INSTITUTO NACIONAL DE CIBERSEGURIDAD

Ciberseguridad

Política - Teletrabajo Seguro

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

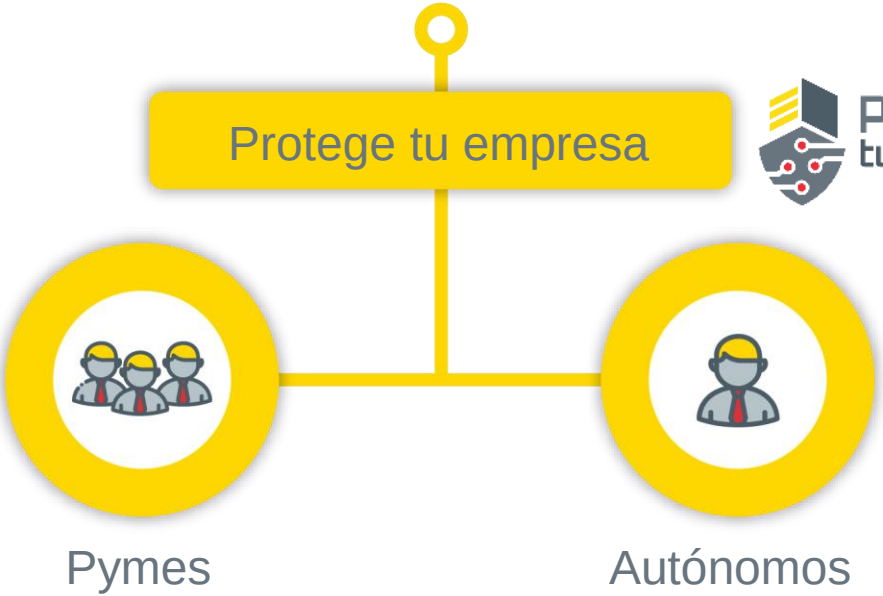
Trasposición Directiva NIS

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

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

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

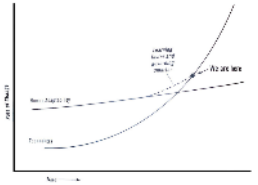
TU AYUDA EN
CIBERSEGURIDAD
incibe_

¿TIENES UN PLAN?

¿Dónde estoy?
¿Cómo estoy?

PLAN

GOBERNARSE DE FORMA MÁS INTELIGENTE: GESTIÓN DE RIESGOS



¿Qué tecnologías utiliza en su empresa?

Tecnología sí pero con seguridad

Seleccione las tecnologías que utiliza en su negocio o aquellas para las que quiera calcular el riesgo.

- ☐ 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:

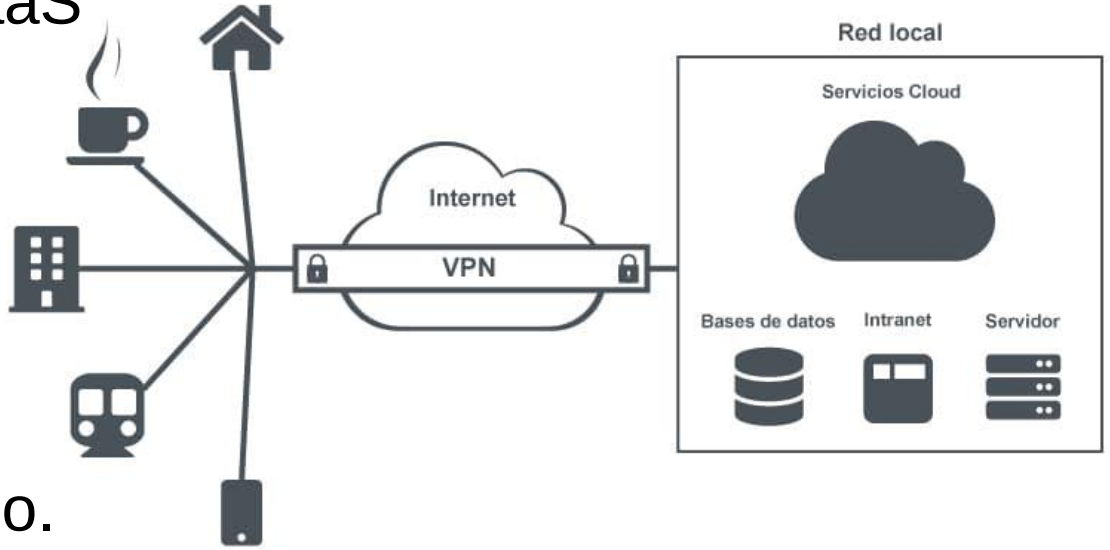
- ¿Cómo ofrecer teletrabajo a tus empleados?
- ¿Qué capacidad y seguridad me ofrecen los sistemas de acceso remoto?
- ¿Qué aspectos legales tiene el teletrabajo?
- ¿Están concienciados para teletrabajar?

