un equipo de la Liga de Fútbol Inglesa (EFL) que sufrió un ataque de ransomware que afectó a sus sistemas corporativos y de seguridad. Los ciber secuestradores pidieron un rescate de 400 bitcoins que el club no pagó pese a que el ataque le costó la pérdida de información almacenada, la inutilización del email corporativo, así como del sistema del circuito cerrado de televisión y los tornos de acceso, lo que casi obliga a cancelar un partido.


Premier League • La intervención del banco evitó que un club perdiera más de un millón de euros

Hackers ponen en peligro la ciberseguridad de la Premier League

Redacción MARCA 23/07/2020 | 06:51 CEST

In English 0 Comentar

PUBLICIDAD

Hackean una dirección de correo electrónico de un director ejecutivo EFE

El **Centro Nacional de Seguridad Cibernética (NCSC)** alertó de que la **dirección de correo electrónico de un director ejecutivo** de un club de la **Premier League** fue **hackeada** durante la negociación de una transferencia de más de un millón de euros. Tan solo la intervención del banco evitó que el equipo perdiera tal cantidad de dinero.


TECNOLOGÍA

Así fue entrenar sin datos de Garmin

Aunque contaba con respaldo de sus datos y los de sus equipos, para una corredora y entrenadora profesional, el ciberataque a las plataformas de Garmin alteró su manera de trabajar a distancia.

mar 28 julio 2020 03:37 PM

La firma de wearables y procesamiento de datos deportivos y de navegación sufrió un ciberataque el 23 de junio. (Foto: Garmin) (Brad Grandon)


FITNESS

Detectado un fallo de seguridad en la app de fitness Polar Flow

HA DEJADO AL DESCUBIERTO LA UBICACIÓN DE SUS USUARIOS

SUSCRÍBETE GRATIS

NEW ARMY FLOORING

SALTER

Fuentes: https://www.ncsc.gov.uk/files/Cyber-threat-to-sports-organisations.pdf
https://www.marca.com/futbol/premier-league/2020/07/23/5f1915d546163fef0d8b463c.html
https://expansion.mx/tecnologia/2020/07/28/asi-fue-entrenar-sin-datos-de-garmin
https://www.cmdsport.com/fitness/actualidad-fitness/detectado-fallo-seguridad-la-app-fitness-polar-flow/

Estado y necesidad de la Ciberseguridad

GOBIERNO DE ESPAÑA · VICEPRESIDENCIA TERCERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

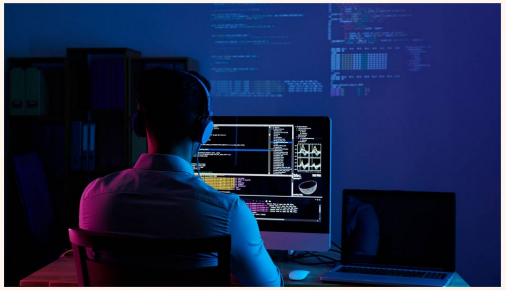
PYMES >

El 70% de los ciberataques son a pymes, con un coste de 40 millones

5D

J. A. VEGA ORTEGA

- La protección en este sentido es insuficiente.



El teletrabajo dispara las brechas de ciberseguridad en las empresas españolas

La filtración involuntaria de información es la causa de la mayoría de pérdidas de datos móviles corporativos

04.11.2020 14:31 h. Actualizado: 04.11.2020 22:40 h. 3 min

La generalización del **teletrabajo** ha provocado un incremento de las brechas de seguridad en las empresas españolas. Según un estudio elaborado por **Kingston**, un 23% de las compañías han sufrido más fallos de seguridad tras los cambios en los centros de trabajo. En concreto, un 7% ha detectado más de cinco brechas de ciberseguridad durante el último año.

El valor de la ciberseguridad: "Un ataque hace desaparecer al 60% de las empresas"

El 'ransomware' es tan peligroso que el 60% de las empresas que lo sufren desaparecen a los seis meses

Mariel Delgado · Bolsamania · A+ A+

01 nov, 2020 06:00 *Actualizado: 03 nov, 2020 15:49* Tiempo de lectura: **8min**

Publicidad

Madrid | 26 FEB 2020 - 07:40 CET

Los **ataques informáticos** dirigidos a empresas continúan creciendo. En España, el coste de los ciberataques ya se cifra en **40 millones de euros**, siendo la pequeña y mediana empresa la que más los sufre.

Los datos indican que siete de cada diez ciberataques tienen como víctimas a pymes. Así lo avala el último informe elaborado por acierto.com.

A pesar de conocer este problema, más del 30% de las pymes españolas solo cuenta con protocolos de seguridad de carácter básico. Según explican desde acierto.com, existen

≡ EL PAÍS NEGOCIOS

Ciberataques que matan a las empresas

Las alertas de seguridad informáticas que ponen en jaque a las compañías comienzan a ser moneda habitual en un mundo hiperconectado

Fuentes: https://cincodias.elpais.com/cincodias/2020/02/23/pyme/1582491990_626988.html
https://www.bolsamania.com/noticias/tecnologia/valor-ciberseguridad-ataque-hace-desaparecer-60-empresas--7695889.html
https://cronicaglobal.elespanol.com/creacion/vida-tecky/teletrabajo-dispara-brechas-ciberseguridad-empresas-espanolas_402936_102.html
https://elpais.com/economia/2020/02/14/actualidad/1581694252_444804.html

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

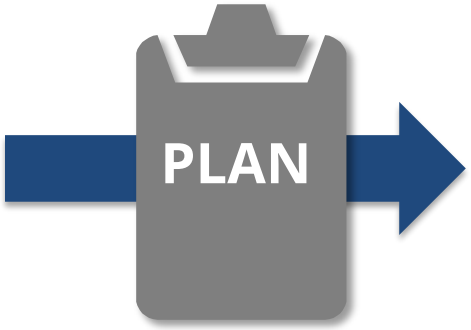
¿Cómo lo conseguimos?

¿Dónde estoy?
¿Cómo estoy?

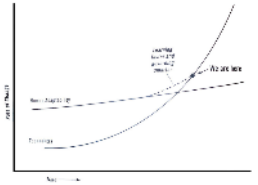
GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

¿TIENES UN PLAN?



ANÁLISIS PRELIMINAR DE RIESGOS



¿Qué tecnologías utiliza en su empresa?

- ☐ Correo electrónico
- ☐ Página web
- ☐ Servidor(es) propio(s)
- ☐ Teletrabajo
- ☐ Dispositivos móviles (tablet / smartphone / portátiles) con información de empresa

https://adl.incibe.es/

PENSAR COMO UN CIBERDELINCUENTE

- **Interrumpir los sistemas o piratearlos**
- Secuestrar información
- **Capturar credenciales de transacciones financieras**
- Identificar vulnerabilidades para explotarlas
- **Controlar y exponer información confidencial, personal o patentada.**

- **Obtener beneficios de manera ilegítima.**
- Pedir rescate para liberar la info secuestrada.
- **Venta de cuentas o interferencia en transacciones.**
- Hacer trabajar a nuestros sistemas para ellos.
- **Causar daños reputacionales y pérdidas.**

CONOCER LAS AMENAZAS

- **Fraude y extorsión**
- **Robo de datos / Fuga de datos**
- **Página web**
  - Defacement
  - Phishing
  - DoS
  - Suplantación
- **Redes sociales**
  - Suplantación
  - Comentarios negativos

TELETRABAJO SEGURO

1. Para el empleador
2. Para el empleado
3. Fraudes y otros incidentes
4. Fuentes de información

TELETRABAJO SEGURO

1. **Para el empleador**
   - Tecnologías para acceso remoto: escalabilidad y seguridad
   - Equipamiento para el empleado o BYOD
   - Aspectos legales (PRL, confidencialidad, RGPD)
   - Concienciación
2. **Para el empleado**
3. **Fraudes y otros incidentes**
4. **Fuentes de información**

COMO EMPLEADOR PLANTEATE:

