OFICINA Acelera pyme

CIBERSEGURIDAD : RETOS Y SOLUCIONES

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA SEGUNDA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"
FREMM
Federación Regional de Empresarios del Metal Murcia

Junio 2022

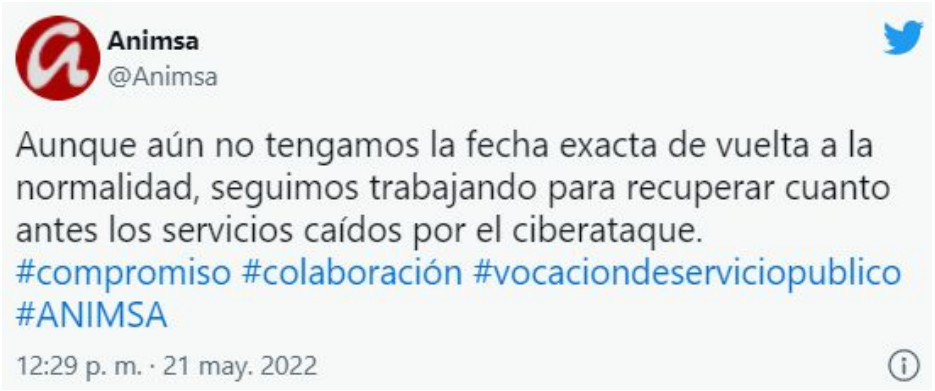
Esta universidad cierra tras 157 años por un ransomware: sobrevivió guerras mundiales y grandes crisis pero no a esto

"El Lincoln College fue víctima de un ciberataque en diciembre de 2021 que frustró las actividades de admisión y obstaculizó el acceso a todos los datos institucionales" y eso paralizó el proceso de inscripción respecto a la segunda mitad de 2022. Todos los sistemas necesarios para el reclutamiento, la retención y los esfuerzos de recaudación de fondos acabaron inoperables"

VER PUBLICACIÓN COMPLETA

Los ayuntamientos navarros llevan 13 días caídos: un ransomware ha dejado a toda la administración como hace 20 años

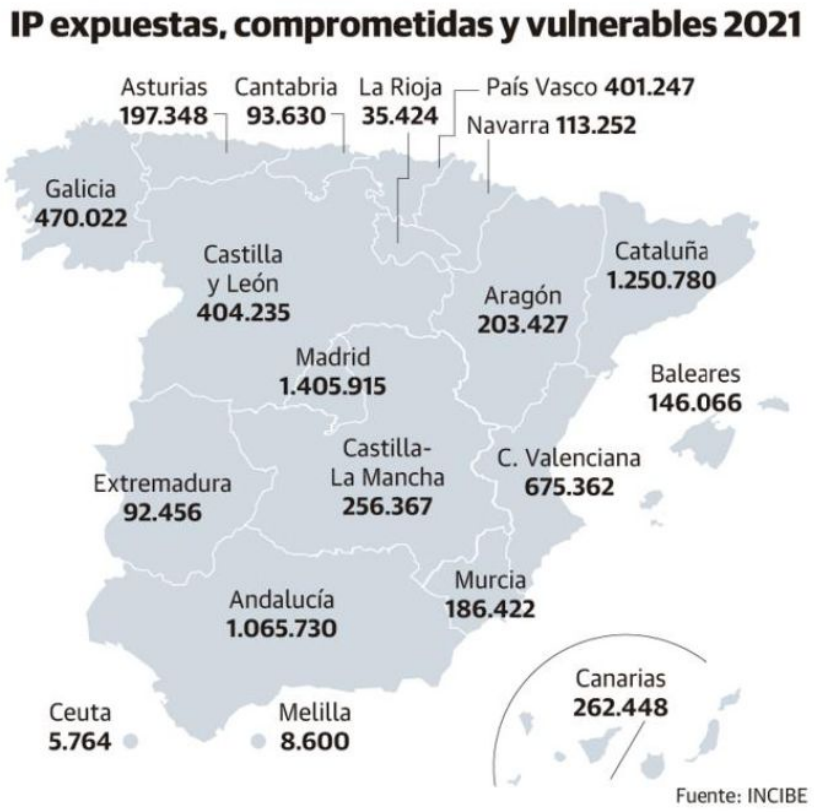
Un ataque informático contra la red de ANIMSA en Navarra (Asociación Navarra de Informática Municipal, empresa pública que gestiona los servicios online de 179 entidades de la Comunidad foral), ha llevado a muchísimos ayuntamientos y entidades públicas a verse forzadas a trabajar fuera de la red desde hace varios días.



VER PUBLICACIÓN COMPLETA

ESCUDO CIBER

Los ciberataques se disparan en Asturias: casi 200.000 intentos de pirateo informático en 2021



«Es una de las regiones con mayor número de incidentes», advierte el Incibe, que urge a la concienciación de toda la sociedad para protegerse

«Nunca había sido tan popular la importancia de la ciberseguridad»,

VER PUBLICACIÓN COMPLETA

ESCUDO CIBER

DE LA CIBERSEGURIDAD AL CIBERSEGURO

LA NUEVA GENERACIÓN DE RIESGOS QUE PUEDEN ARRUINAR A UNA EMPRESA O A UN PROFESIONAL

Hace 15 años los riesgos más preocupantes eran los daños de Incendio, Inundaciones, Catastróficos… o las reclamaciones como Responsabilidad Civil Profesional , Patronal, D&O.

Hoy nos enfrentamos a una generación nueva de riesgos que pueden perfectamente llevar a la ruina a cualquier Pyme y profesional autónomo, derivados de la vulnerabilidad de los sistemas informáticos que contienen datos de los clientes y vitales para el devenir del negocio:

- Sanciones , reclamaciones , gastos legales , notificaciones , extorsiones , pérdida de fondos , interrupción del negocio , reputación…

Veamos dos casos reales y sus efectos en una Pyme

ESCUDO CIBER

CASO REAL 1: TODO EMPIEZA CON UN LINK EN UN CORREO

Una Pyme que se dedica a servicios, que factura **2.500.000€** y tiene datos de 3.000 clientes, datos de salud incluidos, ve como todos sus datos han quedado encriptados de la noche a la mañana. Nadie sabe cómo ha sucedido, aunque siempre hay alguien en la empresa que sabe que no debía haber abierto ese enlace que venía un correo que le urgía a abrir ese enlace para aprovechar una promoción.

Lo cierto es que al intentar abrir los archivos surgen unas instrucciones claras donde se insta al pago de un rescate para liberar los datos: 1 bitcoin, unos **35.000€**

Rápidamente el Responsable de Administración que hace las veces de puente con la empresa de servicios IT, les informa y les pide soluciones alternativas. La empresa de IT les dice que la copia de seguridad más actualizada es de hace un mes, que claro ellos ya les dijeron que reducir las copias a una vez al mes no era buena idea (pero claro el coste se reducía en un 25%).

La perspectiva es perder los datos de un mes de trabajo. Reconstruir los datos son 480 horas, es decir, un coste de **14.400€** como mínimo. La empresa de servicios IT es también quien les ha gestionado la LOPD con un departamento especializado en la materia. Este departamento se pone en contacto con el Responsable de Administración: hay que notificar la brecha de seguridad a la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, y en 72 horas desde que se conocieron los hechos.

ESCUDO CIBER

CASO REAL 1: TODO EMPIEZA CON UN LINK EN UN CORREO

Asimismo, es obligatorio notificar a los clientes afectados por la brecha de seguridad. En este caso los 3.000 clientes (900 de ellos personas físicas de una asociación). El coste de la notificación es de 3,5 euros por cliente, es decir **10.500€.** Llegados a este punto tenemos un coste de **24.900€**, asumiendo que se paga el rescate como mal menor. Pero esto no ha hecho más que empezar.

Una semana después de comunicar a la AEPD, llega un escrito de ésta, donde la AGENCIA notifica que se abre expediente sobre la brecha de seguridad y la vulneración de los datos de los clientes, personas físicas en su mayoría. La sanción propuesta es de **25.000€**

A las dos semanas de la notificación llega un burofax de un despacho de abogados especializado en Demandas Colectivas, informando que 900 clientes afectados por la violación de seguridad y de privacidad de sus datos interponen demanda. Reclaman **200€** por afectado, es decir, **180.000€**

Resumen y conclusiones:

Con un protocolo de seguridad en la gestión del correo electrónico se habría evitado la encriptación: https://www.escudociber.com/best-practices/

Las copias de seguridad se deben hacer a diario.

El coste es de 229.900€, contratar el seguro cuesta = 1.626,48€

ESCUDO CIBER

CASO REAL 2: DOS MESES PLANEANDO LA ESTAFA

En este caso tenemos una Pyme del sector industrial que factura **4.000.000 €.** Tiene 3 proveedores principales de materias primas. Con uno de ellos, Proveedor X hay una relación especialmente buena en lo profesional y en lo personal entre los dos Directores Generales.

La cuestión es que un hacker entra en los servidores de la Pyme donde están instaladas todas las aplicaciones fundamentales para desarrollar la actividad: correo, datos, software especializado, etc.

Durante dos meses observa con detalle la actividad de correo y los procesos de gestión de facturas, relación con los proveedores, flujos de trabajo, y todo lo que le parece pertinente para hacerse una idea clara de donde mejor dar “el golpe”.

Llega a la conclusión que la relación del Director General de la Pyme con el Director General del Proveedor X es la clave para el éxito de la estafa. Y la oportunidad llega de forma natural. La Pyme recibe un encargo importante de un cliente, unos **200.000€.**

Para acometer el pedido la Pyme necesita urgentemente acopio de materiales que son los que el Proveedor X le suele suministrar. El Director General de la Pyme le solicita directamente al Director General de Proveedor X el pedido y le pide ya una proforma de factura con el pedido. El Director General de Proveedor X le indica que dada la cuantía y la urgencia del pedido necesita facturarlo antes de acometerlo. Le hace llegar esta proforma, con **92.367€** de importe. El Director General de la pyme acepta el importe y le pide que le mande la factura.

CASO REAL 2: DOS MESES PLANEANDO LA ESTAFA

El hacker se da cuenta de que es ahora o nunca. Crea un dominio nuevo al que llama ProvedorX, es decir, quita una "e" del nombre ProveedorX.
A su vez conoce bien el nombre del Director General de Proveedor X. Crea un correo nuevo: Director.General@ProvedorX.com
Manda con este correo la factura perfectamente falsificada al Director General de Pyme. Lo único que cambia es la cuenta corriente de pago.
El Director General de Pyme le pide a su Director Financiero que la pague de inmediato, que es urgente para poder recibir los materiales.
A toda prisa el Director Financiero paga la factura a la cuenta indicada en la misma.
Y le confirma el pago al Director General que respira aliviado.
A los dos días llega la factura original de Proveedor X. Y se descubre la estafa.

Los **92.367€** han volado gracias a una elaborada y planificada ingeniería social, ejecutada de forma sencilla y eficaz.

Resumen y conclusiones
Debe existir un protocolo específico para la transferencia de fondo: llamada al proveedor, certificación de titularidad , y doble firma por parte de dos personas de la empresa.
Debe existir un protocolo sobre las buenas prácticas con el correo electrónico, donde una revisión del dominio de correo es fundamental. Más aún con colaboradores habituales y siempre en relación a facturas.

El coste es de 92.367€, contratar el seguro cuesta =1.953,02€

ESCUDO CIBER

COBERTURAS DE UN CIBERSEGURO

- Interrupción del negocio
- Incidente cibernético
- Responsabilidad por eventos de Seguridad en la red
- Costes de remediación
- Pérdidas causadas a terceros por transmisión de vírus, malware o ransomware
- Violación de la seguridad de los datos personales
- Multas y sanciones impuestas por cualquier banco o la industria de tarjetas de pago
- Evento de responsabilidad de medios
- Cobertura de Hacking Telefónico
- Cobertura de reemplazo de hardware (Bricking)
- Cobertura adicional por Fraude por Transferencia de Fondos (opcional)

¿QUÉ TIENE DE ESPECIAL ESCUDO CIBER?

avast CloudCare™

exsel

Incluye todas las coberturas del mercado, siendo opcional contratar el Fraude por Transferencia de Fondos.

El único que incluye un sistema **Gratuito*** de protección de gran calidad como es el **Avast Cloud Care** (antivirus, anti malware, backup en la nube).

*El coste de mercado de Avast Cloud Care es de 50€ al mes

ESCUDO CIBER

¿QUIERES SABER SI ERES ASEGURABLE EN CIBER?

Este es tu check list

NIVELES SEGURIDAD BÁSICOS

√ ¿Despliega antivirus y firewalls corporativos en todas las pasarelas externas y una aplicación antivirus corporativo en toda su red, incluidos los servidores o los endpoints?

√ ¿Usted (o su proveedor externo) realiza una copia de seguridad de los datos críticos al menos cada 7 días?

√ ¿Esta copia de seguridad se almacena en un entorno que está completamente separado de su red y se prueba al menos cada 180 días para verificar su integridad?

¿QUIERES SABER SI ERES ASEGURABLE EN CIBER?

Este es tu check list

√ ¿Instala parches críticos dentro de los 30 días posteriores al lanzamiento?

√ ¿Protege con contraseña todos los medios portátiles, incluidos los teléfonos inteligentes y las tarjetas de memoria?

√ ¿Usted (o un proveedor externo en su nombre) procesa, almacena o transmite datos de tarjetas de pago?

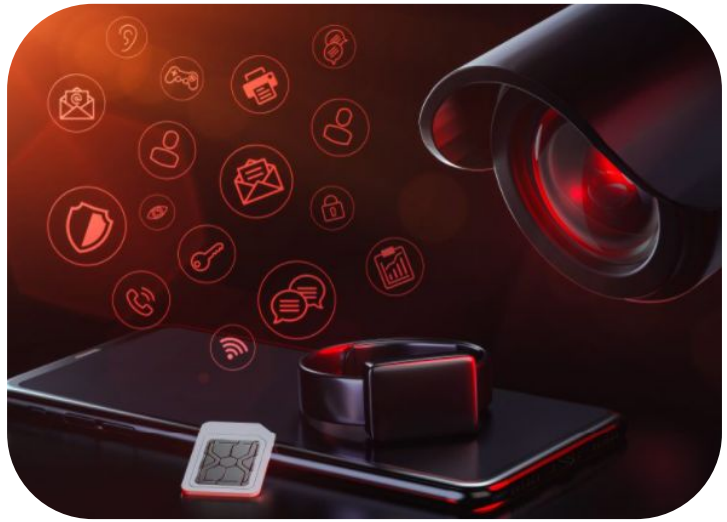
√ ¿Ha sufrido alguna pérdida o se ha presentado alguna reclamación en su contra o tiene conocimiento de algún asunto que sea razonablemente probable que dé lugar a alguna pérdida o reclamación en los últimos 36 meses en los que buscaría una indemnización de nuestra póliza de seguro cibernético?

ESCUDO CIBER

exsel

https://www.exseluwa.com

¡El futuro es seguro, te mostramos cómo!



CUESTIONARIO ESCUDO CIBER FREMM

https://www.escudociber.com/

ESCUDO CIBER