JORNADAS DE SEGURIDAD DE LA INFORMACION EN LAS PYMES

INSTITUTO NACIONAL DE CIBERSEGURIDAD

Comunitat Valenciana
European Entrepreneurial Region 2015

CEEI ELCHE

GENERALITAT VALENCIANA

IVACE

UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional

Una manera de hacer Europa

"Proyecto cofinanciado por los Fondos FEDER, dentro del Programa Operativo FEDER de la Comunitat Valenciana 2014-2020"

Todo el contenido de esta sesión ha sido desarrollado por el Instituto Nacional de Ciberseguridad INCIBE y puesto a disposición y uso de la Asociación Creamos Valor para las Jornadas de Sensibilización en materia de Seguridad de la Información para Pymes.

INDICE

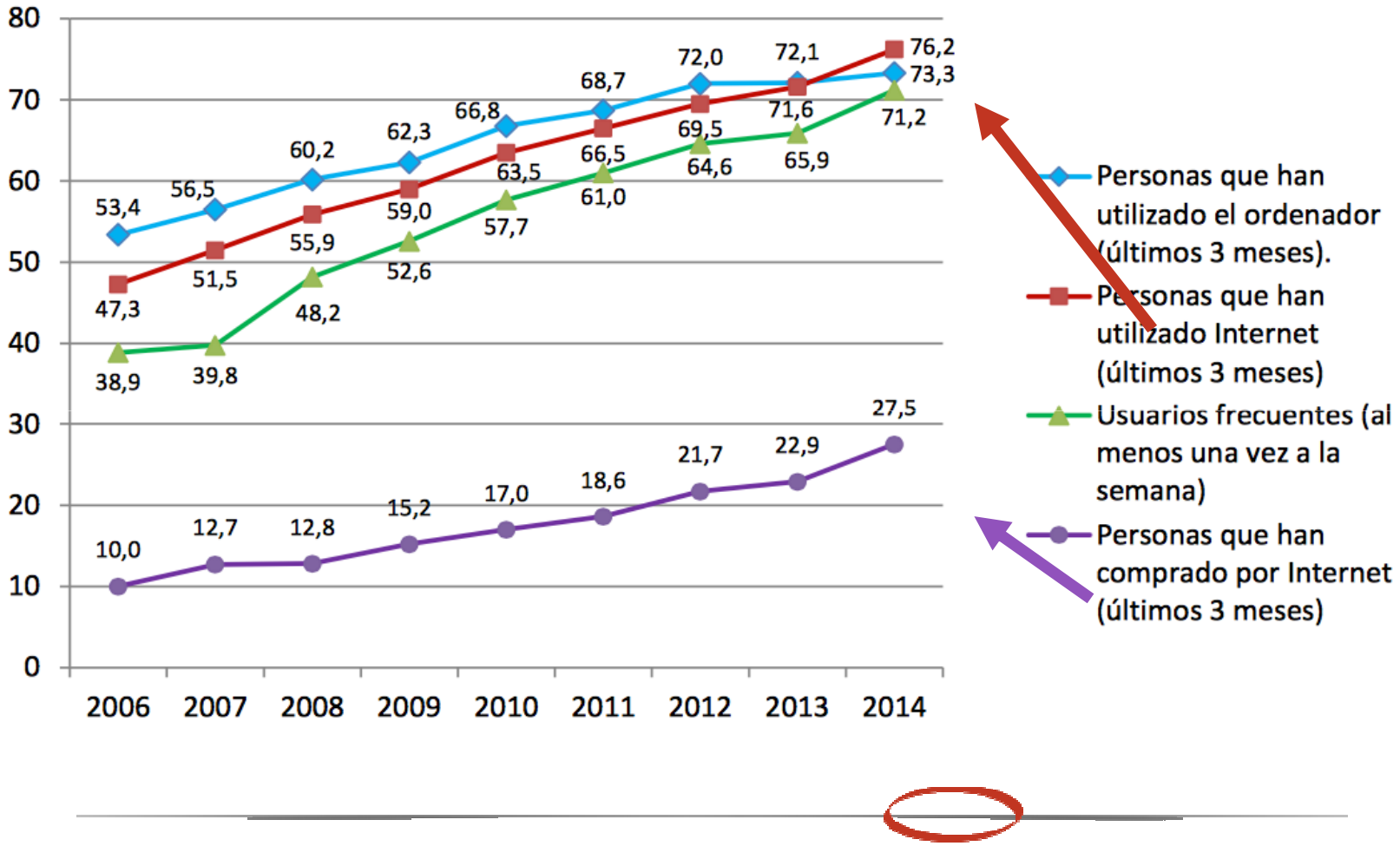
- Introducción.
- La Información.
- Las amenazas.
- Los soportes.
- El puesto de trabajo.
- Los dispositivos móviles.
- Gestión de riesgos en sistemas de información.