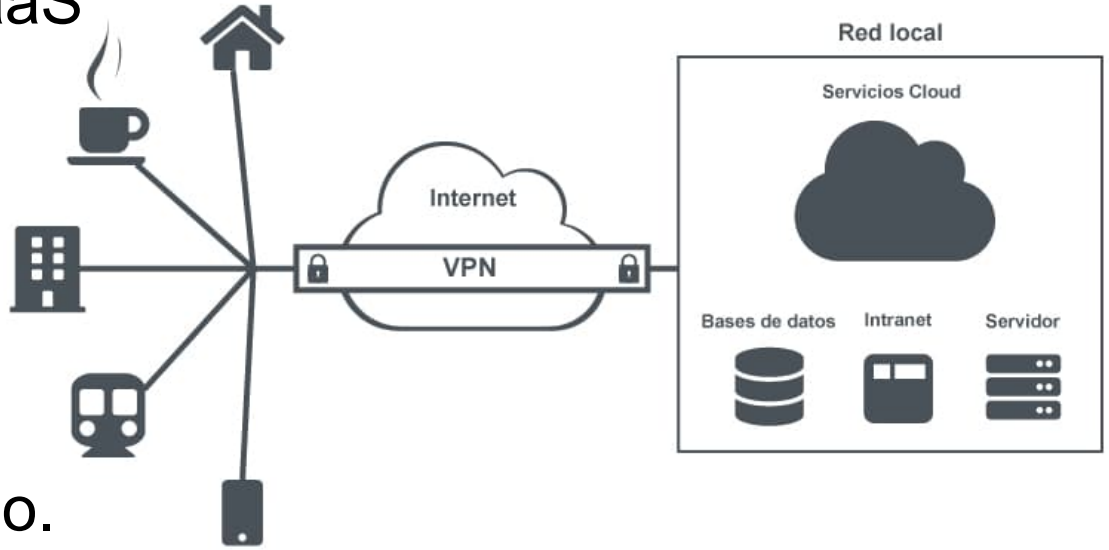
- ¿Cómo ofrecer teletrabajo a tus empleados?
- ¿Qué capacidad y seguridad me ofrecen los sistemas de acceso remoto?
- ¿Qué aspectos legales tiene el teletrabajo?
- ¿Están concienciados para teletrabajar?

EQUIPOS CORPORATIVOS VS BYOD

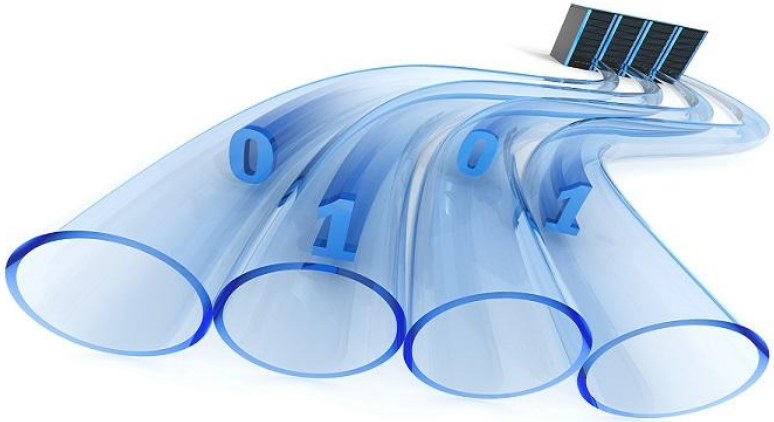
- Corporativo primera opción.
  - Actualizados / Backup
  - Capacidad de reposición
- BYOD con Soluciones de Gestión
  - Configuración
  - Conexiones
  - Cifrado, backup, apps
  - Acceso

ACCESO REMOTO SEGURO

- VPN propia vs VPNaaS
- VPN + Escritorio Remoto
- Accesos a través del móvil
- Red cableada vs wifi en casa del empleado.



Características VPN seguras



- Cifrado extremo a extremo de todo el tráfico.
- Proveedor en la UE.
- Con registros de log.
- Su política de privacidad cumple los requisitos de tu empresa.
- Escalabilidad.

Videoconferencia y herramientas colaborativas en cloud

- Permitir solo aplicaciones que garanticen los estándares de privacidad y seguridad.
- Establecer una **política de uso permitido** de apps en la nube.

Videoconferencia segura

- **Cifrar** todas las comunicaciones
- **Proveedor externo** que cumpla los requisitos legales y de seguridad.
- Añadir únicamente a **contactos** conocidos y **de confianza.**
- **Deshabilitar** la compartición de **escritorio, audio y video por defecto**.

Protege el backend de la web y los perfiles en RRSS

- Aplicaciones corporativas accesibles solo a través de **canales cifrados** (SSL VPN, IPSec VPN).
- El acceso a los portales web y perfiles corporativos RRSS con **autenticación multifactor**.

PRL, RGPD, acuerdos confidencialidad

- PRL (entorno seguro)
- RGPD, LOPDGDD
- Acuerdos confidencialidad
- LPI (propiedad intelectual)

Concienciación

- Establecer políticas uso y darlas a conocer.
- Recordar cómo proteger los datos personales.
- Entrenarles en detección de amenazas.
- Facilitar el reporte de incidentes.
- Revisar los acuerdos confidencialidad y RGPD.

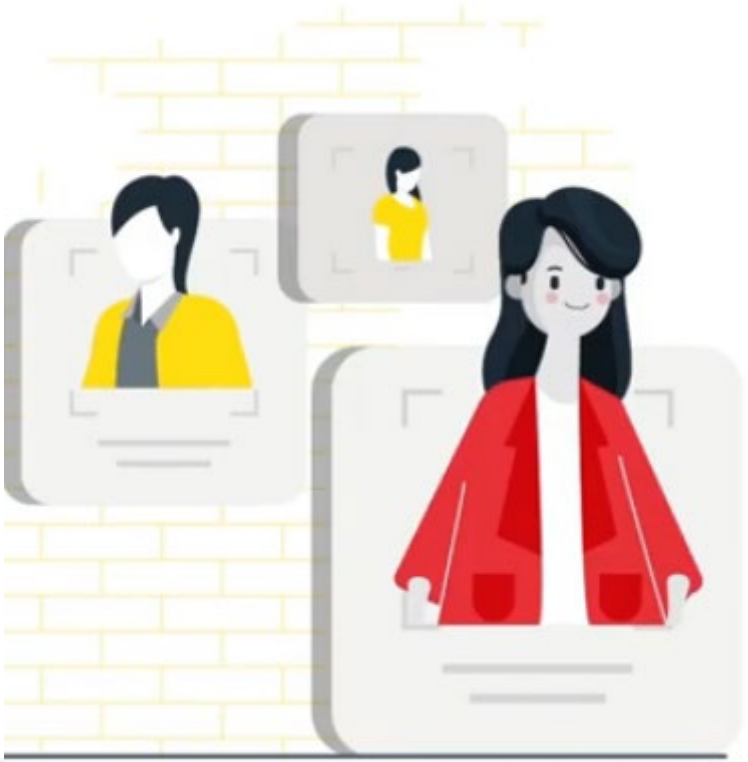
Teletrabajo seguro

1. **Para el empleador**
2. **Para el empleado**
   - Mi entorno doméstico seguro
   - Gestión de tiempo y del espacio en casa
   - Conexiones seguras
   - Confidencialidad y protección de datos
3. **Fraudes y otros incidentes**
4. **Fuentes de información**

Entorno de trabajo seguro

- Evita el acceso de terceros a información confidencial.
- Protege tus contraseñas y soportes.
- No pierdas de vista los dispositivos.
- Cumple LOPDGDD.
- No mezcles ocio y trabajo.

Seguridad en acceso remoto



- Contraseñas robustas y doble factor.
- Sistemas actualizados.
- Cifrado de soportes y dispositivos.
- Backup y borrado seguro.
- Comparte a través de la red corporativa no a través de redes externas.

Seguridad en acceso remoto

- Prioriza el cable frente al wifi.
- Configura la seguridad de tu red.
- Verifica la seguridad de las comunicaciones antes de compartir información confidencial.

Consejos #1

¿Cómo acceder de forma segura a los sistemas e información de la empresa?

Utilizar una red privada virtual (VPN).

Utilizar una VPN, en caso de trabajar en un escritorio remoto.

Revisar el Acuerdo de Nivel de Servicios si trabajas en la nube.

VPN

Cuidado con los correos y mensajes maliciosos

Tener precaución con adjuntos de correos, enlaces a páginas fraudulentas,etc.

Introducir o usar la URL o aplicación oficial del organismo legítimo.

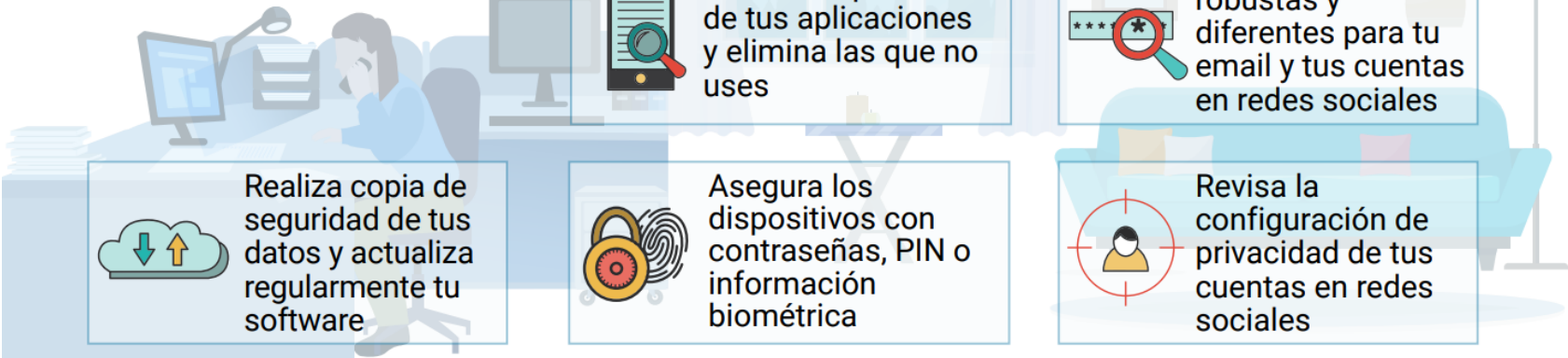
Revisar los enlaces a noticias sobre la crisis de coronavirus.

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Consejos #2

CÓMO HACER DE TU HOGAR UN CIBER LUGAR SEGURO

EUROPOL EC3 European Cybercrime Centre



- Wi-fi: cambia siempre la contraseña por defecto del rúter
- Instala un antivirus en todos los dispositivos conectados a internet
- Revisa los permisos de tus aplicaciones y elimina las que no uses
- Elije contraseñas robustas y diferentes para tu email y tus cuentas en redes sociales
- Realiza copia de seguridad de tus datos y actualiza regularmente tu software
- Asegura los dispositivos con contraseñas, PIN o información biométrica
- Revisa la configuración de privacidad de tus cuentas en redes sociales

Consejos #3

Mantente alerta y no:

- ⊗ Respondas a mensajes o llamadas sospechosas

- ⊗ Abras enlaces y archivos adjuntos no solicitados

- ⊗ Compres cosas online que parezcan estar agotadas en cualquier otro lugar
- ⊗ Compartas detalles de tu tarjeta bancaria o información financiera personal

- ⊗ Envíes dinero por adelantado a alguien que no conoces
- ⊗ Compartas noticias que no vengan de fuentes oficiales