EQUIPOS CORPORATIVOS VS BYOD

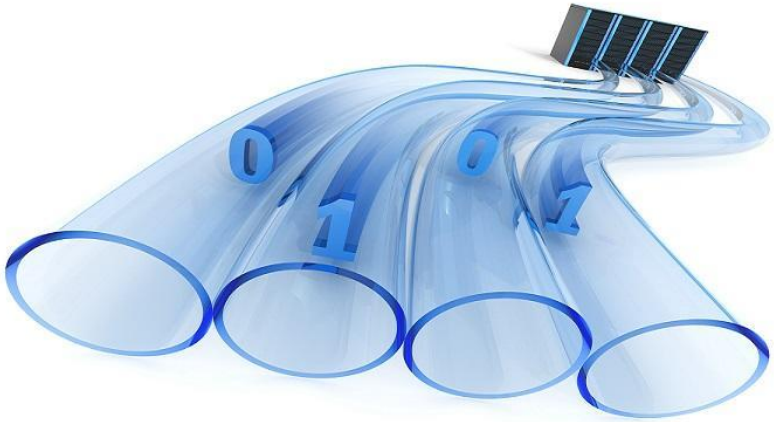
- Corporativo primera opción.
  - Actualizados / Backup
  - Capacidad de reposición
- BYOD con Soluciones de Gestión
  - Configuración
  - Conexiones
  - Cifrado, backup, apps
  - Acceso

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.

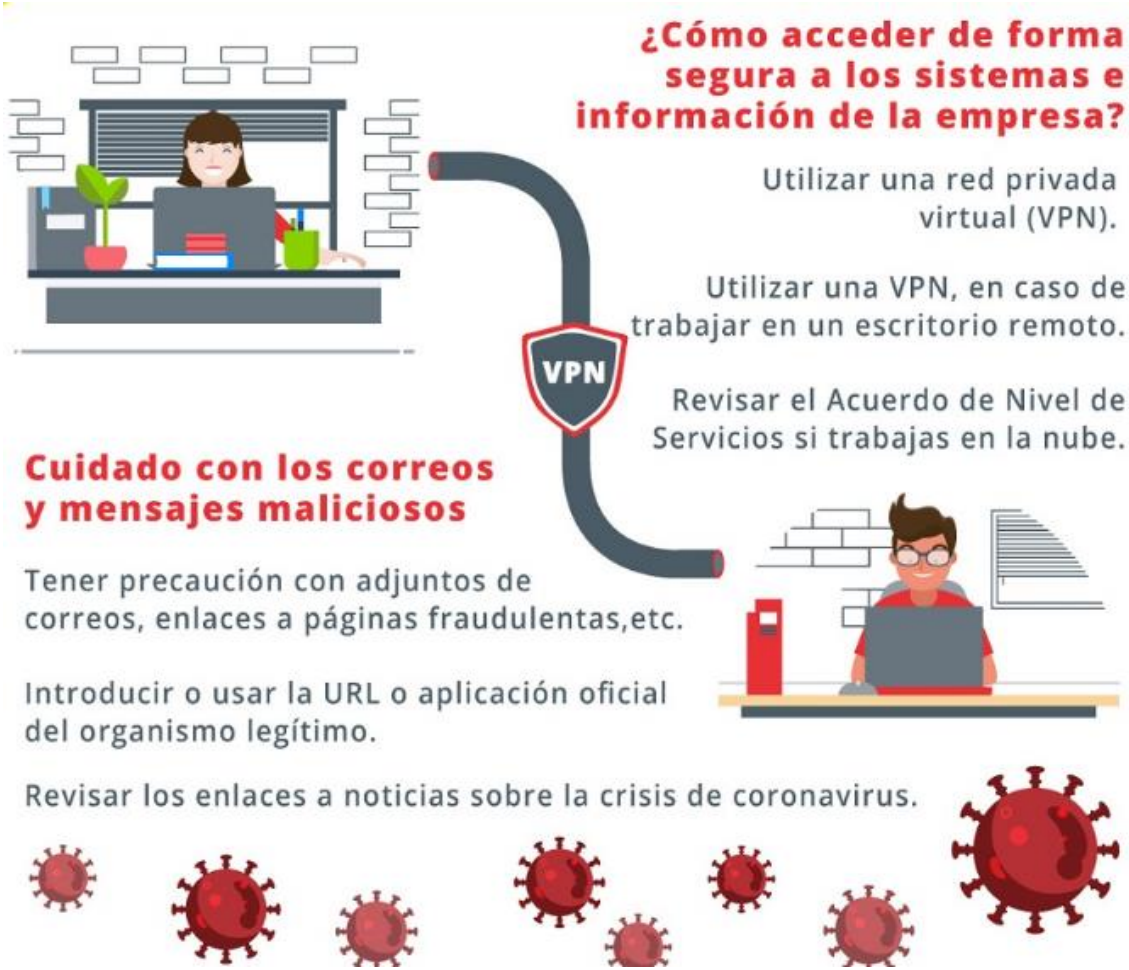
Seguridad en acceso remoto

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

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

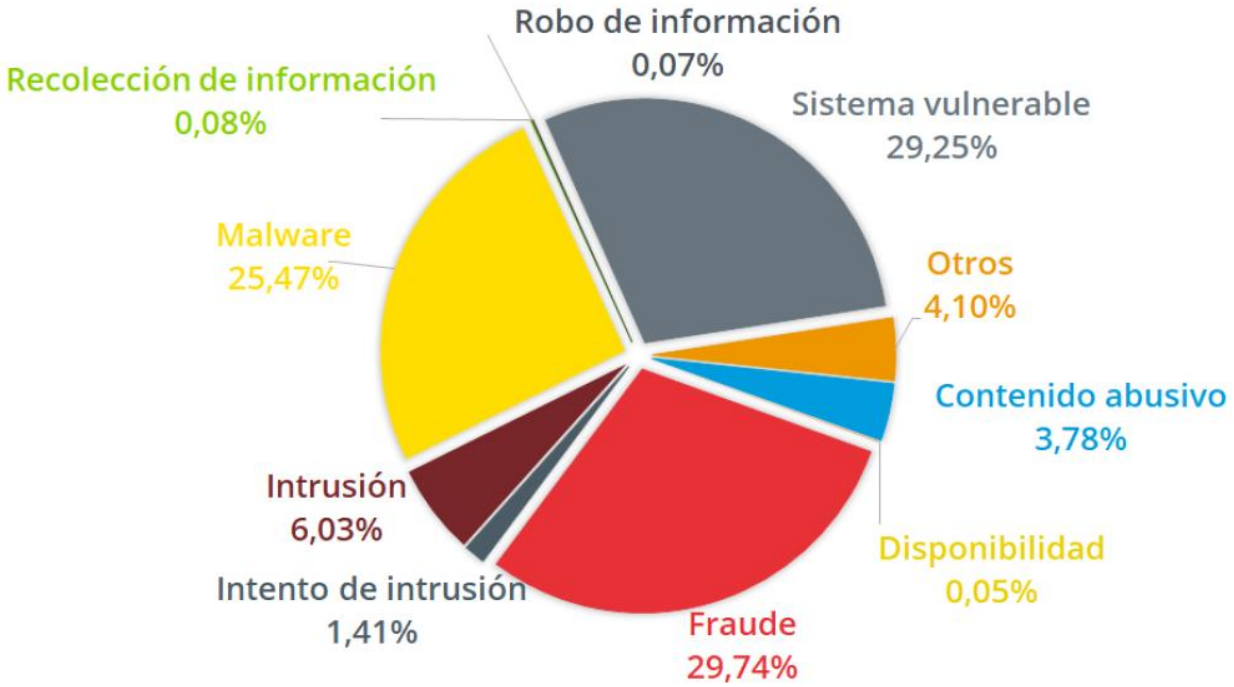
- Gestores de contraseñas.
- Configuraciones de seguridad para equipos domésticos.
- Migración a teletrabajo de ida y vuelta.
- Vulnerabilidades de tu equipo (y de tu red) domésticos.
- Correo electrónico personal para uso profesional, riesgos.
- Pendrives, discos externos y otras formas de almacenamiento (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

En caso de incidente o de desastre

- Planifica la gestión de incidentes.
- Revisa tu plan de contingencia.

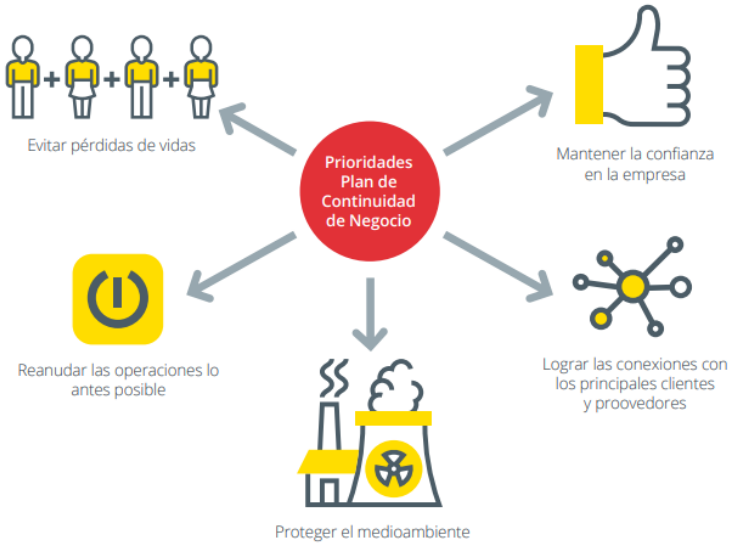
En caso de incidente

- Primeros pasos en la respuesta a incidentes:
  - evaluación inicial,
  - comunicación,
  - contención de daños y minimización de los riesgos.

En caso de incidente

- Respuesta a incidentes: tomando evidencias y recuperando la actividad:
  - identificar la gravedad del ataque,
  - proteger las pruebas,
  - Notificar a organismos externos,
  - recuperar los sistemas afectados,
  - lecciones aprendidas.

Continuidad de negocio

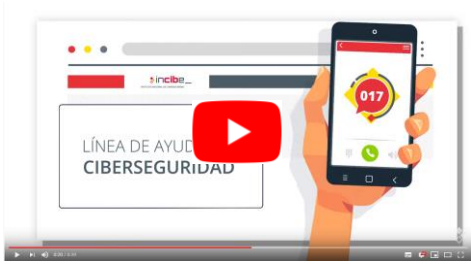


- Mantener el nivel de servicio en los límites definidos
- Establecer un período de recuperación mínimo
- Recuperar la situación inicial antes de cualquier incidente de seguridad
- Analizar los resultados y los motivos de los incidentes
- Evitar que las actividades de la empresa se interrumpan

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