INTRODUCCION

En la actualidad se están produciendo importantes cambios en nuestra sociedad relacionados con las tecnologías de la información que afectan a todos los ámbitos de la sociedad, como el económico, el tecnológico o el normativo. Estos cambios también han modificado el concepto de Seguridad de la Información.

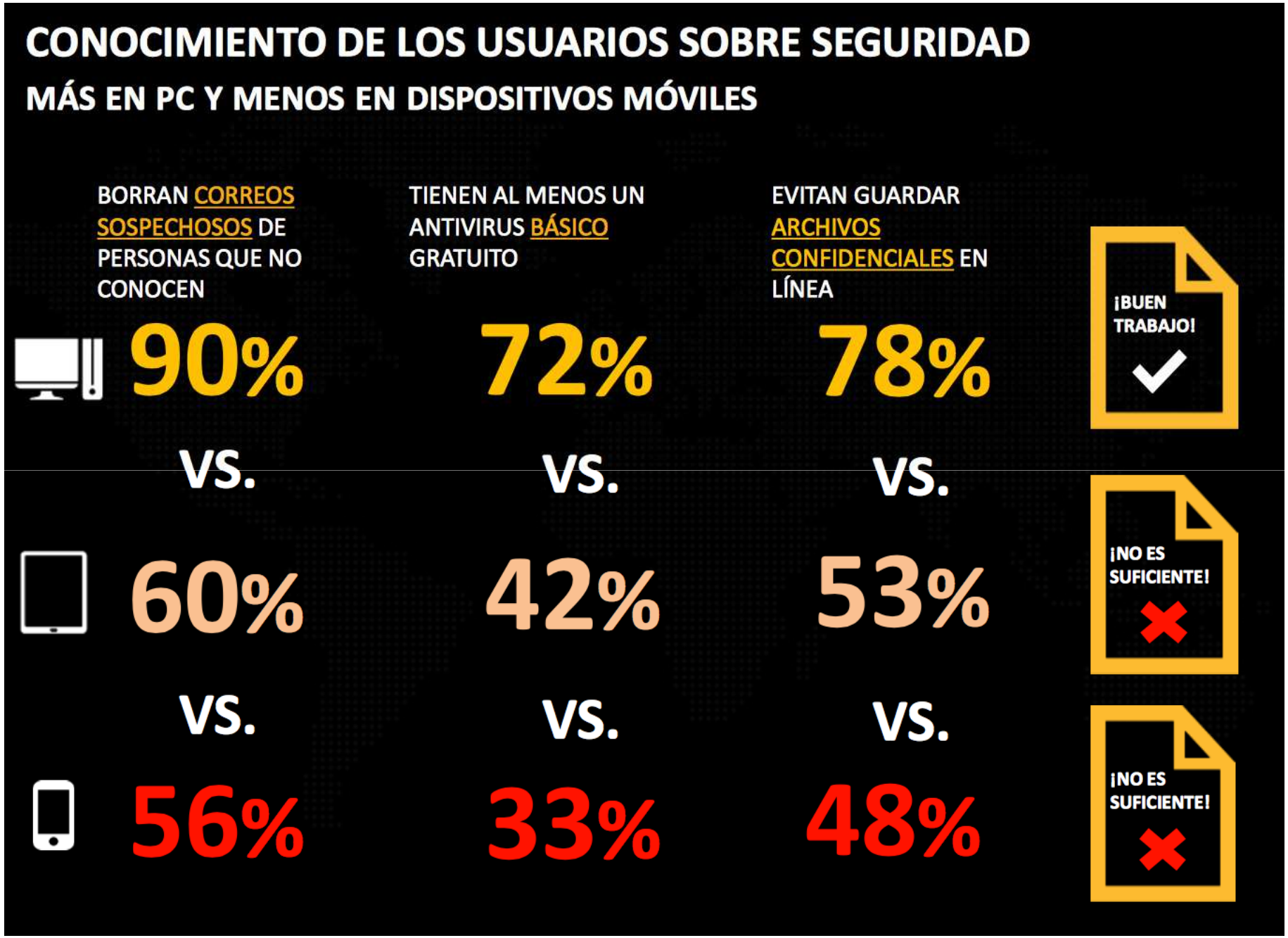
Evolución del uso de TIC por las personas de 16 a 74 años

Serie homogénea 2006-2014. Total nacional (% de personas)



Para comprender qué es la seguridad de la información, en primer lugar, debemos conocer que la información en este área es referida a los activos de información (es decir, los datos por supuesto, pero también los equipos, las aplicaciones, las personas, que se utilizan para crear, gestionar, trasmitir y destruir la información), que tienen un valor para la organización.

CreamosValor


CONOCIMIENTO DE LOS USUARIOS SOBRE SEGURIDAD
MÁS EN PC Y MENOS EN DISPOSITIVOS MÓVILES
BORRAN CORREOS SOSPECHOSOS DE PERSONAS QUE NO CONOCEN
TIENEN AL MENOS UN ANTIVIRUS BÁSICO GRATUITO
EVITAN GUARDAR ARCHIVOS CONFIDENCIALES EN LÍNEA
90%
72%
78%
¡BUEN TRABAJO!
VS.
VS.
VS.
60%
42%
53%
¡NO ES SUFICIENTE!
VS.
VS.
VS.
56%
33%
48%
¡NO ES SUFICIENTE!

ENFOQUE SOBRE SEGURIDAD

La seguridad se puede contemplar desde varios puntos de vista: Seguridad Informática, Seguridad TIC y Seguridad de la Información.

CreamosValor

La Seguridad Informática suele ser la forma más habitual con la que nos referimos a todo aquello que tiene que ver con la seguridad de los ordenadores y los sistemas. Es un término obsoleto.

CreamosValor

Es imprescindible realizar una revisión del enfoque de seguridad y dotarlo de mayor amplitud, como es el caso de la Seguridad TIC o Seguridad de las Tecnologías de la Información y las Comunicaciones

La Seguridad de la Información (SI) tiene en cuenta la protección de la información desde tres puntos de vista: **técnico, organizativo y legal.**

CreamosValor

¿PORQUE ES NECESARIA LA SI?

La Seguridad de la Información (SI) nos ayuda precisamente a identificar los riesgos y las amenazas a las que está expuesta nuestra organización, en qué medida nos pueden afectar y cómo podemos minimizarlas. Y, en el caso de que se produzca algún desastre, nos ayuda a establecer pautas y procedimientos para reducir sus consecuencias.

CreamosValor

La Seguridad de la Información también es un camino para identificar malos hábitos y usos inadecuados de los recursos de la organización, y buscar la manera de implementar buenas prácticas y hábitos más correctos y responsables.

CreamosValor

Actualmente nos encontrarnos en un escenario de Internet mucho más agresivo y peligroso que en sus comienzos.

CreamosValor

LA INFORMACION

¿Qué es la confidencialidad?

Una norma de seguridad reconocida internacionalmente define la confidencialidad como la propiedad de la información “por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados”. Es decir, la información confidencial es aquella que debemos proteger del acceso de personas no autorizadas.

Los datos personales. Leyes y marco regulador.

- **Ley Orgánica de Protección de Datos -LOPD**
- **Reglamento de Desarrollo de la LOPD–RDLOPD**

La Agencia Española de Protección de Datos

Hemos de tener en cuenta que legislación de protección de datos es de obligado cumplimiento para cualquier empresa española, y cumplir con ella es tan sencillo como llevar a cabo unos sencillos trámites administrativos y poner en marcha algunas medidas de seguridad básicas.

En nuestro caso, debemos evitar el acceso de personas no autorizadas a los datos personales que tengamos en nuestra empresa, gestionarlos siempre de la manera adecuada e informarnos cuando tengamos alguna duda.

¿Por qué decimos que una información es confidencial?

1. Porque es **información crítica para nuestro trabajo.**
2. Porque es **información "sensible" y puede haber otras empresas interesadas.**
3. Porque está **protegida por la legislación, como por ejemplo los datos personales.**
4. Porque nos hemos comprometido **con un tercero a mantener la información en secreto: un cliente, un socio, un proveedor, etc.**

¿Qué debemos hacer al gestionar información confidencial?

1. Firmar un acuerdo de confidencialidad con cualquier persona u organización a la que le demos acceso a la información.
2. Evitar que personas no autorizadas tengan acceso a la información confidencial que utilizamos, no dejándola a la vista ni en directorios o sistemas en los que pueda ser accedida por otras personas.
3. Aplicar medidas de cifrado cuando la información sea especialmente sensible.

Cifrado de la Información.

A la hora de proteger la información en formato electrónico, una de las medidas más eficaces es el cifrado de la información. Mediante esta técnica podemos codificar cualquier fichero y hacerlo inaccesible a otras personas que no sepan la clave de descrifrado.

¿Qué información debemos cifrar?

1. Toda aquella que sea de vital importancia en nuestro trabajo y sobre todo, si su difusión podría ser un problema.
2. Si trabajamos con datos personales de nivel alto como datos de salud, la legislación requiere que los almacenemos cifrados en ciertas circunstancias.
3. También es recomendable cifrar un fichero si lo vamos a enviar a clientes y/o proveedores.

Las copias de seguridad

Las copias de seguridad son uno de los principales elementos para evitar la pérdida de información cuando tenemos un problema. Aunque en general este tipo de sistemas los gestiona el personal de informática, hay varios aspectos que hay que tener en cuenta:

Información: Debemos asegurarnos de que se está realizando copia de seguridad de toda la información que utilizamos en nuestro trabajo. Es necesario que almacenemos la información en los sistemas y directorios de los que sabemos que se hace copia.

Soportes externos: Si para trabajar utilizamos soportes como discos duros externos, debemos asegurarnos de que se hace copia de la información que almacenan

Frecuencia: Si hacemos copias periódicas de nuestra información, debemos definir una periodicidad adecuada para que un problema con nuestro equipo no suponga la pérdida de las últimas semanas o meses de trabajo.

Salida de copias: Si tenemos que trasladar las copias fuera de la empresa debemos cifrarlas, para evitar que si las perdemos alguien pueda acceder a su contenido.

Personal de informática: Puesto que los sistemas de copia de seguridad suelen estar gestionados por el personal responsable de la informática, para cualquier duda debemos hablar con ellos.

LAS AMENAZAS

Con la expresión delito tecnológico se define a todo acto ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes.

- Empleados infieles e insatisfechos.
- Ataques que se producen contra el derecho a la intimidad.
- Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor.
- Falsificación de documentos.
- Sabotajes informáticos.
- Fraudes informáticos.
- Amenazas. Realizadas por cualquier medio de comunicación.
- Calumnias e injurias.
- Pornografía infantil. Existen varios delitos en este epígrafe.

¿Qué amenazas existen?

- **Software malintencionado.** Virus diseñados para infectar rápidamente sistemas de cómputo en todo el mundo utilizando Internet, correo electrónico y mensajes instantáneos.

- **La ingeniería social.** Es la herramienta más utilizada para llevar a cabo toda clase de estafas, fraudes y timos sobre los usuarios más confiados a través del engaño. Estas técnicas consisten en utilizar un reclamo para atraer la atención del usuario y conseguir que actúe en la forma deseada, por ejemplo convenciéndole de la necesidad de que reenvíe un correo a su lista de direcciones, que abra un archivo que acaba de recibir que contiene un código malicioso, o que, como ocurre en el phishing, proporcione sus códigos y claves bancarias en una determinada página web.

- **Correo electrónico no deseado.** Buzones inundados con emails no solicitados que bloquean los recursos de la red y sobrecargan las bandejas de entrada de correo electrónico. El Spam representa una amenaza a la productividad empresarial además se ha convertido en un transporte común para códigos maliciosos.

- **Acceso no autorizado a la red.** Los procedimientos y las políticas de seguridad que son adecuados para proteger los datos pueden ser inefectivos cuando la red se abre a extraños para mensajes y colaboración.

- **Acceso no autorizado a los datos.** Los negocios están cada vez más preocupados sobre la información confidencial que se filtra fuera del negocio a través de la infraestructura de mensajes y colaboración.

LOS SOPORTES

Cuando hablamos de soportes de información nos referimos a todos aquellos dispositivos que nos permiten almacenar información en formato electrónico y que en general, son fáciles de transportar.

Entre los soportes más utilizados encontramos los siguientes:

- Discos duros (internos y externos).
- Cintas y discos de copias de seguridad.
- Unidades USB o pendrives.
- Tarjetas de memoria (SD, microSD, etc.)
- Discos ópticos (CD/DVD).

La principal medida a aplicar sobre los soportes que utilizamos para evitar que la información se vea comprometida en el caso de robo o pérdida, es la de cifrar la información. De este modo nos aseguramos de que la información no es accesible por una persona no autorizada.

Cualquier soporte tiene una vida útil determinada, ya sea por quedarse obsoleto, tener poca capacidad en comparación con otros soportes, o mostrar fallos en su funcionamiento.

Una vez llegado el final de esta vida útil, debemos destruir el soporte de una manera adecuada, para evitar que alguien pueda obtener la información que éste almacena.

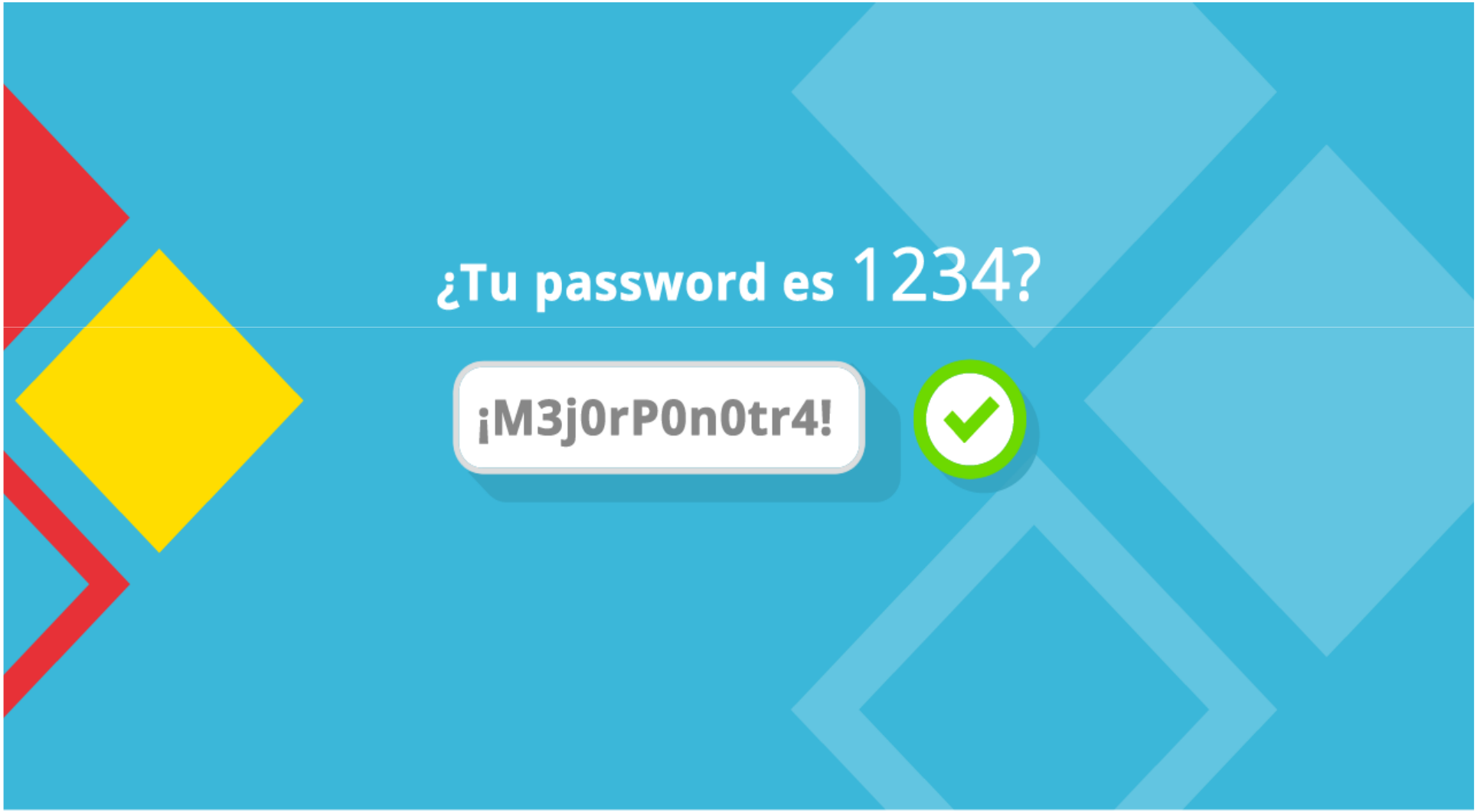
Algunas de las medidas de seguridad que debemos aplicar para evitar confusiones en el uso de soportes son:

• Marcar o etiquetar los soportes de las distintas áreas o propietarios para que no sean intercambiados por error.

• Evitar en la medida de lo posible el uso de memorias USB. En lugar de esto, podemos establecer carpetas departamentales con control de acceso lógico basado en perfiles y puestos.

• Documentar el procedimiento a seguir para realizar un borrado seguro.

EL PUESTO DE TRABAJO



El puesto de trabajo es el lugar en el que realizamos el trabajo diario. Como parte de las tareas cotidianas, cualquier usuario requiere acceder a diversos sistemas y manipular diferentes tipos de información.

Como consecuencia directa, debemos tener en cuenta que el puesto de trabajo es un punto clave desde el punto de vista de la seguridad de la información.

Gestión de la Documentación.

Cuando pensamos en un puesto de trabajo estándar, nos viene a la cabeza un puesto de trabajo en una oficina, con una mesa de trabajo, cajoneras, etc. Sin embargo, muchos trabajamos en puestos de trabajo ubicados en entornos industriales. Es aquí donde hay que tomar una serie de sencillas medidas preventivas:

- Almacenar o guardar nuestra información en una ubicación adecuada. Evitar su cercanía a sistemas de refrigeración, canalizaciones de agua o instalaciones que puedan afectar al papel.
- Emplear elementos adecuados para almacenar el papel, como por ejemplo armarios y cajoneras que dispongan de dispositivos de cierre, o cajas fuertes o armarios ignífugos en caso necesario.
- Destruir la documentación de manera segura. Dependiendo del volumen de papel, podemos utilizar destructoras de papel convencionales o subcontratar la retirada y destrucción a un proveedor.

En este último caso no debemos olvidar firmar el acuerdo de confidencialidad pertinente y solicitar los certificados de destrucción segura.

Contraseñas seguras.

Debemos hacer uso de una política de contraseñas seguras, que defina al menos los siguientes aspectos de las claves que utilicemos:

- La longitud mínima de las claves.
- La obligación de utilizar minúsculas, mayúsculas y símbolos.
- La periodicidad con la que se debe cambiar la contraseña.

También debemos recordar que las contraseñas son personales, secretas e intransferibles. No debemos apuntarlas en post-its, libretas, documentos de texto o cualquier otro medio que permita acceder fácilmente a nuestras claves.

Métodos de Autenticación.

Un método de autenticación es la técnica o el procedimiento que un sistema utiliza para verificar que un usuario es quien dice ser.

Métodos:

- Los basados en algo que sabemos. El caso más evidente es la utilización de contraseñas.
- Los basados en algo que poseemos, como por ejemplo, una tarjeta de acceso magnética.
- Los basados en una característica física de la persona, como por ejemplo, su huella dactilar, retina o rasgos faciales.

Mesas Limpias.

Una política de mesas limpias requiere que:

- El puesto de trabajo esté limpio y ordenado.

- La documentación que no estemos utilizando en un momento determinado debe estar guardada correctamente, especialmente cuando dejamos nuestro puesto de trabajo y al finalizar la jornada.

- No haya usuarios ni contraseñas apuntadas en post-it o similares.

Ingeniería Social.

Los ataques de ingeniería social tienen como objetivo a cualquier empleado, sin importar en el puesto que esté. A través de ellos un atacante puede obtener información confidencial de las propias víctimas, o utilizar a ésta para acceder a otras personas de la organización de manera inadvertida.

Existen cuatro pilares de los ataques de ingeniería social, que permiten que en muchos casos éstos sean exitosos:

1) El deseo de ayudar a otras personas.

2) La confianza de que las personas actúan por buena voluntad.

3) El no querer decir que no a las peticiones de otras personas.

4) El deseo de ser halagado.

Aunque parezca algo fruto de la casualidad, los ataques de ingeniería social se llevan a cabo de manera planificada, obteniendo información de múltiples fuentes, lo que permite simular un conocimiento similar al que tendría alguien que trabajase en la organización.

Uno de los medios más utilizados en la ingeniería social es el correo electrónico. Bajo cualquier pretexto o excusa invitan al usuario a enviarles información personal o de la empresa, a hacer clic en algún enlace o a abrir un fichero infectado adjunto.

El ataque por correo electrónico se realiza través de una cuenta falsa con características similares a las cuentas de correo de la empresa, para darle más credibilidad en caso de ser un ataque dirigido contra la misma.

Fugas de Información.

La mayoría de las fugas de información que se producen en las empresas tienen como origen el puesto de un empleado. Pueden ser fruto tanto de actos malintencionados por parte de empleados descontentos como de errores al utilizar los sistemas con los que gestionamos la información.

Para evitar fugas de información, debemos ser muy cautelosos a la hora de usar el correo electrónico y las redes sociales.

Existen soluciones informáticas cuyo objetivo principal es reducir el riesgo de las fugas de información, sin embargo, debemos tener en cuenta que ninguna herramienta es capaz de sustituir al ya mencionado sentido común a la hora de gestionar la información.

LOS DISPOSITIVOS MOVILES

No te olvides de mí

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Existen muchos tipos de dispositivos móviles. Hasta hace poco, en las empresas se utilizaban los ordenadores portátiles, pero actualmente, casi la totalidad de los empleados hacen uso de smartphones, ya sea para uso personal o corporativo, y también existe una tendencia creciente en el uso de las tablet.

Los riesgos más habituales de los dispositivos móviles son la pérdida, el robo y la rotura, destrucción o avería. Sin embargo, aunque en muchos casos esta tecnología tiene un coste elevado, el mayor problema que se deriva de estos incidentes no es la pérdida económica directa, sino la pérdida o robo de información.

Para evitar estos riesgos debemos implantar diversas medidas de seguridad.

Cifrado.

Habitualmente, los dispositivos móviles se utilizan fuera de las dependencias de nuestra organización.

Por este motivo, debemos cifrar la información almacenada en estos soportes.

Existen múltiples herramientas para el cifrado de información, y la mayor parte de fabricantes de herramientas de seguridad tienen aplicaciones para ello.

BYOD

El BYOD, llamado así por sus siglas en inglés Bring Your Own Device, es una tendencia que se basa en que los empleados hacen uso de sus dispositivos personales en el entorno de trabajo.

Esto permite al empleado hacer uso de un dispositivo que está adaptado a sus necesidades y por tanto deriva en una mayor productividad, y a la empresa le supone un ahorro de costes y una mayor productividad de la persona.

Sin embargo, este tipo de prácticas BYOD tienen importantes implicaciones desde el punto de vista de la seguridad de la información, dado que aunque el dispositivo que utilicemos esté personalizado según nuestras preferencias, esto no necesariamente significa que tenga las necesarias medidas de seguridad.

Redes WiFi Públicas.

Es frecuente hacer uso de las redes WiFi públicas cuando nos encontramos en lugares públicos, como aeropuertos, cafeterías, tiendas, restaurantes o bibliotecas. Por lo general, lo hacemos para evitar el coste de la conexión 3G/4G o por velocidad, si no tenemos suficiente cobertura de datos.

Sin embargo, las redes WiFi públicas presentan diferentes riesgos, siendo el principal no saber quién controla la WiFi. Esto no significa que el dueño de un local tenga malas intenciones, sino que un usuario malintencionado puede atacar la red y hacerse con su control si ésta no tiene las medidas de seguridad adecuadas, sin que el propietario del local lo sepa.

Si eso sucede, es posible que nuestros datos sean interceptados por algún ciberdelincuente, capturando toda la información que transmitimos.

Configuraciones de seguridad Vs. por defecto.

Por norma general, las configuraciones de seguridad por defecto de los dispositivos móviles no tienen activadas todas las medidas de seguridad que ofrece el sistema, ya que éstas pueden introducir demasiada complejidad para algunos usuarios básicos. Sin embargo, cuando se trata de dispositivos que vamos a utilizar en el entorno corporativo, ya sea BYOD o dispositivos de la empresa, es imperativo que apliquemos a cualquier tipo de dispositivo las necesarias medidas de seguridad.

Entre las principales medidas que podemos destacar están las siguientes:

- Cifrado de los soportes de almacenamiento.
- Contraseña de acceso al sistema.
- Funcionalidad que permita restablecer la configuración por defecto del
- dispositivo vía remota (también llamado wipe remoto).
- Copias de seguridad periódicas.

Geoposicionamiento.

Llamamos geoposicionamiento a la capacidad de algunos dispositivos de ubicarse geográficamente. Esta funcionalidad es utilizada por ejemplo por los GPS para guiar al usuario en su trayecto.

Sin embargo, la información de geoposicionamiento también es utilizada por otros servicios y aplicaciones. Por ejemplo, en diversas redes sociales existe la posibilidad de que autoricemos a la red a posicionarnos, y las aplicaciones para capturar y editar imágenes también guardan información sobre la ubicación en la que se ha la foto.

El principal riesgo asociado a estos datos de localización es que estamos recabando, almacenando y quizás, difundiendo, más información de la necesaria. Esto ocurre en la mayor parte de los casos de forma involuntaria.

Dado que la mayor parte de los dispositivos móviles permiten habilitar y deshabilitar las funciones de geoposicionamiento, según las preferencias y necesidades del usuario, se recomienda deshabilitar esta funcionalidad siempre que no sea estrictamente necesario.

GESTION DE RIESGOS EN SI

La gestión de riesgos está presente, con mayor o menor protagonismo, en distintos ámbitos de la sociedad y la empresa. Son algunos ejemplos la gestión de riesgos:

- Laborales
- Alimentarios
- Bancarios, financieros
- Corporativos, de proyectos
- Medioambientales
- De seguridad de la información.

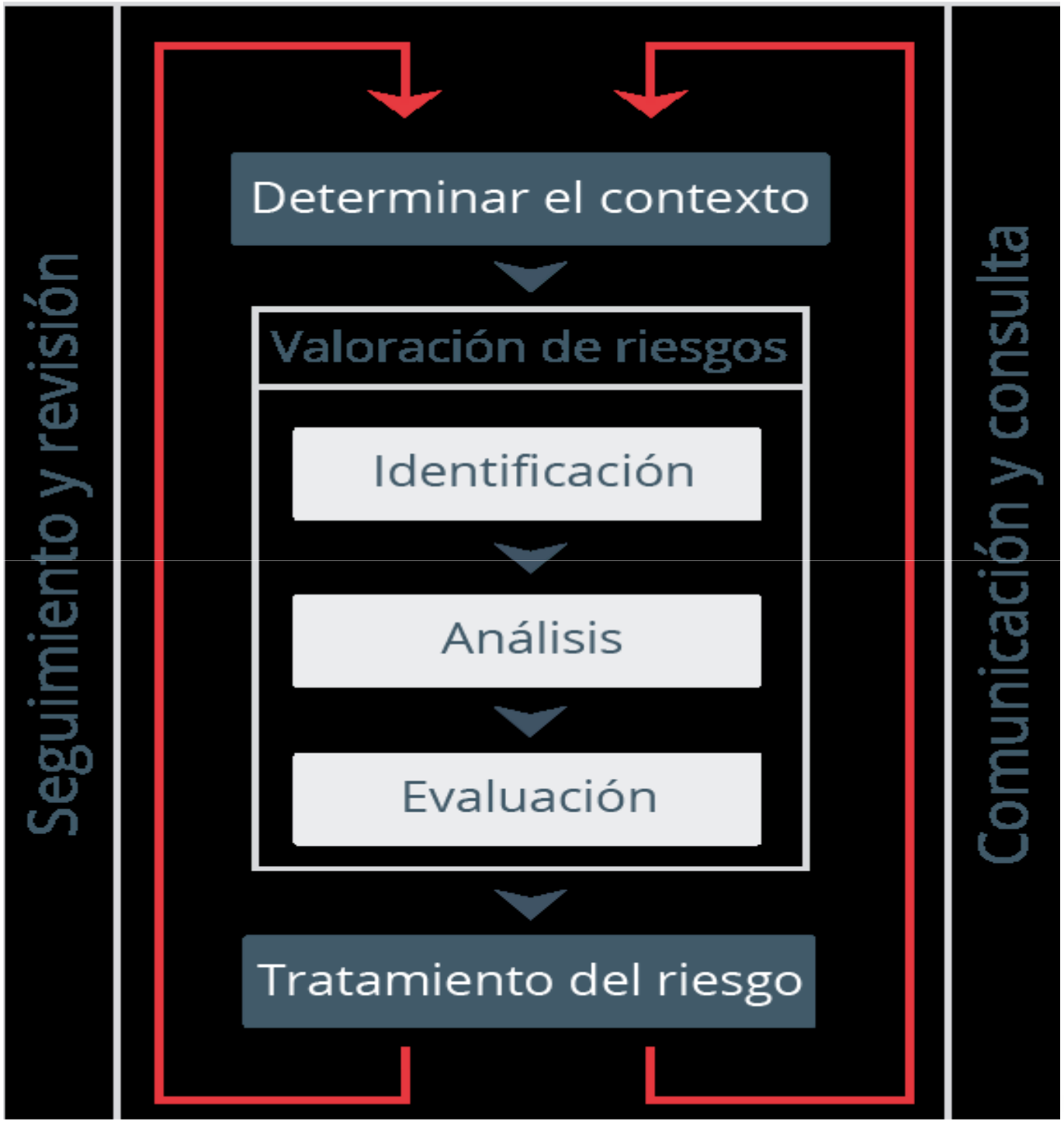
Un hecho común a todos ellos, es que los responsables son conscientes de la existencia de amenazas que suponen un peligro para la consecución de sus objetivos.

Dedican esfuerzos y recursos a mantener estos riesgos por debajo de un límite previamente consensuado en sus organizaciones.

Las organizaciones que decidan gestionar el riesgo para su actividad deberán realizar dos grandes tareas:

1. Análisis de riesgo: que consiste en averiguar el nivel de riesgo que la empresa está soportando. Para ello, tradicionalmente las metodologías proponen que se realice un inventario de activos, se determinen las amenazas, las probabilidades de que ocurran y los posibles impactos.

2. Tratamiento de los riesgos: para aquellos riesgos cuyo nivel está por encima del umbral deseado la empresa debe decidir cuál es el mejor tratamiento que permita disminuirlos. Esta decisión siempre ha de pasar un filtro económico donde el coste del tratamiento, o coste de protección, no supere el coste de riesgo disminuido.



CreamosValor

En términos de gestión de riesgos de seguridad de la información, el activo a proteger es la información de la compañía.

Para la **evaluación de riesgos de seguridad de la información** en primer lugar se han de identificar los activos de información. En general estos pueden ser de dos tipos:

Primarios:

- **Información:** estratégica, de carácter personal o que esté sujeta a legislación que la proteja, esencial para el desarrollo del negocio, de difícil o muy costosa reposición, etc.
- **Actividades y procesos de negocio:** que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

De soporte:

- Hardware: PC, portátiles, servidores, impresoras, discos, documentos en papel
- Software: sistemas operativos, paquetes, aplicaciones,…
- Redes: conmutadores, cableado, puntos de acceso,…
- Personal: usuarios, desarrolladores, responsables,…
- Edificios, salas, y sus servicios
- Estructura organizativa: responsables, áreas, contratistas,…

Para valorar los daños estas son algunas de las preguntas:

- ¿qué valor tiene este activo para la empresa?
- ¿cuánto cuesta su mantenimiento?
- ¿cómo repercute en los beneficios de la empresa?
- ¿cuánto valdría para la competencia?
- ¿cuánto costaría recuperarlo o volverlo a generar?
- ¿cuánto costó adquirirlo o su desarrollo?
- ¿a qué responsabilidades legales o contractuales nos enfrentamos si se ve comprometido?

El nivel de tolerancia de riesgo se establece en base a criterios de coste-beneficio.

COSTE-BENEFICIO	TRATAMIENTO
El coste del tratamiento es muy superior a los beneficios	**Evitar el riesgo**, por ejemplo, dejando de realizar esa actividad
El coste del tratamiento es adecuado a los beneficios	**Reducir o mitigar el riesgo**: seleccionando e implementando los controles o medidas adecuadas que hagan que se reduzca la probabilidad o el impacto
El coste del tratamiento por terceros es más beneficioso que el tratamiento directo	**Transferir el riesgo**, por ejemplo, contratando un seguro o subcontratando el servicio
El nivel de riesgo está muy alejado del nivel de tolerancia	**Retener o aceptar el riesgo** sin implementar controles adicionales. Monitorizarlo para confirmar que no se incrementa.

Tabla 3: Ejemplo criterios para el tratamiento de riesgos

Para reducir o mitigar los riesgos se realizan estas acciones:

- instalar productos o contratar servicios
- establecer controles de seguridad
- mejorar los procedimientos
- cambiar el entorno
- incluir métodos de detección temprana
- implantar un plan de contingencia y continuidad
- realizar formación y sensibilización

Gracias por su atención

El campo de batalla puede parecer confuso y caótico, pero el bando propio debe permanecer ordenado. Así será a prueba de derrotas.

Sun Tzu - El Arte de la Guerra

INSTITUTO NACIONAL DE CIBERSEGURIDAD

www.peritosjudicialesforenses.com

https://www.linkedin.com/in/angeldelarivarodriguez

https://www.facebook.com/peritotelamticaforense