- ⊗ Hagas donaciones benéficas sin verificar su autenticidad

Otras consideraciones

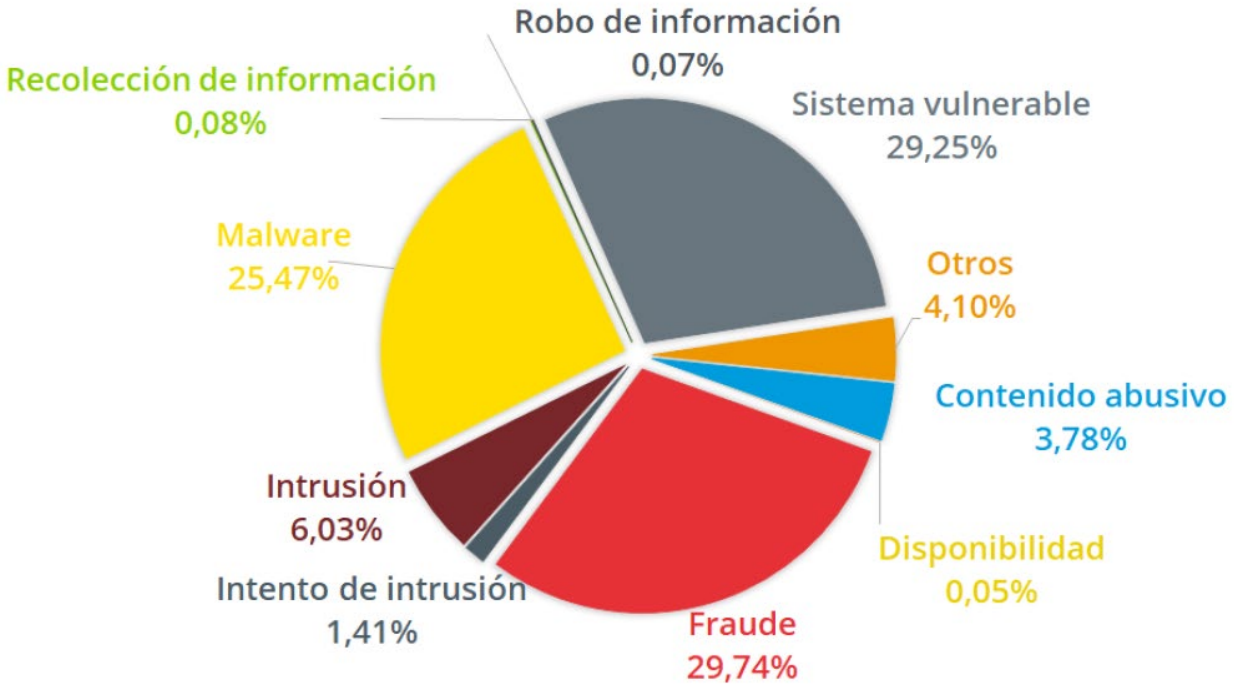
- Gestores de contraseñas.
- Configuraciones de seguridad para equipos domésticos.
- Migración a teletrabajo de ida y vuelta.
- Vulnerabilidades de tu equipo (y de tu red) domésticos.
- Correo electrónico personal para uso profesional, riesgos.
- Pendrives, discos externos y otras formas de almacenamiento (nube) para intercambiar documentos de forma segura y fiable en esta situación.
- Si usas Whatsapp o similares para organizar el trabajo en remoto o acciones solidarias… privacidad y otros temas de seguridad.
- Soluciones de seguridad (catálogo) para tu trabajo en remoto.
- Privacidad en teletrabajo.

Teletrabajo seguro

1. **Para el empleador**
2. **Para el empleado**
3. **Fraudes y otros incidentes**
   - Fraudes a través de correo electrónico
   - Incidentes relacionados con el sw. / hw. Teletrabajo
   - Gestión de incidentes
   - Planes de contingencia
4. **Fuentes de información**

Incidentes gestionados por incibe

Categorías


Robo de información
0,07%
Recolección de información
0,08%
Sistema vulnerable
29,25%
Malware
25,47%
Otros
4,10%
Contenido abusivo
3,78%
Intrusión
6,03%
Disponibilidad
0,05%
Intento de intrusión
1,41%
Fraude
29,74%

Fraudes y otros incidentes #CiberCOVID19

- Falsas app, servicios gratuitos
- Fraudes y bulos
  - Consejos
  - Solicitud ayuda
  - Cursos
  - Venta material sanitario,…
- Corona-*phishing*
- *Ransomware*

Privacidad


agencia
española
protección
datos
Inicio
La Agencia
Derechos y deberes
Áreas de actuación
Informes y resoluciones
Guías y herramientas
Prensa y comunicacion
Notas de prensa
Comunicado de la AEPD sobre apps y webs de autoevaluación del Coronavirus
26 DE MARZO DE 2020
Comunicado de la AEPD sobre apps y webs de autoevaluación del Coronavirus

Phishing


MinSaludCol
@MinSaludCol
⚠️CUIDADO⚠️ Por e-mail y WhatsApp circula información falsa, a nombre del @MinSaludCol, que advierte la llegada del coronavirus a su sector, junto con un archivo que se instala en su dispositivo móvil y roba información personal. Informate solo en canales oficiales de MinSalud
Translate Tweet
From: Ministerio de Salud <comunicados@minsalud.gov.co>
Sent: Thursday, March 5, 2020 10:43:34 AM
Subject: Detectamos en su sector la presencia de COVID-19 (Corona virus) intentamos comunicarnos via telefonica con usted .
La salud es de todos
Minsalud
Estimado ciudadano
Hemos intentado comunicarnos via telefonica con usted en el dia de hoy pero ha sido imposible , se trata de un tema muy delicado el cual le relatamos a continuación
Detectamos en su sector la presencia de COVID-19 (Corona virus) es por eso que como medida preventiva hemos adjuntado los sitios en los cuales no le recomendamos visitar , ya que estos se encuentran a pocos metros de su residencia .
Adjuntamos un archivo pdf este se encuentra con una clave es : salud
FALSO
GDT Guardia Civil
@GDTGuardiaCivil
#NiCaso a este mensaje que circula por #Whatsapp. Suplantan al Ministerio de Sanidad @sanidadgob para dar supuestas "recomendaciones" contra el #coronavirus #COVID19 y un enlace para venderte mascarillas.
Translate Tweet
+34 632
en línea
ALERTA POR CORONAVIRUS
Mensaje urgente del Ministerio de Sanidad:
http://www coronavirus.es
¡Compártelo en tus grupos de WhatsApp y en tus Redes Sociales!
¡¡PUEDES SALVAR VIDAS!!
Es muy importante que siga las medidas de protección recomendadas:
#NiCaso
DEPARTAMENTO DE DELITOS TELEMÁTICOS

Incidentes #CiberCOVID19

Avisos de seguridad

Ingeniería social, phishing, ransomware, actualizaciones... En nuestra sección de avisos te facilitamos toda la información necesaria para prevenir, proteger y responder ante incidentes de seguridad en el entorno empresarial. Visita cada día esta página y sé más rápido que tus amenazas. Y recuerda, que también puedes suscribirte a nuestro boletín para recibir la información.

Campaña de smishing suplanta al SEPE utilizando como gancho los ERTE

Publicado el 30/03/2020

Importancia: 4 - Alta

Etiquetas: #CiberCOVID19 Fraude Ingeniería social Phishing

La FNMT seguirá admitiendo los certificados electrónicos recientemente caducados durante el estado de alarma

Publicado el 26/03/2020

Importancia: 5 - Crítica

Etiquetas: #CiberCOVID19 Actualización Navegador

INCIBE


incibe_
Servicios públicos Ciberseguridad
• Detección, análisis y respuesta ante ciberataques
• Concienciación en ciberseguridad
Fomento de la industria, I+D+i y talento
• Desarrollo de la industria nacional
• Fomento I+D+i
• Promoción e identificación de talento
Desarrollo tecnologías ciberseguridad
• Desarrollo de tecnologías de ciberseguridad
• Inteligencia en el ciberespacio

¿QUÉ ES PROTEGE TU EMPRESA?

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Protege tu empresa

protege tu empresa

Pymes

Autónomos

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

¿CUÁL ES EL OBJETIVO DE PROTEGE TU EMPRESA?

Concienciación y sensibilización

Formación

Soporte

https://www.incibe.es/protege-tu-empresa

SERVICIOS DE CIBERSEGURIDAD PARA EMPRESA

Información

Formación

Herramientas

Soporte

DESGLOSE DE LOS SERVICIOS

Información

Blog

Avisos de seguridad

RGPD para pymes

Sellos de confianza

¿Qué te interesa?

Formación

Itinerarios interactivos

Hackend

Curso online

Juego de rol

Talleres en ciberseguridad

Kit de concienciación

DESGLOSE DE LOS SERVICIOS

Herramientas

Políticas de seguridad

Servicio Antibotnet

¿Conoces tus riesgos?

Ayuda ransomware

Catálogo de Ciberseguridad

Guías

Soporte

Formulario de contacto

Línea de ayuda

KIT DE CONCIENCIÓN

- ¡Todo lo necesario para concienciar a los empleados en ciberseguridad!
- Fomentar buenos hábitos en ciberseguridad
- Materiales en diversos formatos
  - Ataques dirigidos
  - Documentos
  - Posters
  - Imágenes
  - Trípticos
  - Test de evaluación
- Distribución programada

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ITINERARIOS SECTORIALES INTERACTIVOS

- Videos interactivos por sector empresarial
- Aspectos esenciales en ciberseguridad
- Laura y Miguel nos guiarán en esta aventura
- 29 videos interactivos con situaciones cotidianas de cualquier empresa
  - Popups
  - Documentación adicional
  - Elementos específicos

HACKEND, SE ACABÓ EL JUEGO

- Juego cuyo objetivo es formar y concienciar en ciberseguridad
- Inspirado en el juego de Carmen SanDiego
- Disponible para varias plataformas y online
- Múltiples escenarios
- Premio Mejor Serius Game 2016 en el Fun&Serious Game Festival

JUEGO DE ROL

¿Estáis **preparados** para resolver un incidente de seguridad?

Sin necesidad de conocimientos técnicos específicos

Entrenamiento en la **toma de decisiones** durante una crisis

5 escenarios distintos habituales

Ransomware

Phishing alojado en la web empresarial

Fuga de información

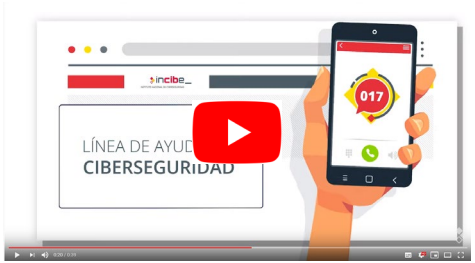
Ataque de ingeniería social

Formar parte en un botnet

LINEA DE AYUDA EN CIBERSEGURIDAD 017

017

TU AYUDA EN
CIBERSEGURIDAD
incibe_



Fuentes de información #1

- Blog:
  - ¿Tu casa es también tu oficina? ¡Protégela!
  - Conéctate a tu empresa de forma segura desde cualquier sitio con una VPN
  - ¿Es seguro tu escritorio remoto?
  - Precauciones al realizar una videoconferencia
  - Bondades y riesgos del BYOD
- Itinerarios (videos)
  - Vídeo 6 ¿Fuera de la oficina?
  - Vídeo 15 Tu trabajo en el móvil
  - Vídeo 26 Trabajando desde casa

Fuentes de información #2

- Glosario de términos de ciberseguridad
- Incibe #CiberCOVID19
- Políticas
  - Aplicaciones permitidas
  - Almacenamiento en la nube
  - Uso de dispositivos móviles corporativos / no corporativos
  - Uso de wifis y redes externas
- Guías:
  - Cloud computing
  - Seguridad en redes wifi
  - Dispositivos móviles personales para uso profesional (BYOD)

Fuentes de información #3

- Dosier: Protección en movilidad y conexiones inalámbricas
- Infografías:
  - Protección en movilidad y conexiones inalámbricas
  - VPN en dispositivos móviles
  - Uso seguro de BYOD
  - Pautas para teletrabajar seguro

Otras fuentes de información

- Teletrabajo: decálogo de ciberseguridad Basque Ciberescurity Centre
- Make your home a cyber safe stronghold EUROPOL
- Tips for cybersecurity when working from home ENISA
- Campañas de phishing sobre el COVID-19 AEPD
- CCN-CERT CiberCOVID19

Gracias por su atención

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD