



WEBINAR

“CIBERSEGURIDAD PARA PYMES. HACIA UNA DIGITALIZACIÓN SEGURA.”

OFICINA DE TRANSFORMACIÓN DIGITAL PARA PYMES

Te ayudamos a transformar tu negocio. Asesoría gratuita.



Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa



¿QUIÉNES SOMOS?

Digital Hand Made es una empresa aragonesa que nació orientada al desarrollo de servicios de redes e internet.

Nuestra gran dedicación, capacidad de innovación y calidad de servicios durante los **20 años** que tenemos como experiencia nos ha permitido convertirnos en un referente en soluciones de tecnología de valor añadido.

Ofrecemos **soluciones integrales** de transformación digital, comunicaciones, informática, telefonía, diseño web, redes, sistemas de control geriátrico, seguridad, consultoría de proyectos y más.



NUESTRAS ÁREAS DE ACTIVIDAD

TRANSFORMACIÓN DIGITAL Y UX



CIBERSEGURIDAD



SOLUCIONES CLOUD



COMUNICACIONES-CONTACT CENTER




SERVICIOS IT



OUTSOURCING Y VERTICALES



ÍNDICE

Situación actual 0. 


La información como activo de la empresa. 1. 

Identificación y gestión de riesgos. 2. 

Principales riesgos. El correo electrónico. 3. 

 4. Protección de la información. Backups

 5. Protección básica del entorno de trabajo

 6. Gestión de incidentes y continuidad de negocio.

 7. Decálogo conclusión



0- Situación actual

TRAS EL CIBERATAQUE A TRABAJO HACE 2 SEMANAS

Inspectores de Trabajo sin 'mail', ordenador y usando papel y boli. "Estamos desesperados"

Más de 1.900 inspectores y subinspectores de Trabajo en España están trabajando con sus portátiles personales, desde casa y sin conexión con el ministerio. Sigue el caos tras el ciberataque



La vicepresidenta tercera y ministra de Trabajo, Yolanda Díaz. (EFE)



Una oficina de empleo, en Madrid.

EMPLEO

El SEPE no pagará a 150.000 personas sus prestaciones en abril por los retrasos causados por el ciberataque

Este mismo martes, la ministra de Trabajo negó que se fuera a producir cualquier tipo de retraso.

bits

Acer, bajo un ciberataque de ransomware: exigen a la compañía 50 millones, el mayor rescate de la historia

20BITS, MARTA GASCÓN NOTICIA 22.03.2021 - 16:22H

[f](#) [t](#) [e](#)

- Se trata del mayor rescate de la historia hasta la fecha y detrás parece estar el grupo de cibercriminales REvil. Dan a la compañía hasta el 28 de marzo para pagar.
- El Área Metropolitana de Barcelona sufre un ciberataque similar al del SEPE que paraliza sus servicios.



BLOGS DE 20MINUTOS

DANDO LA NOTA
Gran polémica en USA por Lil Nas X: El rapero negro y gay que baila con el diablo

YA ESTÁ EL LISTO QUE TODO LO SABE
¿De dónde surge llamar 'vivaquear' a pasar la noche de acampada al aire libre?

1 DE CADA 10

CIENCIA ABIERTA

Ciberataque al IES Zaidín-Vergeles



0- Situación actual


lu. 12/04/2021 15:41
 Ibercaja <ibercaja-servicio-28392@city-takaoka.jp>
 RE: alertas de seguridad.

Para Ibercaja Banco | Particulares

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.
 Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática de algunas imágenes en este mensaje.

T20210114-10058528.pdf 25 KB
 ATT00002.pdf 27 KB

******* WARNING: Correo Externo. No haga clic en enlaces ni abra archivos adjuntos a menos que reconozca al remitente y sepa que el contenido es seguro. *******



Aviso Importante :

Estimado cliente,

Para evitar el uso fraudulento de tarjetas de crédito en internet, Ibercaja tiene un nuevo sistema de control:

[Iniciar sesión en su cuenta](#)

Ibercaja Banco Online © 2021

Servicio personalizado todos los días .
 este sitio web contiene información de carácter personal.



Estimado cliente,
 Su paquete está esperando la entrega, Confirme el pago (1.99EUR) en el siguiente enlace, la verification en linea debe hacerse en los proximos 14 dias antes de que caduque.

Haga clic aqui

10:41

MediaMarkt >

Mensaje de texto hoy, 10:40

Numero de pedido # 21792C
 Gracias por realizar una compra en nuestra tienda. Encontraras mas informacion en nuestra app o aqui: <http://ok6.us/3lcbIZ>

13:59

Mensaje de texto sábado, 11:46

CORREOS: Tu envío esta en camino: <https://correos-app.com/>

14:00

Mensaje de texto domingo, 11:17

CORREOS: Tu envío esta en camino: <https://correos-cdn.com/>





0- Situación actual

La web para pedir cita de vacunación en Cataluña sufre un ciberataque

ACN NOTICIA 12.07.2021 - 15:12H



- Una brecha en el portal para pedir cita para vacunarse provocó un "riesgo de exposición" de datos personales.
- Salut asegura que la "vulnerabilidad" está resuelta.
- DIRECTO:** Sigue toda la información sobre Covid-19.



Personas entre 55 y 59 años aguardan para de Barcelona.

BLOGS DE 20MINUTOS

CIENCIAS MIXTAS
No todo está en el virus: unos 40 genes pueden influir en la gravedad de la COVID-19

EL BLOG DE LILIH BLUE
Condones de sabores: ¿sirven solo para practicar sexo oral?

REALITY BLOG SHOW
Olga Moreno es la Velázquez del victimismo o cómo arreglar una metedura de pata a la desesperada en Supervivientes

1 DE CADA 10
No cabe duda: una nueva ola de odio LGTB+ se está extendiendo

CincoDías

EL PA

Compañías Mercados Economía Mi Dinero Fortuna / Cotizaciones f

ACTUALIDAD El sector financiero y las tecnológicas tiran de la contratación de oficinas »

TERRITORIO PYME > Pyme



AUTÓNOMOS / PYMES / EMPRENDEDORES / FRANQUICIAS / CURSOS Y EVENTOS / GUÍAS / FINANCIACIÓN

PYMES >

Los ciberataques en España crecen un 125%. La pyme la gran perjudicada

1.000 ciberataques al día.

DEL PROGRAMA DE FIDELIZACIÓN

Un ciberataque expone datos de clientes de 39 aerolíneas

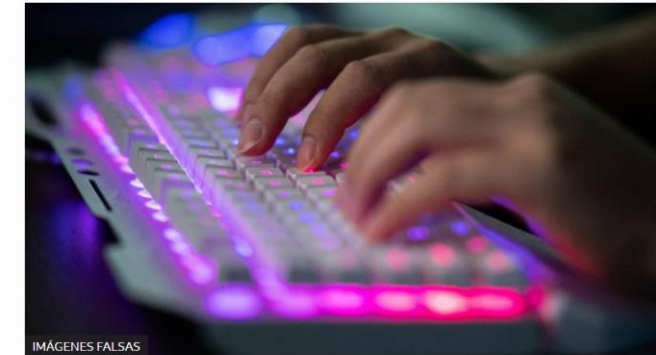
- British Airways, United Airlines Holdings Inc. y Singapore Airlines son algunas de las compañías afectadas



"Colosal" ciberataque golpea a cientos de empresas en EE.UU.

Redacción BBC News Mundo

3 julio 2021



IMÁGENES FALSAS

Unas 200 empresas en Estados Unidos fueron golpeadas por un "colosal" ataque cibernético tipo "ransomware" o cibersecuestro, en el que los sistemas quedan

OFICINA **Acelera** pyme



5 LEYES DE LA CIBERSEGURIDAD (NICK ESPINOSA):

- 1) Si hay una vulnerabilidad (física, lógica o humana) será explotada.
- 2) Todo sistema es vulnerable de alguna forma y en algún momento.
- 3) Los humanos creen cosas que deberían creer.
- 4) Junto con nuevas tecnologías vienen nuevas vulnerabilidades.
- 5) En caso de duda, volver a la ley número 1.





0- Situación actual

PRINCIPALES VECTORES

- Enlace malicioso
- Documento (WORD, EXCEL, PDF)
- Riesgos lógicos (malware, bad USB, etc)
- Riesgos físicos.(kill USB)
- JavaScript.
- Ingeniería social.
- Páginas maliciosas.





1- La información como activo de la empresa

- A. La información en el centro de nuestro negocio
- B. La seguridad de la información
 - A. Sucesos accidentales
 - B. Sucesos intencionados insiders
 - C. Cibercriminalidad
- C. Los tres pilares de la seguridad
 - A. Disponibilidad
 - B. Integridad
 - C. Confidencialidad
- D. La privacidad y la ley





1- La información como activo de la empresa



A. IDENTIFICANDO LOS RECURSOS CRÍTICOS

- INVENTARIADO IT.
- CLASIFICACIÓN. CRITERIOS
- TRATAMIENTO.

Limitar el acceso



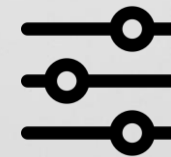
Cifrado



Copias de seguridad



Controles específicos



Acuerdos de confidencialidad





2- Identificación y gestión de riesgos CHECKLIST BÁSICO

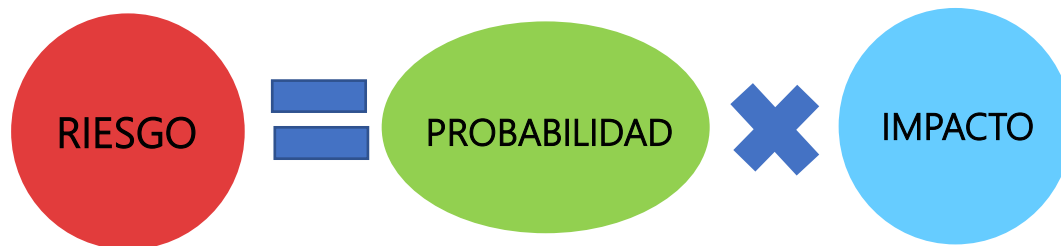
- 1) ¿Qué tecnologías utiliza en su empresa? ¿Correo electrónico, web, servidores propios, teletrabajo, dispositivos móviles con información empresarial?
- 2) ¿Mantenemos los sistemas informáticos al día?
- 3) Sistemas de protección de los ordenadores. ¿Dispones de antivirus, cortafuegos o cifrado de discos y equipos?
- 4) Estamos formado internamente en conocer los riesgos del uso de la tecnología
- 5) ¿Tienes alguna política de gestión de contraseñas?
- 6) ¿Qué haces con la información, soportes, y sistemas que no vas a utilizar?
- 7) ¿Cuánto tiempo podría estar tu empresa sin acceso al correo electrónico sin que le supusiera un problema?
- 8) ¿Hago copias de seguridad de equipos y correo? ¿Cada cuanto?
- 9) ¿Que servicio de mail utilizo? ¿Gratis, en servidor propio, contratado a una empresa de servicios?
- 10) ¿Cuánto tiempo podría estar tu empresa sin web sin que le supusiera un problema? ¿Cada cuanto se actualiza la herramienta de gestión de contenidos?
- 11) ¿Cuánto tiempo podría estar tu empresa con los sistemas caídos que le supusiera un problema? ¿Hago copias de seguridad de los sistemas?
- 12) ¿Se realizan conexiones remotas a los sistemas? ¿Quién lo gestiona?
- 13) Tienes un plan B por si ocurre algún desastre que impida utilizar sus sistemas de información



2- Identificación y gestión de riesgos OPCIONES DE GESTIÓN

- 1) ELIMINAR
- 2) MITIGAR
- 3) ASUMIR
- 4) TRANSFERIR

Modelo de Cálculo de Riesgo





3- Principales riesgos. El correo electrónico

A. Tipos de correos fraudulentos

- A. Phising
- B. Scam
- C. Sextorsion
- D. Malware

B. Detección de correos fraudulentos

- A. Remitentes desconocidos
- B. Remitentes falseados
- C. Ingenieria social
- D. Comunicaciones impersonales
- E. Adjuntos maliciosos
- F. Mala redacción
- G. Enlaces falseados

C. Otros riesgos





3- Principales riesgos. El correo electrónico TIPOS DE CORREOS FRAUDULENTOS

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. Infórmate 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 silios 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

GDT Guardia Civil @GDTGuardiaCivil

#NiCaso a este mensaje que circula por #Whatsapp. Suplantando 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

Romamos la relación ciudadana y máxima función de este mensaje

¡Compártelo en tus grupos de WhatsApp y en tus Redes Sociales

¡¡PUEDES SALVAR VIDAS!!

Es muy importante que siga las medidas de protección recomendadas:

MERCADONA 18 agosto 2015

¡Gana compras GRATIS en Mercadona!

¡Participa en esta encuesta de 1 minuto para conseguir

FALSO

SI NO

€150 VALE

Llama 806 535 455

paypal.hilfeservice.com/de/news/dp/B0028YZ758/ref=sr_2_home&locale/sicherheit/umstellung

PayPal

PayPal, Inc. (US) https://www.paypal.com/at/cgi-bin

Mein Konto Übersicht Geld ein Kreditkarte hinzu Fügen Sie Ihrem PayPa jederzeit sicher und sch Geben Sie nachfolgend

Startseite Privatkunden Geso

Willkommen bei PayPal!

Neu anmelden



3- Principales riesgos. El correo electrónico

DETECCIÓN CORREOS FRAUDULENTOS

De: Banco <jose ramos@cochesymotos.es> **Remitente desconocido, no coincide con la entidad**

Asunto: Tu cuenta ha sido bloqueada

BANCO

Hola cliente,
Tu cuenta ha sido bloqueada.
Motivo: alta de información. **Ingeniería social, genera situación de alarma**

Detalles:
Falta información personal.
Falta información de facturación.
Falta información de la tarjeta de crédito. **Faltas de ortografía, una entidad legítima no las tendría**

Haga clic en el enlace y siga los pasos para desbloquear su cuenta.

ENVIAR PETICION **Enlace, una entidad legítima no pone enlaces**

Este mensaje va dirigido, de manera exclusiva, a su destinatario y puede contener información confidencial y sujeta al secreto profesional, cuya divulgación no está permitida por Ley. **Firma de correo distinta a la habitual**



3- Principales riesgos. El correo electrónico DETECCIÓN CORREOS FRAUDULENTOS


De Movistar - Telefónica <shop@ginzanso.jp>
Asunto **Información de interés sobre su factura móvil**

Estimado cliente,
Su cuenta Movistar.es se encuentra suspendida en estos momentos , por favor asegurese de actualizar todos sus datos.
Por favor, haga clic abajo para activar su cuenta.
Activa tu cuenta ahora:
<https://correo.movistar.es/telefonica/appsuite/#!/!&app=io.ox/mail&folder=default0/INBOX>
Gracias,
Garcia Roche Loma
Departamento de Seguridad de Telefonica.

Nómina - RRHH

jo [redacted] <su [redacted]@gmail.com>
To jo [redacted]

i This message has extra line breaks.

 Nomina.zip
408 bytes

Buenos días,
Adjunto su nómina del último mes.
Se ha cambiado el formato y es necesario ejecutar el archivo incluido para su visualización.
Gracias
Arribas - RRHH

[URGENTE] Actualización de Datos

jo [redacted] <su [redacted]@gmail.com>
To jo [redacted]

i We removed extra line breaks from this message.

Buenas tardes a todos,
Se ha producido una filtración de datos y es necesario cambiar las contraseñas del portal corporativo inmediatamente.
[https://bit.ly/2 \[redacted\]tFr](https://bit.ly/2 [redacted]tFr)
Es obligatorio para todos los empleados.
Muchas Gracias
Pilar Salgado - CEO



COMO DETECTAR UN CORREO MALICIOSO



3- Principales riesgos. El correo electrónico

DETECCIÓN CORREOS FRAUDULENTOS

De: Centro de Atención Mercantil Commercebank <drest@blu.ben.cn> 1

Para: Destinatarios no revelados. 2

Responder-a: atencionalcliente@email.com 3

Asunto: 4 Solicitud de información urgente. ¡Responda ahora !! 5

Su cuenta necesita atención inmediata. 6

Por favor proporcione la siguiente información lo antes posible para evitar que su cuenta sea cerrada ora mismo.

8 Presione aquí para saber más acerca de su cuenta. 7

Número de Seguro Social: _____

Si Usted tiene una cuenta en línea, también necesitaremos obtener de usted la siguiente información. 9

Nombre de usuario de su Banca En-línea: _____

Contraseña de Banca En-Línea: _____

Mercantil Commercebank Servicio al Cliente 10



3- Principales riesgos. El correo electrónico OTROS RIESGOS CORREO ELECTRÓNICO

- CC y CCO
- Función de autocompletado
- Descarga automática de imágenes



4- PROTECCIÓN DE LA INFORMACIÓN. BACKUPS

- A. ¿Dónde guardo mi información?
- B. ¿Que información copiar?
- C. ¿Cada cuanto tiempo?
- D. ¿Dónde almacenar la copia?
- E. ¿Que tipo de copia elegir?
- F. La estrategia 3-2-1.





5- PROTECCIÓN BÁSICA DEL ENTORNO DE TRABAJO (II)

- A. Software legítimo.
- B. Reporte incidentes seguridad.
- C. Dispositivos extraíbles.



5- PROTECCIÓN BÁSICA DEL ENTORNO DE TRABAJO (III)

h) CONTRASEÑAS. GESTIÓN Y BUENAS PRÁCTICAS





5- PROTECCIÓN BÁSICA DEL ENTORNO DE TRABAJO (IV)

I. DISPOSITIVOS MÓVILES

- RIESGOS Y MEDIDAS DE PROTECCIÓN





5- PROTECCIÓN BÁSICA DEL ENTORNO DE TRABAJO (V)

A. TELETRABAJO SEGURO

- ACCESO SEGURO
- ENTORNO SEGURO



6- GESTIÓN DE INCIDENTES Y CONTINUIDAD DE NEGOCIO

OBJETIVO:

- 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





6- GESTIÓN DE INCIDENTES Y CONTINUIDAD DE NEGOCIO

PLANIFICACIÓN PRE-CRISIS IT



Condiciones del disparo. Es decir, qué situación límite debe darse para que declaremos una situación de crisis. En este caso tendremos en cuenta especialmente los MTDs de los procesos críticos.



Flujos de toma de decisiones.



Medios para la declaración de la situación



Personal responsable de activar el Plan de Crisis y gestionarlo.



Teléfonos y datos de contacto del personal implicado en la gestión de la crisis.



Niveles de priorización en la recuperación de la infraestructura de la organización.

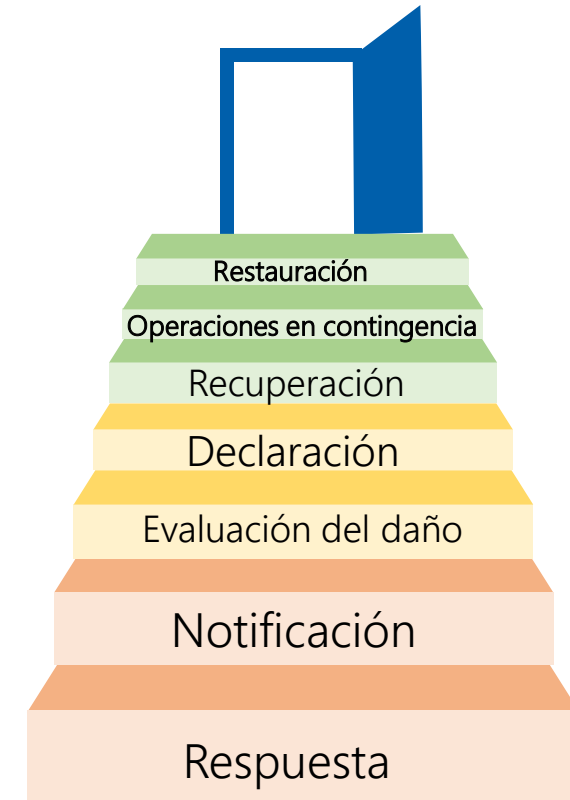


Requisitos temporales de puesta en marcha.



Planes Operativos existentes y personal responsable de su activación.

FASES DE GESTIÓN DE INCIDENTES



Evento de seguridad



7- DECÁLOGO RESUMEN

1. Comprende y gestiona tus riesgos
2. Ten actualizado tu software
3. Protege tu red
4. Instala defensas contra el malware
5. Gestiona los accesos a tu sistema
6. Controla tus dispositivos extraíbles
7. Monitoriza tus redes y servicios
8. Sensibiliza a todos los usuarios
9. Controla los dispositivos móviles de los trabajadores
10. Gestiona los incidentes y la continuidad de tu negocio

MUCHAS GRACIAS



Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa