TECH CONSULTING

Consciencia en Ciberseguridad
RGPD Y CIBERSEGURIDAD
¿Sólo para los grandes?

GENERALITAT VALENCIANA

IVACE INSTITUT VALENCIÀ DE COMPETITIVITAT EMPRESARIAL

UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

CEEI ALCOY VALENCIA

¿Qué tal tu día?

ME

LA VANGUARDIA

Ciclismo Sigue minuto a minuto la undécima etapa del Giro de Italia

Multa de 300.000 euros por tirar a la basura datos clínicos

Un total de 158 historiales acabaron en un contenedor de Sevilla

VÍCTOR BEJARANO
27/08/2010 00:37 | Actualizado a 27/08/2010 08:27

No garantizar la privacidad de los **datos médicos** de pacientes puede acarrear fuertes **sanciones**. Una sociedad médica tendrá que abonar una multa de 300.000 euros por tirar a la basura 158 **historias clínicas** de pacientes de ginecología con antecedentes y tratamientos recibidos en el **hospital** del Sagrado Corazón de **Sevilla**. La elevada sanción fue impuesta por la Agencia Española de Protección de Datos y ha sido confirmada por el **Tribunal Supremo**. Este organismo consideró "muy grave" la falta cometida en la clínica contra lo establecido por la ley orgánica de **Protección de Datos**.

La Agencia abrió en el 2004 expediente contra la Sociedad Tocoginecológica Doctor Chacón después de ser hallados los expedientes médicos en un contenedor de basura. Los documentos recogen

Más noticias

Nadal - Dzumhur, en directo

Bélgica rechaza entregar a España a los exconsellers Comín, Puig y Serret

Marsella - Atlético: Previa de la final de la Europa League, en directo

¿Sabes qué es el Watsu? Descubre los beneficios de esta experiencia en el agua

PROTECCIÓN DE DATOS

Primera multa de la AEPD a un particular por difundir imágenes por WhatsApp grabadas en vía pública

La Agencia Española de Protección de Datos (AEPD) determina en su resolución que la mera captación de imágenes de las personas o su difusión a través de WhatsApp puede considerarse un tratamiento de datos personales a efectos de la normativa. Impone una sanción de 2000 euros al denunciado.

Un policía local denuncia ante la AEPD a un particular que grabó desde su casa unas imágenes suyas en la vía pública. A pesar de que el funcionario pide al denunciado que cese en la grabación, no sólo ignora tal requerimiento, sino que difunde estas imágenes por WhatsApp. El denunciado alega que la grabación se efectúa por motivo de una agresión machista que estaba teniendo lugar en la vía pública, y la actuación de la policía local en el desarrollo de sus competencias profesionales.

_RGPD

_RGPD

- Los siete principios fundamentales del Privacy by Design son los siguientes:
- 1.- Protección Preventiva y Proactiva.
- 2.- Privacidad “por Defecto”
- 3.- Privacidad integrada en el Diseño
- 4.- Funcionalidad Plena “Win-Win” en lugar de “Suma cero”
- 5.- Protección durante todo el Ciclo Vital: “End to End”
- 6.- Visibilidad y Transparencia: “Trust but Verify”.
- 7.- Respeto y Empoderamiento del Usuario. El Usuario en el Centro. “User-centric”
- By Ann Cavoukian 20 años de antigüedad.

_RGPD

¿Qué tenemos ahora con la LOPD?

- Obligaciones para cualquier empresa/autónomo.
- Sanciones desde 900 € hasta 600000 €.
- 10571 denuncias y 17 millones € en sanciones.
- Un elevado cumplimiento pero no efectivo.
- Nuevo reglamento por tanto nueva partida.

RGPD

El Nuevo Reglamento

Introducción.

- Aplicación a partir del **25 de mayo de 2018** – 8 MESES

- **MOTIVOS:**
  - Incremento del intercambio de datos (cambios tecnológicos)
  - Necesidad de un marco normativo único para toda la UE.

- **OBJECTIVOS:**
  - Dar más garantías de control al ciudadano.
  - Simplificar la regulación.
  - Medidas especificas para los grandes de internet.
  - Libre circulación de datos personales en la UE.
  - Establecer reglas claras para la transferencia internacional de datos.

BUROCRACIA VS CULTURA EMPRESARIAL

LOPD VS RGPD

_RGPD

LOPD

Datos nivel
BÁSICO

Datos nivel
MEDIO

Datos nivel
ALTO

MEDIDAS A APLICAR SEGÚN EL TIPO DE DATOS TRATADOS

RGPD

- NO ESTABLECE NIVELES DE DATOS.
- NO ESPECIFICA MEDIDAS PARTICULARES A NIVEL TECNICO.
- SE SIGUEN CONSIDERANDO DATOS 'ESPECIALMENTE SENSIBLES'.
- SE AÑADEN NUEVOS CONCEPTOS (datos biométricos, genéticos, …)

_RGPD

LOPD

- Notificación de ficheros a la AEPD.

RGPD

- DESAPARECE OBLIGACIÓN NOTIFICAR FICHEROS.
- HASTA MAYO 2018 SIGUE SIENDO OBLIGATORIO.
- SE SUSTITUYE POR EL ‘REGISTRO DE ACTIVIDADES DE TRATAMIENTO’.

_RGPD

LOPD

- Disponer de un **documento de seguridad**.

- ✓ Estructura de los ficheros.
- ✓ Escenario informático.
- ✓ Usuarios por áreas y accesos.
- ✓ Inventario de dispositivos.
- ✓ Protocolos (E/S, incidencias).

RGPD

- SE PUEDE ENGLOBAR DENTRO DEL REGISTRO DE ACTIVIDADES.

_RGPD

LOPD

- Firmar **compromisos de confidencialidad**.

  ✓ Con trabajadores + MANUAL USUARIO

  ✓ Con terceros con acceso a datos (*encargados de tratamiento*)

RGPD

- SE AMPLIA EL CONTENIDO DEL CONTRATO CON ENCARGADOS DE TRATAMIENTO.
- DESCRIPCION DETALLADA SERVICIOS PRESTADOS, MEDIDAS APLICADAS, POSIBLES TRANSFERENCIAS INTERNACIONALES, SUBCONTRATACIONES, …

_RGPD

LOPD

- Incluir <u>cláusulas y avisos legales</u>.
  - Facturas.
  - Presupuestos.
  - Contratos.
  - Impresos.
  - Correo electrónico.
  - Uso de imágenes.
  - Recogida de datos.
  - Cartel de video vigilancia.
  - Derechos ARCO.
  - AVISOS LEGALES WEB.

RGPD

- SE AMPLIA EL DETALLE DE LA INFORMACIÓN QUE SE PROPORCIONA AL AFECTADO (base jurídica para el tratamiento, destinatarios de los datos, derechos de los afectados, reclamaciones, …)

- SE PLANTEA INCLUIR ESTA INFORMACIÓN POR CAPAS:

1ª CAPA: Info básica primer nivel de recogida datos.
2ª CAPA: Información adicional detallada.

_RGPD

LOPD

- Implantar **medidas técnico-organizativas**.
  - Claves de acceso para cada usuario.
  - Perfiles de usuario.
  - Copias de seguridad.
  - Inventario de soportes / Registro de salidas.
  - Control acceso físico servidores.
  - Ficheros servidor.
  - Antivirus / Firewall.
  - Auditorias.
  - Cifrado de datos.
  - Registro de accesos.
  - ...

RGPD

- NO ENTRA EN DETALLE EN MEDIDAS TÉCNICAS A APLICAR.
- RESPONSABILIDAD ACTIVA, CONCEPTOS COMO PRIVACY BY DESIGN O BY DEFAULT.
- ANALISIS DE RIESGOS.

_RGPD

- Implantar **<u>medidas técnico-organizativas</u>** (**PAPEL**)
    - Criterios de archivo.
    - Dispositivos de almacenamiento.
    - Destructoras.
    - …

LA LSSICE

La LSSICE (*Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico*) establece obligaciones a:

Regula actividades como:

- Comercio electrónico.
- Contratación en línea.
- Información y publicidad.
- Servicios de intermediación.

SIEMPRE QUE CONSTITUYAN ACTIVIDAD ECONOMICA O LUCRATIVA PARA EL PRESTADOR.

_RGPD

'**AVISO LEGAL**' (art.10 LSSICE): razón social, CIF, datos de contacto, datos inscripción registro, datos profesión regulada, códigos de conducta, ...

'**POLITICA DE PRIVACIDAD**' (LOPD): Informar del tratamiento que se hará de los datos recogidos.

'**POLITICA DE COOKIES**' (LSSICE): Si se utilizan, informar de su uso, finalidad y mecanismo de desactivación.

'**CONDICIONES GRALES. CONTRATACION**' (especificas para cada tienda online).

'CLAUSULA PARA COMUNICACIONES COMERCIALES': Posibilidad de darse de baja.

Otros avisos legales:

- formulario de contacto web
- sección envío CV, etc.
- **términos y condiciones (apps)**

LA LSSICE

'Ley de cookies'

No es una "ley" como a tal sino el texto correspondiente a el artículo 22 de la LSSICE.

- Pedir el **consentimiento** per su utilización. Si se continua navegando se da por aceptado. Con la primera visita es suficiente (sino hay cambios en la política).

-Tipología: analíticas, publicitarias, de seguimiento, técnicas, de personalización, de sesión, de seguridad…

-Mostrar una 'política de cookies' clara y visible que incluya: finalidad, quien las instala y como se pueden desinstalar.

Comunicaciones comerciales vía electrónica

El régimen jurídico de este tipo de comunicaciones se regula en los artículos 19 a 22 de la LSSICE.

El articulo 21.1 LSSICE **prohíbe el envío de comunicaciones comerciales por correo electrónico sin el consentimiento previo y exprés del afectado**.

Además del consentimiento previo, se deberá informar en las comunicaciones sobre la finalidad del tratamiento i el derecho a denegar o retirar el consentimiento; inclusión de una dirección valida.

No es necesario el consentimiento previo si ha existido una relación contractual previa, siempre que se hayan obtenido los datos de forma lícita y se trate de publicidad de productos/servicios similares a los contratados.

Aplicación práctica LOPD

RESUMEN - ¿Qué tiene que tener mi negocio, actividad, web?

- Ficheros registrados a la AEPD (clientes, proveedores, trabajadores, usuarios web, etc.)
- Tener un documento de seguridad actualizado.
- Firmar compromisos de confidencialidad con trabajadores (si hay).
- Firmar acuerdos con encargados de tratamiento externos.
- Incluir cláusulas de información y consentimiento (mail, facturas, documentos, ...).
- Avisos legales web (aviso legal, política privacidad, política cookies, newsletter, etc)
- Atender los derechos ARCO.
- Implantar las medidas técnicas (RD1720/2007).

Errores habituales

- NO tener los ficheros inscritos a la AEPD.
- Tener solo los ficheros, no la documentación al día.
- No atender los derechos ARCO – baja newsletter.
- Realizar la auditoría a través de la 'tripartita'.
- Controlar el correo del trabajador sin informar.
- Pensar: 'yo no trato datos, esto a mi no me afecta'.
- Copiar el aviso legal de otra página web.

El Nuevo Reglamento

Aspectos más relevantes.

- Se **amplia el ámbito de aplicación** a RF i ET no establecidos en la UE.
- **Consentimiento** libre, informado, especifico, inequívoco y para las diferentes finalidades. **Prohibido consentimiento tácito o casillas pre-marcadas en páginas web**.
- **Transparencia en los avisos legales** (leguaje claro y comprensible).
- Clausulas de información y consentimiento por **capas**.
- Se mantienen los derechos **ARCO** pero no plazos de respuesta.
- Se contempla el **derecho al olvido** (supresión) y **portabilidad de datos**.
- Desaparece la obligación de **notificar ficheros** a la AEPD.
- Realizar **evaluaciones de impacto**.
- Notificar '**violaciones de seguridad**' a la autoridad de control y al afectado.
- Aparece la figura del **DPO**.
- Sistema de **ventanilla única**.
- Responsabilidad proactiva de las empresas (***privacy by design*** *and* ***privacy by default***).
- Regulación de las **transferencias internacionales de datos**.

- **MULTAS DE HASTA 20 MILLONES DE EUROS o 4% DE LA FACTURACIÓN.**

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS


MISIÓN
CUMPLIDA

_RGPD Y CIBERSEGURIDAD

_CIBERSEGURIDAD

CIBERSEGURIDAD

Hackeo de Equifax: ¿qué puedes hacer?

8 Sep 2017

El pasado jueves 7 de septiembre Equifax, una de las agencias de reporte de crédito más grandes de EE. UU., anunció estar investigando sobre una propia fuga de datos que podría afectar a 143 millones de americanos aproximadamente.

Según lo que dice el comunicado de la empresa, la fuga dio acceso a los siguientes datos:

- Nombres
- Números de la seguridad social
- Fechas de nacimientos
- Direcciones

En algunos casos se pudo acceder también a números de tarjeta de crédito, números de licencia de conducir y otros tipos de datos personales.

Si estás leyendo este articulo sacudiendo la cabeza de decepción, no eres el único.

_CIBERSEGURIDAD

AMENAZAS Y VULNERABILIDADES EN SISTEMAS GENERALES

2013 VS 2017

15000

120000

Información.es » Sucesos y Tribunales »

Estafan más de 83.000 euros a una empresa de Banyeres tras «hackear» su sistema informático

La Guardia Civil detiene a los 2 presuntos cabecillas del fraude y a 2 "mulas", personas que recibían el dinero a cambio de una comisión

P. Cerrada | | 12.10.2017 | 00:33

La Guardia Civil ha esclarecido un **fraude cibernético** de más de 83.000 euros a una empresa de Banyeres de Mariola mediante la conocida como «estafa al CEO», en la que «hackean» el sistema informático de las mercantiles para acceder a datos de clientes y ordenar pagos por supuestos servicios. En la operación han sido detenidos en Alcorcón y Aranjuez a los dos presuntos cabecillas de la estafa y a dos personas en València y El Álamo (Madrid), que fueron las que recibieron las transferencias en sus cuentas a cambio de una comisión, según informó ayer la Comandancia de Alicante.

La investigación fue iniciada por el Equipo de Investigación Tecnológica (EDITE) de la Guardia Civil de Alicante tras tener conocimiento de varias **estafas** a una empresa con sede social en Banyeres de Mariola.

_CIBERSEGURIDAD

Destinada desde pequeños empresarios y autónomos, micro-pymes, pymes a grandes empresas.

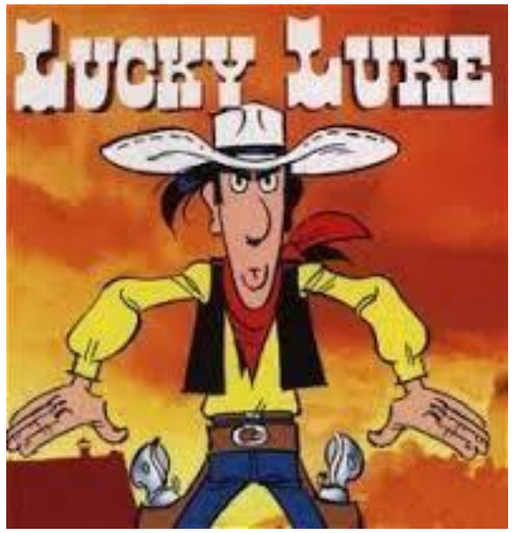
La CiberSeguridad consiste en implantar protocolos de seguridad para ayudar a la empresa a controlar la información y los procesos, salvaguardando el conocimiento de la misma y su entorno.

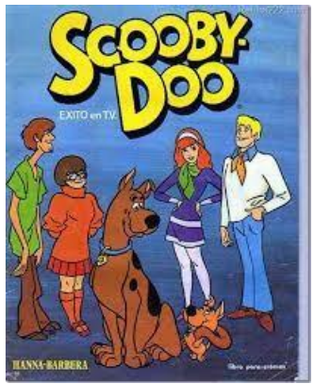
Se implanta mediante consultoría, formación, instalación de Software - hardware y certificación.

_Por qué la Ciberseguridad Industria 4.0

Conocida como la nueva revolución Industrial, La industria 4.0 es la incorporación de sistemas y tecnología a los procesos industriales y de negocio.

_Nuestro Nivel Nativo de Tecnología





_Dependencia

Dependencia Baja

Dependencia Moderada

Dependencia Alta

Se caracterizan por:

- **utilizar PC para realizar el trabajo administrativo** (ofertas, correspondencia,...).
- **utilizar aplicaciones en local para mantenimiento de aplicativos con bases de datos y hojas de cálculo** (clientes, finanzas,...).
- **utilizar internet fundamentalmente para consulta y búsqueda de información.**
- **es posible que utilicen correo electrónico como medio de comunicación con empresas proveedoras y con clientes, pero no es común disponen de servidor de correo.**
- **pueden disponer de una página web informativa** (descarga de documentación, información de contacto, ...) **que generalmente aloja externamente.**
- **utilizar la red de área local o wifi para compartir recursos** (impresoras, discos, acceso a internet...), **pudiendo disponer de un servidor de ficheros.**

_Dependencia

Dependencia Baja

Dependencia Moderada

Dependencia Alta

Se caracterizan por:

- **utilizar herramientas colaborativas en red para gestión del negocio** (gestión de procesos, RRHH, gestión de clientes,...).
- **utilizar internet para el potenciar el negocio** (mailings, publicidad,...) **y para el cumplimiento de las obligaciones con la administración.**
- **disponer de servidores de correo electrónico que se administran localmente o se subcontratar el servicio.**
- **utilizar la red de área local para compartir recursos** (aplicaciones, ficheros,...) **con servidores propios.**
- **su página web cambia con frecuencia de contenidos** (noticias, boletines RSS, catálogo de productos,...) **y puede contener servicios interactivos** (formularios,...).
- **es posible que utilicen dispositivos portátiles para acceso remoto a su red corporativa.**

_Dependencia

Dependencia Baja

Dependencia Moderada

Dependencia Alta

Se caracterizan por:

- **utilizar internet u otras redes para el desarrollo del negocio** (B2B, B2C,...).
- **es posible que dispongan de servicios/productos que se distribuyen y/o venden on-line.**
- **utilizar el intercambio electrónico para el desarrollo del negocio** (contratación, facturación,...).
- **disponer de una intranet** (formación, aplicativos internos,...).
- **formar redes particulares con sus proveedores y sus clientes** (extranets).
- **utilizar herramientas colaborativas basadas en internet.**

_Riesgo

Riesgo	Impacto
Robo de información privilegiada o esencial	Pérdida de ventaja competitiva / comercial
Intrusiones en mis sistemas y acceso a información sensible o confidencial	• Acceso a la información y los datos de mi negocio a través de intrusiones difíciles de detectar • Exponer datos / información confidencial • Impacto reputacional /pérdida de imagen
No ser capaces de restaurar la situación después de un incidente (Resilencia)	Tener una situación desventajosa en un tiempo alargado acentúa el daño (más pérdidas por inactividad). No poder restaurar la situación debidamente pone en riesgo la continuidad de nuestra actividad, con la consiguiente pérdida económica y de imagen.
Estar expuesto a ciberdelincuentes	• Pérdidas económicas por robo/fraude • Impacto reputacional
Ataques a la marca (redes sociales)	• Pérdidas de clientes • Impacto reputacional
Estar expuestos a un ataque cibernético de denegación de servicio (por ejemplo en nuestros servicios web)	• Interrumpir el servicio tanto interno como a cliente (pérdida de ventas) • Impacto reputacional • Incumplimiento normativo o contractual y posibles sanciones

_Incidentes

MALWARE

También llamado código malicioso; incluye virus, gusanos, troyanos, etc.

EXPLOIT

Es un programa que aprovecha una vulnerabilidad de un sistema informático para robar datos o contraseñas de los usuarios, espiar la actividad de los mismos, controlar o modificar la configuración del equipo, entre otros.

ATAQUES DE DENEGACIÓN DE SERVICIO (DOS)

Se entiende como denegación de servicio a un conjunto de técnicas cuyo objetivo es inutilizar un servidor (por ejemplo la web de una empresa).

Un ataque de Denegación de Servicio Distribuido (DDoS) es más sofisticado y permite enviar peticiones coordinadas entre distintos equipos a un mismo servidor para inutilizarlo o «tirarlo».

PHISHING

Este tipo de ataque se realiza comúnmente a través de correos electrónicos (e-mail) donde se intenta convencer a un usuario para que confíe en el contenido del email, con la intención de obtener información (por ejemplo contraseñas o claves de acceso). Este tipo de ataques también puede realizarse a través de WhatsApp, servicios de mensajería, etc.

APT Amenaza persistente avanzada

Amenazas complejas avanzadas y persistentes, a través de ataques coordinados dirigidos a una entidad u organización específica.

_Incidentes

Los tipos de incidentes que nos pueden afectar pueden clasificarse en función de su origen.

_Actores en Ciberseguridad

70%

_Riesgo

RIESGO = PROBABILIDAD (de que se materialice una amenaza) **x IMPACTO**

¿Qué es un riesgo?

1

Contingencia o proximidad de un daño.

Situación provocada por la posibilidad de que ocurran desastres naturales, fortuitos o intencionados. Por ejemplo, daño por agua o fuego.

2

Contingencia que puede ser objeto de un contrato de seguro.

Hechos que provocan consecuencias negativas, cuyo impacto puede ser trasladado a un tercero a través de un contrato de seguro. Por ejemplo, que el cliente aplique una cláusula del contrato.

3

Conjunto de circunstancias que pueden disminuir el beneficio.

Hechos que provocan una disminución de ingresos (beneficios económicos o materiales de un individuo o organización). Por ejemplo, que disminuya el beneficio por falta de actividad.

_Ciber-Riesgo

En el ámbito de la ciberseguridad el riesgo se define por la normativa de aplicación (*) como **la posibilidad de que una amenaza concreta pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información.**

RIESGO

Suele considerarse como una combinación de la probabilidad de un evento (es decir, de que una amenaza aproveche una vulnerabilidad en un activo de información) **y sus consecuencias** (magnitud del daño resultante para el negocio, en términos económicos).

_Ciber-Riesgo

Fase 1

Fase 1: **Definir el alcance del análisis de riesgos**, es decir, dónde vamos a analizar los riesgos. Pueden ser todos los servicios, departamentos y actividades o centrarse en algunos en concreto.

Fase 2

Fase 2: Identificar y valorar los activos de información del departamento, proceso o sistema objeto del estudio.

Fase 3

Fase 3: Identificar las **amenazas** a las que estos están expuestos estos activos.

Fase 4

Fase 4: Estudio y análisis de las características de nuestros activos para identificar **los puntos débiles o vulnerabilidades y las salvaguardas existentes.**

Fase 5

Fase 5: Para cada par activo-amenaza, estimaremos la **probabilidad** de que la amenaza se materialice y el **impacto** sobre el negocio que esto produciría.

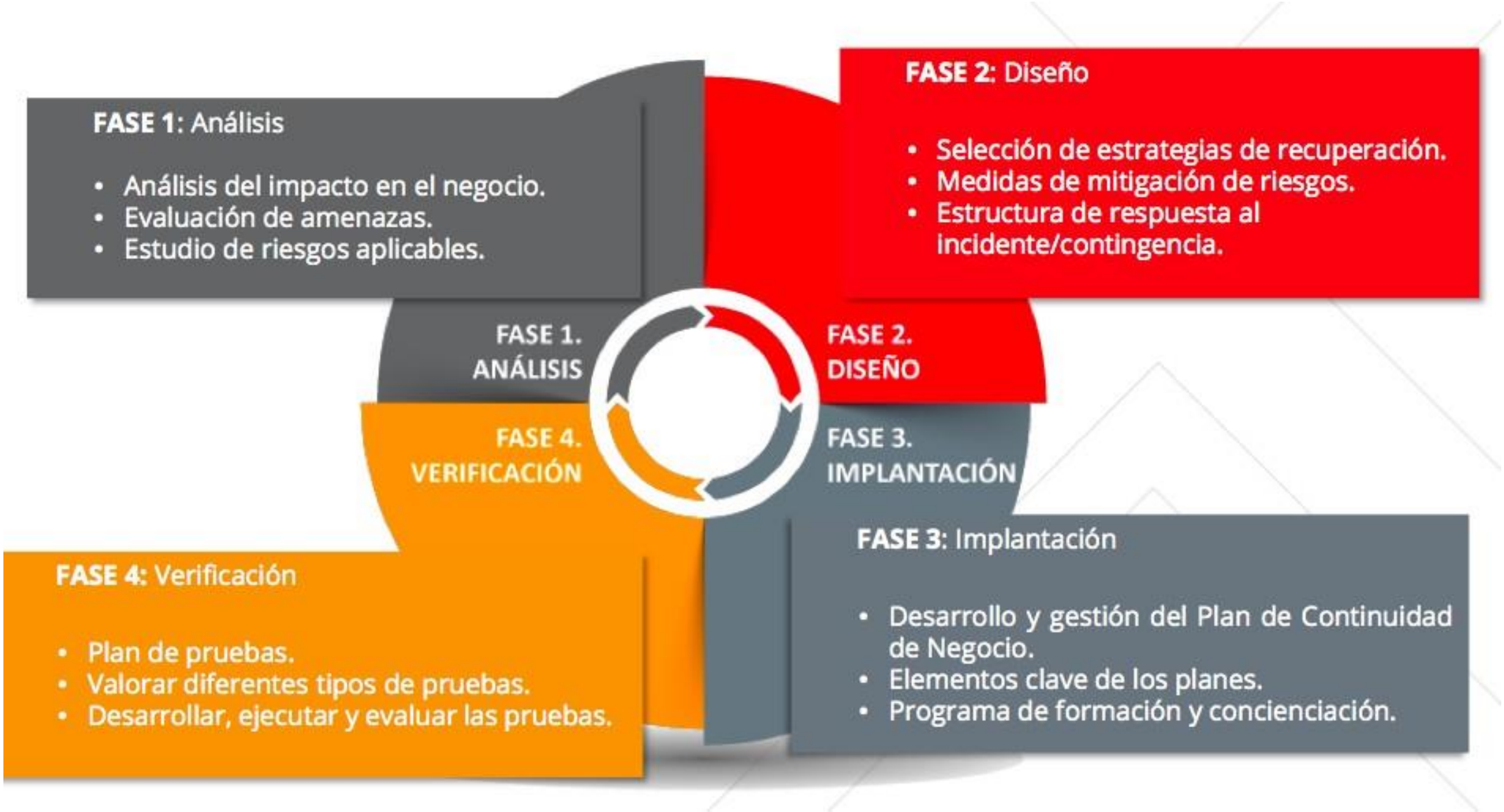
Fase 6

Fase 6: Una vez calculado el riesgo, debemos **tratar aquellos riesgos que superen un límite** que nosotros mismos hayamos establecido.

_Ciber-Riesgo

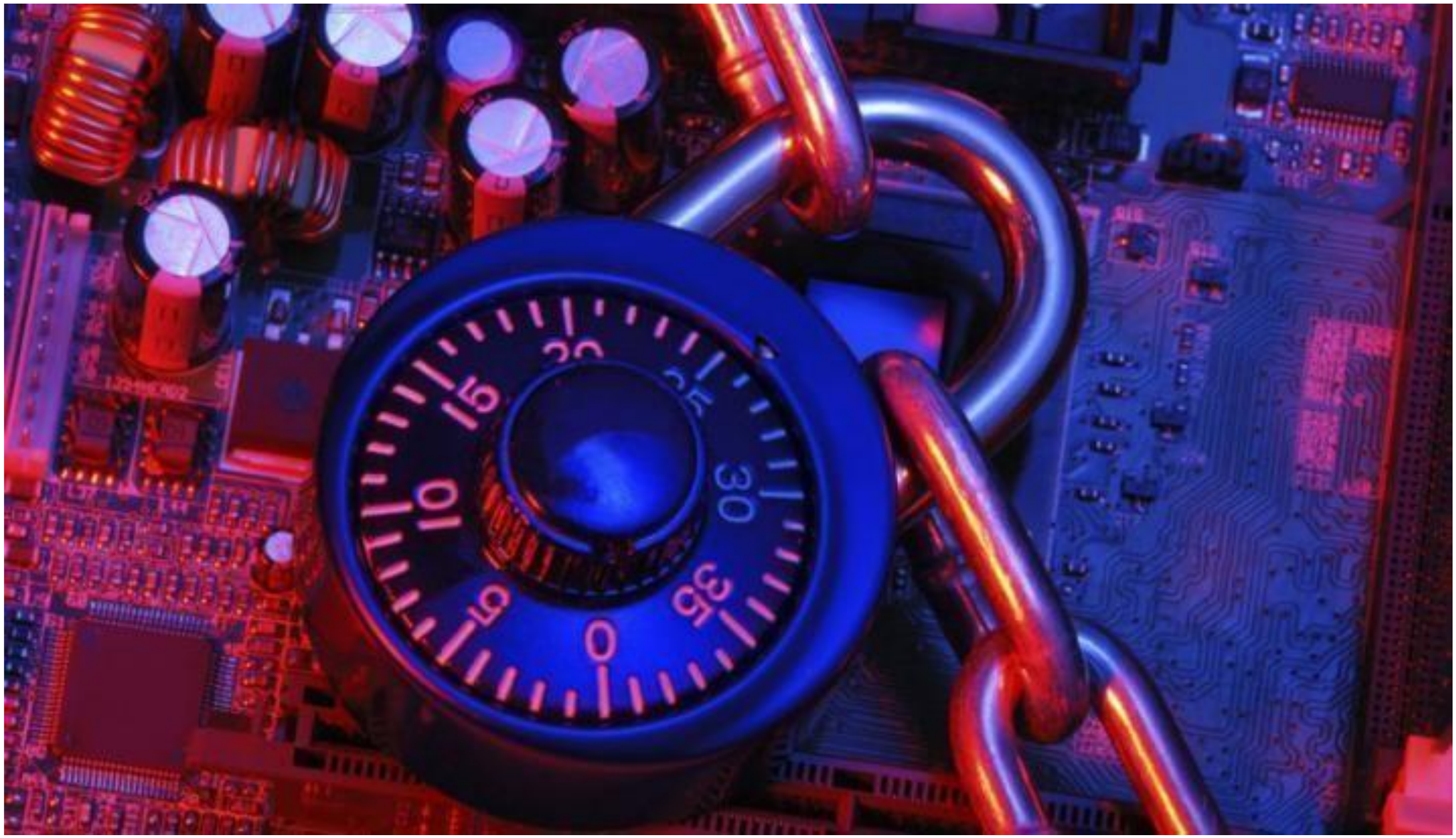
Incidentes más comunes en pymes y el presupuesto medio necesario para solucionarlos:

_Plan de continuidad



_Las tres fases de la ciber

CERRAR PERIMETROS(tic)



_Las tres fases de la ciber

POLÍTICAS INTERNAS (Consultoría)

_Las tres fases de la ciber

CUMPLIMINETO DE LA LEY

- Rgpd
- Compliance Penal
- LSSI

_ Metodología

FASE 0: Pre - Auditoría CiberRiesgo

Esta fase consta de la realización de una pre-auditoría de Ciber- Riesgo donde se extrae la situación actual de la empresa, el punto de partida de la misma, las necesidades actuales inmediatas, a corto plazo y a medio plazo.

FASE 1: Redes y usuarios

La seguridad implantada por fases empieza por controlar la seguridad perimetral de la misma, implantado procesos, sistemas y hardware para poder controlar accesos y salidas de información.

Además en esta fase se implanta si fuere necesario el control de los accesos de información por parte de los usuarios.

FASE 2: Copias de seguridad

Como reza la ciberseguridad, la recuperación ante un desastre es imprescindible, por ello en esta fase se implanta, revisa y optimizan los procesos de copias de seguridad y se crea el protocolo de recuperación de desastres.

_Metodología

FASE 3: Monitorización de usuarios

La monitorización del uso de sistemas, información y servicios TIC de los usuarios es clave para mantener el orden de la información, detectar fugas de información, etc.

Importante recalcar que este proceso también indicará a la empresa el uso de los recursos TIC.

Esta fase es clave fundamental a la hora de evaluación de rendimiento de usuarios, ante problemas de delitos tecnológicos de la empresa (Voluntaria o involuntariamente) y la resolución de incidencias.

FASE 4: Gestión de Riesgos

Desarrollo e implantación de los protocolos de gestión de Riesgos sobre delitos informáticos ligados a la empresa y las resoluciones adoptadas por al empresa.

FASE 5: Protocolos

Desarrollo e implantación de los protocolos de ciberseguridad implantados en la empresa, así como la documentación pertinente.

_Metodología

FASE 6: Auditoria

Realización de auditorias de ciberseguridad de la empresa.
Incluye las fases de pentester realizados por hackers éticos a nómina.

FASE 7: Documento de seguridad

Realización de Documento de Seguridad del sistema de Ciberseguridad de la empresa, bien sea a medida o un SGSI.

FASE 8: Formación

Formación e implantación de los sistemas de Ciberseguridad implantado en la empresa a los responsables.

Jornada informativa a los usuarios para que comprendan el trabajo realizado en la empresa y sus fundamentos.

En esta fase si realizarían, si fuera necesario, las certificaciones de empleados.

El debate

_Otro día más

TECH CONSULTING

GRUPO TECNOLÓGICO MANTIS S.L.