ESPECIAL

"Consejo de Amigo"

DE Tecnología & Sentido Común

AGOSTO 2021

ESPECIAL "Consejo de Amigo" DE Tecnología & Sentido Común

EQUIPO DIRECTO:
Javier Peris - Piloto
Manuel D. Serrat - Copiloto
Alberto Rodríguez - Equipo Directo
Juan Carlos Muria - Equipo Directo

MICRO-ESPACIOS
Marlon Molina - Es Tendencia
Ricard Martínez - Ojo Al Dato
Catalina Valencia - Ecosistema Emprendedor
Víctor Almonacid - La Nueva Administración
Shirley Villacorta - América Próxima
Fernando Ley - Geo Energía

PUBLICIDAD Y CONTRATACIÓN
Carmen Usagre
carmen.usagre@businessandcompany.com
Teléfono: +34 96 109 44 44

GABINETE JURÍDICO
Jesús López Peláz

ATENCIÓN AL LECTOR
tecnologiaysentidocomun@businessandcompany.com

EDITA
Business, Technology & Best Practices, S.L.

Av. San Onofre, 20
46930-Quart de Poblet (Valencia)
Teléfono: 96 109 44 44
Fax: 96 109 44 45
https://businessandcompany.com
soluciones@businessandcompany.com

JESÚS P. LÓPEZ PELAZ

Abogado especialista en Derecho Civil, Mercantil y Nuevas Tecnologías.

Profesor de Master de Marketing y Comunicación Digital en en Universidad Camilo José Cela.
Profesor en el Master de Experto en Redes Sociales de la Universidad de Alicante y AERCO.

Mentor de creación de empresas tecnológicas en StartUp Weekend (Valencia y Salamanca), Weekend Emprende, Reset Weekend e iWeekend Valencia. Colaborador del Centro de Europeo de Empresas Innovadoras (CEEI). Mentor de empresas sociales en Socialnest.
Profesor en LearningLaw.

PREPARA A TU ORGANIZACIÓN PARA RETOS FUTUROS CON ITIL® 4

Los avances tecnológicos han transformado la forma en la que adquirimos e interactuamos con bienes y servicios; creando nuevos comportamientos, expectativas y experiencias.
Pero ¿estás preparado para esos retos?

El mundialmente reconocido ITIL 4, es el método de gestión de servicios que proporciona, a organizaciones y profesionales, un modelo operativo digital / de TI de extremo a extremo para la entrega y operación de productos y servicios habilitados por tecnología y permite a los equipos de TI continuar desempeñando un papel crucial en una estrategia de negocios más amplia.

¿Quieres conocer más?

AXELOS.com/ITIL4-futuro
(Página en inglés)

ESPECIAL
AGOSTO 2021

#TYSC
TECNOLOGIA Y SENTIDO COMÚN

índice
DE CONTENIDOS

https://tecnologiaysentidocomun.com

Índice de Contenidos

#TYSC

Un SLA completo es un acuerdo eficaz

El contrato de SLA (Service Level Agreement) o acuerdo de nivel de servicios es uno de los contratos más conocidos por los profesionales de la gestión de de TI en entornos empresariales.

Aunque muchos abogados consideran los contratos de SLA como contratos de arrendamientos de servicio tradicionales en los que la descripción del servicio es un servicio tecnológico, existe una diferencia clave que debemos tener en cuenta en el momento de su descripción y definición: mientras que el arrendamiento de servicio tradicional procede a describir conductas que son desarrolladas por el prestador en los SLA se procede a definir entornos de tolerancia de la fiabilidad del servicio contratado. Para hacerlo, en función del servicio contratado mediante el Service level Agreement, deberán ponderarse elementos técnicos como:

• **Disponibilidad del servicio:** es decir la continuidad en la prestación de un determinado servicio sin interrupciones.

• **Tasa de errores**

• **Calidad Técnica del Servicio**: En muchas ocasiones el servicio disponible debe cumplir determinadas especificaciones para que sea efectivo a la finalidad TI requerida por la organización para mantener su funcionabilidad

CONTINÚA EN PRÓXIMA PÁGINA

Con ello debemos establecer rangos de tolerancia (como se define en ITIL) en los que el servicio resulta cumplidor o no de la finalidad requerida así como las métricas en las que se basará la fiabilidad esperada, las responsabilidades derivadas del incumplimiento de las tolerancias y las consecuencias o acciones que se desencadenan por haberse producido la excepción en el servicio fuera del margen fijado en el contrato.

Por lo tanto para poder contratar un servicio de TI y documentarlo a través de acuerdo de nivel de servicios que se suscriba con el proveedor, en primer lugar procede un estudio interno del entorno
corporativo en el que el servicio de TI va a estar operativo. Ese estudio previo de las necesidades tecnológicas de la organización permitirá describir el impacto que en la infraestructura podrá producir cada una de las pérdidas de disponibilidad de las funciones contratadas con el proveedor.

Así, por ese conocimiento del funcionamiento de la estructura TI a la que el proveedor sirve, podremos fijar niveles de impacto que nos permitirán describir las consecuencias en caso de que se produzca la excepción al nivel contratado. Podremos definir aquellas en las que simplemente el proveedor se obligue a realizar cierta actuación (por ejemplo, recuperación del backup) sin coste, o bien indemnizaciones de la pérdida ocasionada (por ejemplo, indemnización por minuto/hora de caída del servidor), o bien soluciones técnicas alternativas en función del servicio. Cuando pretendemos documentar un acuerdo de nivel de servicios adecuadamente deberemos al menos regular los siguientes extremos:

• **Descripción del servicio:** En el SLA la definición del servicio y de sus componentes adquiere una importancia fundamental, puesto que es preciso adecuar la terminología al entorno y conocer exactamente qué referencias se están usando para referirse a qué componentes de la tecnología que constituye el servicio contratado. Además, desde un punto de vista práctico jurídico, la existencia de definiciones claras en el propio contrato de SLA permiten acreditar ante quien deba conocer de un futuro litigio (juez o árbitro) cada uno de los elementos que eran objeto de contratación. Las ambigüedades propias del lenguaje no técnico pueden generar verdaderas incertidumbres a la hora de dar cumplimiento a un contrato de esta naturaleza

• **Soporte y asistencia:** Los contratos de SLA documentan los servicios contratados con proveedores externos a la organización (a diferencia del los OLA, Operational Level Agreement) y por ello no sólo debemos fijar qué deben hacer y cómo deben hacerlo si no también cómo deben aten- dernos y darnos soporte.

• **Medidas de seguridad.** En el marco de la definición de las características del servicio debemos atender especialmente a los requisitos de seguridad que debe cumplir el servicio para que sea adecuado a la finalidad operativa que se desarrolla.

• **Garantías del sistema y tiempos de respuesta.**

• **Disponibilidad del sistema.**

Y por último, y como consecuencia de la graduación de impacto que cada incumplimiento provoque dentro de nuestra organización, se establecerán las consecuencias (pecuniarias o de cualquier otro tipo) que provoquen los incumplimientos del proveedor.

Un SLA completo es un acuerdo eficaz.


ENTER THE CODE
function decorate(event) {
event = event || window.event;
var target = event.target || event.srcElement;
if (target && (target.getAttribute('action') ||
ga(function (tracker) {
var linkerParam = tracker.get('linkerParam');
document.cookie = '_hola ga=' + linkerParam
});
abogado amigo
Abogado Amigo
Bufete Experto en
Nuevas Tecnologías
www.abogadoamigo.com

El software espía en el Código Penal

Muchas de las conductas delictivas que se realizan en el entorno telemático van dirigidas a lograr la obtención de información reservada de las empresas o de las personas. En ese marco se encuadran los diferentes delitos de revelación de secretos que en muchos supuestos se llevana cabo mediante la utilización de algún tipo de software espía o ciberespionaje que permite acceder a los datos informáticos secretos almacenados en un soporte conectado a la red, ya sea su teléfono smartphone, bases de datos en servidores, cuentas de redes sociales o cuentas bancarias. Nuestro Código Penal, después de las últimas modificaciones, dedica especial interés a la represión de los delitos desarrollados en el ámbito electrónico. El art. 197 ter regula la creación de programas informático maliciosos que facilitan el ciberespionaje. La conducta típica viene definida por los verbos producir, adquirir para su uso, importar o de cualquier modo facilitar a tercero, las herramientas o instrumentos que se relacionan en los apartados a) y b) del mismo precepto. Por tanto los comportamientos objeto de sanción se encuentran definidos de una forma abierta que incluye tanto la elaboración para uso propio, o para distribución a terceros, como la importación, la adquisición y en consecuencia la ulterior posesión.

No obstante la posibilidad de actuar penalmente ante dichos comportamientos, se encuentra acotada por dos elementos.

El primero de ellos, la falta de autorización para su elaboración, adquisición o facilitación a terceros y el segundo, de carácter teleológico, al exigirse que dichas acciones estén orientadas a facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del art. 197 o el art. 197 bis. En realidad ambos elementos son complementarios y responden a una preocupación de la que se deja constancia de forma espe- cífica en la propia Directiva europea 2013/40/UE de la que se deriva este artículo para perseguir el ciberespionaje. Muchas de las herramientas o instrumentos susceptibles de ser empleadas para cometer estos hechos ilícitos pueden haber sido creadas y comercializadas para su uso con objetivos legítimos e incluso necesarios, como los de auditar la seguridad de los sistemas, programas o aplicaciones, detec- tar vulnerabilidades, garantizar la solidez o fiabilidad de contraseñas o sistemas de seguridad etc.

Por una parte que quien así actúa no esté autorizado para ello, bien sea legalmente o porque se le haya encomendado dicha responsabilidad por quien tenga capacidad para ello en el marco concreto de la activi- dad de que se trate. Pero además ha de actuarse con la finalidad específica de facilitar la comisión de un delito de los indicados en el precepto, circunstancia que habrá de acreditarse en cada supuesto, atendiendo a los elementos, pruebas o indicios existentes. En el caso de un software como el suyo, toda la orientación, publicidad, comercialización y utilidad legitima es la que debe ser explicada en caso de cuestionarse si la creación y puesta a disposición del software estaba orientada a facilitar la comisión de alguno de estos delitos.

CONTINÚA EN PRÓXIMA PÁGINA

La pena prevista para quien concurra en el delito del 197.ter es una multa de seis a dos años. La multa se calcula asignando un valor económico a cada día y multiplicándolo por la duración de la condena. Así, si se establece un valor día de (por ejemplo) 10 euros y una condena de un año, el importe será de 365x10= 3650euros.

Es por esto que no se puede fijar cual es el importe máximo que puede resultar la condena si no que depende de aspectos como la capacidad económica del condenado por el ciberespionaje. Además de la multa debe tenerse en cuenta que la condena por la comisión de este delito puede llevar aparejada además la obligación de reparar el caño causa a través de la responsabilidad civil derivada del delito.

Por otro lado también cabe que se impongan a la persona jurídica las siguientes condenas:

b) Disolución de la persona jurídica. La disolución producirá la pérdida definitiva de su personalidad jurídica, así como la de su capacidad de actuar de cualquier modo en el tráfico jurídico, o llevar a cabo cualquier clase de actividad, aunque sea lícita.

c) Suspensión de sus actividades por un plazo que no podrá exceder de cinco años.

d) Clausura de sus locales y establecimientos por un plazo que no podrá exceder de cinco años.

e) Prohibición de realizar en el futuro las actividades en cuyo ejercicio se haya cometido, favorecido o encubierto el delito. Esta prohibición podrá ser temporal o definitiva. Si fuere temporal, el plazo no podrá exceder de quince años.

f) Inhabilitación para obtener subvenciones y ayudas públicas, para contratar con el sector público y para gozar de beneficios e incentivos fiscales o de la Seguridad Social, por un plazo que no podrá exceder de quince años.

g) Intervención judicial para salvaguardar los derechos de los trabajadores o de los acreedores por el tiempo que se estime necesario, que no podrá exceder de cinco años. La intervención podrá afectar a la totalidad de la organización o limitarse a alguna de sus instalaciones, secciones o unidades de negocio dependiendo de cómo se determine en la sentencia que se ha venido a cometer el delito. El Juez o Tribunal determinará exactamente el contenido de la intervención y determinará quién se hará cargo de la intervención y en qué plazos deberá realizar informes de seguimiento para el órgano judicial para asegurar que ésta sea efectiva para garantizar que no vuelva a colaborarse en actividades de ciberespionaje. La intervención se podrá modificar o suspender en todo momento previo informe del interventor y del Ministerio Fiscal. El interventor tendrá derecho a acceder a todas las instalaciones y locales de la empresa o persona jurídica y a recibir toda la información que sea necesaria para el ejercicio de sus funciones.

La clausura temporal de los locales o establecimientos, la suspensión de las actividades sociales y la intervención judicial podrán ser cordadas también por el Juez Instructor como medida cautelar durante la instrucción de la causa.

Entre todo el software que queda incluido en la conducta tipificada en el artículo 197.ter se encuentran los conocidos como programas espía (spyware) creados con el objetivo de recolectar, sin conocimiento, información personal de una pluralidad de usuarios o, en su caso, información de interés más general, almacenada en un sistema informático, para enviarla al atacante o a un tercero vía internet con finalidades diversas. Un ejemplo característico de este tipo de malware es el software utilizado para realizar el phishing bancario y cuyo objeto es el robo de credenciales de usuarios de banca electrónica para su utilización posterior en transacciones fraudulentas. También pueden producir un efecto similar los programas llamados keyloggers que registran las pulsaciones en un teclado y de esta forma permiten apoderarse de contraseñas personales.

más información en:
https://javierperis.com/bpm

Y tú ¿Transformas o Trastornas tu Organización?

Aprende a:

- ✓ Modelar
- ✓ Mejorar
- ✓ Automatizar Procesos de Negocio

Curso Oficial de Certificación en
Gestión de Procesos de Negocio
ISO/IEC 19510
BPM Professional

Si quieres Aprender, Certificarte, Practicar y recibir posteriormente Ayuda para Liderar con Éxito la Transformación Digital en tu Departamento, Startup, Empresa o Administración, no te quede la menor duda de que este es tu Curso y esta es tu Certificación.

Business&Co.®
Business, Technology & Best Practices, S.L.

El Descubrimiento y Revelación de Secretos

El descubrimiento y revelación de secretos es probablemente el tipo delictivo que permite la persecución de mayor cantidad de conductas delictivas en el ámbito tecnológico. Cuando nos encontramos en un entorno digital, cualquier información se trasforma en paquetes de datos que intentamos mantener protegidos en un entorno seguro. Ya sea un documento, foto, estadística, base de datos… toda la información es un "archivo" sobre el que aplicamos (con más o menos éxito) medidas para preservarlos del conocimiento de agentes externos.

Es por ello que en este tipo de delitos el bien jurídico protegido será la privacidad, no la integridad informática. Para ofrecer una protección adecuada del perímetro de seguridad de nuestra privacidad, la barrera penal se adelanta a la mera "puesta en peligro" de la misma mediante la interdicción de intrusiones o inmisiones principalmente de carácter técnico, que la colocan en situación de riesgo evidente, pues la privacidad supone poder excluir a terceros de la órbita de lo que uno preserva como íntimo.

La ventaja de definir el tipo delictivo con referencia a la privacidad y no a concretas actuaciones o procedimientos informáticos, facilita la adaptación de la persecución penal a las diferentes formas de agresión que podemos ir encontrando, cubriendo la evolución de las técnicas de los ciberdelincuentes.

Para poder enjuiciar estas conductas deberemos definir en primer lugar el entorno de priva-

cidad que ha sido violado o puesto en peligro por el delincuente. Además deberemos acreditar la existencia del "secreto" entendido como información que es mantenida en una esfera restringida a la que no hemos autorizado su acceso al delincuente.

Este delito lo encontramos definido en el art. 197 CP que define las coonductas que pueden dar lugar a su comisión:

- Apoderamiento inconsentido de correspondencia, documentos o efectos personales, o interceptación de telecomunicaciones o uso de artificios de escucha/grabación/ transmisión/reproducción de audio o video, para descubrir secretos de alguien o vulnerar su intimidad.

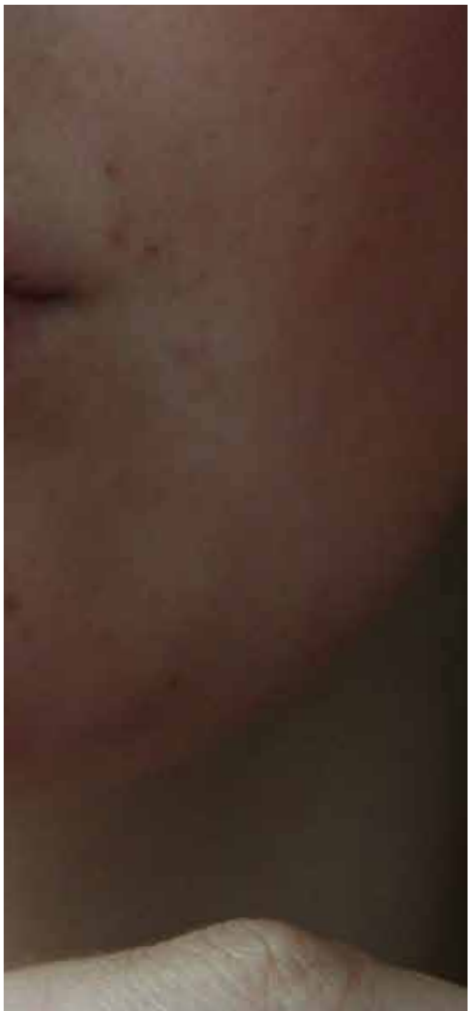
- Apoderamiento uso o modificación inconsentidos, de datos reservados de ficheros, soportes, archivos, en perjuicio de tercero, o acceso o alteración de los mismos, conformando con el anterior, los delitos básicos de descubrimiento.

Será delictivo revelarlos, cederlos o difundirlos, aunque no se haya tomado parte en su ilícita obtención, si se sabe de su origen ilícito.

- Se agravan las penas para las intrusiones que afecten a datos ultraprotegidos, los que revelan ideología, religión, creencias, salud, raza, vida sexual, personas especialmente protegidas, menores o personas con discapacidad, o cuando los realizan encargados /responsables de

CONTINÚA EN PRÓXIMA PÁGINA





bases de datos o se ejecuten usando de forma no autorizada datos personales de la víctima o con fines lucrativos.
- Difundir, revelar o ceder imágenes o grabaciones audiovisuales sin autorización del afectado aunque se hayan obtenido con su anuencia inicial, obtenidas en un domicilio o lugar fuera del alcance de !a mirada de terceros, sólo para la contemplación de determinada persona y no ce cualquier, en el ámbito íntimo, siempre que la divulgación, menoscabe además, gravemente, su intimidad.

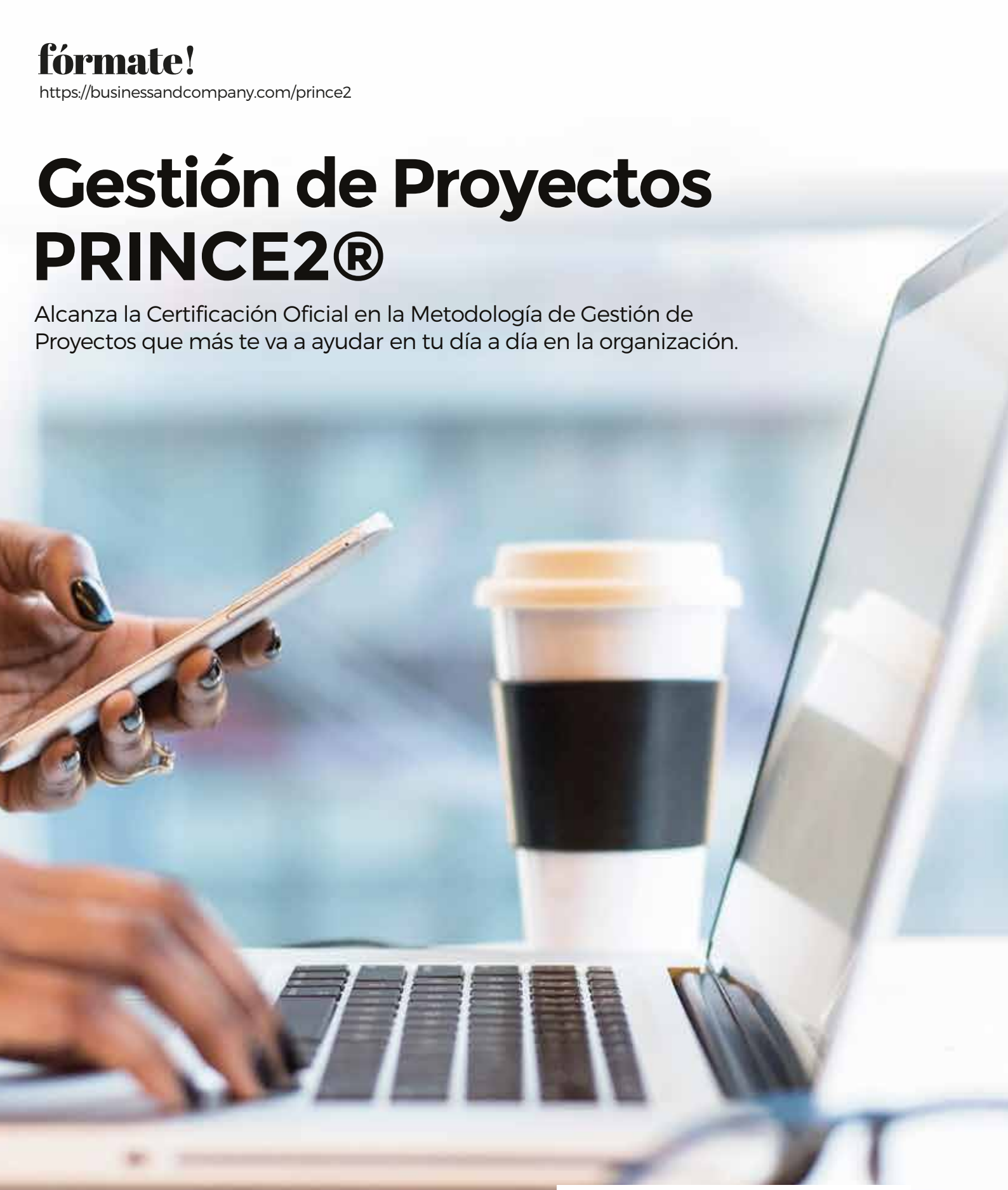
Este último punto, puede entenderse que protege en cierta forma la intimidad de quien la protege deficientemente porque confía en cesionarios indiscretos o inmaduros, pues el material personal se cede a quien al final no es capaz de mantenerlo sin revelarlo. Antes de las reformas legislativas que nos llevaron a la presente redacción, el contenido que había sido compartido con otros no era considerado “secreto” y por ello no daba lugar a la aplicación de este tipo delictivo y sólo podía ser perseguido como Daño al Honor que ocasionaba la divulgación.
El inicial consentimiento que una parte otorgó a la otra para que tuviera la información queda anulado (sin necesidad de previo requerimiento al efecto) cuando se produce un cambio radical de circunstancias.

fórmate!

https://businessandcompany.com/prince2

Gestión de Proyectos PRINCE2®

Alcanza la Certificación Oficial en la Metodología de Gestión de Proyectos que más te va a ayudar en tu día a día en la organización.



Business&Co.®
Business, Technology & Best Practices, S.L.

PRINCE2®
ACCREDITED TRAINING ORGANIZATION
PeopleCert ON BEHALF OF AXELOS

La defensa de tu marca

La marca indica el origen empresarial de los productos o servicios y protege la función de condensación del "good will" o experiencia de usuario. Las marcas funcionan en nuestro mercado como condensadores de prestigio de tal forma que conociendo la procedencia del producto podemos de forma fácil e intuitiva conocer sus características. Existen productos de los cuales la marca nos anuncia sus características, incluso aunque existan diferentes modelos o versiones, la marca indica su categoría. La marca anticipa las expectativas del consumidor en el momento de la compra.

Las marcas y nombres comerciales permiten al empresario ser encontrado por los usuarios de forma sencilla, directa, inequívoca y por ello facilita sus ventas en el mercado. Pero la marca también son de utilidad al consumidor. Gracias a las marcas el usuario final puede reducir su coste de información (el tiempo y el esfuerzo necesario para conocer las características de un producto) pudiéndose guiar simplemente por las marcas para diferenciar entre los productos similares y así elegir de una forma rápida y eficiente aquel producto que mejor se adapta a sus necesidades en el momento de la compra. Sin marcas o nombres comerciales, la experiencia de usuario se difuminaría al no poder identificar de forma directa el producto o servicio en el acto de compra posterior.

Por ello la defensa marcaria no es un acto exclusivamente de defensa del productor o del empresario, si no que debe ponerse necesariamente en relación con la defensa de los consumidores que han identificado la reputación de un producto en base a actos de compra anteriores, referencias, experiencias, opiniones de terceros…

¿QUÉ INSTRUMENTOS TENEMOS PARA PODER DEFENDER NUESTRA MARCA EN EL MERCADO?

Por un lado contamos con la acción reivindicatoria de la solicitud de nombre comercial.
Siempre que podamos acreditar un uso de la denominación marcaria previo a la solicitud de registro de un tercero en el mercado permitiendo identificar nuestros productos, podremos oponernos al registro y evitar la ocupación de una denominación vinculada a nuestra reputación. Obviamente, la posibilidad de registrar la marca que usamos se deriva directamente de no haber registrado la marca que nos proponíamos explotar, por lo que una adecuada planificación de riesgos jurídicos y una minima inversión hubiera sido suficiente para evitar esta situación.
De forma paralela, en caso de ocupación de dominios de internet coincidentes con nuestra marca registrada podremos reivindicar nuestra preferencia sobre ellos y conseguir el cese en el uso por parte de aquellos que los hubieran

ocupado. La reclamación de los dominios, además de judicialmente, puede tramitarse mediante arbitraje ante Red.es o WIPO según las características del caso.

Como ya hemos dicho, el nombre comercial permite identificar la procedencia de productos en el mercado. Supone por ello una garantía simultáneamente para el empresario que puede hacer valer su autoría como para los consumidores que identifican de forma sencilla y práctica la procedencia y calidad del producto. La propia finalidad del nombre comercial requiere publicidad en el mercado. De esta forma la propiedad industrial actúa como un canalizador de los valores intangibles que acompañan a la autoría, calidad y reputación de un determinado producto.

Pero la marca no sólo puede protegerse en el ámbito de la ley marcaria propiamente dicha. Al ser un elemento que aglutina la reputación de su explotador, el uso de la misma puede generar una situación de competencia desleal al aprovecharse de la misma un tercero ilegitimamente. Es por ello, que podemos encontrar la necesidad de defender nuestra marca en el mercado mediante una acción derivada de la Ley de competencia desleal

La Ley nos ofrece la posibilidad de buscar amparo en una acción amplia basada en el artículo 4 de la Ley de Competencia Desleal que supone una cláusula abierta de la forma en la que los empresarios deben proceder en el mercado. La Ley de Competencia Desleal impone con carácter general su influencia en todas las conductas de carácter concurrencial, por lo que éstas no deberán resultar objetivamente contrarias a las exigencias de la buena fe.

CONTINÚA EN PRÓXIMA PÁGINA

Sin embargo, el citado carácter general de esta norma jurídica hace necesaria una concreción de la misma, pues la complejidad que pueden llegar a tener las relaciones de mercado así lo acon - sejan. En este sentido, y además de la necesaria integración de la cláusula general, la Ley de Competencia Desleal realiza, a lo largo de su articulado, una serie de concreciones, caracterizadas por una gran amplitud, limitando de este modo la eficacia de la cláusula general y contribuyendo así a alcanzar el máximo grado posible de seguridad jurídica en este ámbito.

Los artículos 6-17 de la Ley disponen un amplio catálogo de conductas objetiva - mente desleales (contrarias a las exigencias de la buena fe), pero que contienen excepciones que dotan de licitud a determinadas conductas, lo que permite concretar un grado más el principio de buena fe. De esta forma, la buena fe se va subjetivizando, pues se incorpora como parte del supuesto de hecho de la norma jurídica, corrigiendo el posible rigor que en ocasiones puede implicar el principio de buena fe en el ámbito de una cláusula general.

Por ello cuando se acude a esta vía, además del general y abstracto perjuicio de acción contraria a la buena fe, la demanda debe dejar incardinada la acción en actuaciones concretas más que en ese criterio amplio y polivalente de la buena fe.

Acreditar de forma positiva que se realizaron actos colusorios o actos de engaño de los regulados en los preceptos de la Ley de Competencia Desleal, es decir, aquellos que concretan y cristalizan la buena fe abstracta en actos concretos, podrá montarse una estrategia que permita calificar como lícita la actuación de los usurpadores marcarios.

Por último podemos igualmente contar con la defensa de nuestra marca en vía penal, para lo cual contamos con lo regulado en el artículo 274 del Código Penal que regula el delito de usurpación de signos distintivos.

fórmate!

https://businessandcompany.com/msp

Managing Successful Programmes MSP®

Curso de Gestión de Programas de Proyectos MSP® Fundamentos

MSP®

ACCREDITED TRAINING ORGANIZATION

PeopleCert ON BEHALF OF AXELOS

Business&Co.®

Business, Technology & Best Practices, S.L.

Internet y confianza ciega

Internet, la red de redes, llegó hace décadas para quedarse entre nosotros, para facilitar la manera en la que nos relacionamos con los demás, y para conseguir en segundos lo que hasta entonces costaba horas, días e incluso semanas.

Las novedades en comunicación e interacción entre los usuarios se cuentan por miles cada día. Los sistemas de inteligencia artificial, cada vez más logrados, son el presente, cuando hace pocos años las historias de Isaac Asimov nos parecían algo irrealizable, una suerte de ciencia ficción.

Sin embargo, todos estos avances no siempre van acompañados de unos sistemas de seguridad a la altura. Desde que en 1971 fuera creado el primer virus informático, los *"malos"* han intentado, intentan e intentarán obtener beneficios de esos agujeros de seguridad o, en la mayoría de las ocasiones, de la falta de conocimiento o la confianza de cualquiera que tenga un ordenador, una tableta, un teléfono, una televisión o incluso un *smartwatch* a mano. Vivimos en la era de la conectividad.

Son muy frecuentes, durante los últimos años, las consultas que estamos recibiendo en el Despacho de gente que ha visto cómo sus cuentas bancarias han sido vaciadas. Y la práctica forense y judicial nos indica que en casi todos los casos la víctima de ese delito de estafa ha "ayudado" a ello de manera activa. ¿Y de qué manera?

Imagina que recibes un correo electrónico o un mensaje en tu móvil con una apariencia totalmente "legal". La interfaz no te hace sospechar que quien se encuentra al otro lado no tiene buenas intenciones. No es tu Banco, aunque lo parezca. No es un verdadero Príncipe Nigeriano que quiere entregarte millones de euros. No es una belleza rusa que se muere por tus huesos sin conocerte. En ese correo electrónico nos incluyen un enlace, para restablecer nuestra contraseña o para poner cara a nuestra "futura esposa"

Una vez hayamos pinchado en ese enlace, emocionados por ser nuevos ricos o haber encontrado el amor, lo que encontraremos será un gran problema, generalmente de muy difícil resolución, porque nuestra rusa de ojos azules o el director de nuestro "Banco" se encontrará en Pakistán, Nigeria u otros países en los que poco podremos hacer contra ellos.

Con esa apariencia de legalidad o de inocencia, si no extremamos las precauciones, no sería difícil que los hacker instalen un virus o un programa espía en nuestro terminal informático que les permita conocer todas nuestras claves o incluso tener acceso a todo lo que tecleemos y veamos en nuestra pantalla.

Este tipo de situaciones se puede evitar fácilmente. Dice el refranero tradicional español que “nadie da duros a cuatro pesetas”. Aplicándolo al caso que nos ocupa, hemos de ser conscientes de que ningún desconocido nos va a regalar absolutamente nada.

¿Acaso le abrirías la puerta de tu casa a un desconocido? ¿le darías las claves de tu tarjeta de crédito a alguien que te encuentres por la calle?

Ocurre, sin embargo que, en otras ocasiones, los delincuentes vayan bastante pasos por delante de los conocimientos que un usuario medio tenga sobre seguridad informática.

Hablamos, por ejemplo, de la figura delictiva conocida como “man in the middle” o “ataque de intermediario”.

Resulta cotidiano que en el tráfico mercantil las empresas comuniquen sus pedidos o envíen sus Facturas a través de correo electrónico. En un gran número de ocasiones los servidores de correo electrónico, ya sea de la empresa remitente o de la destinataria, no se encontrarán encriptados, las redes inalámbricas de los terminales que

CONTINÚA EN PRÓXIMA PÁGINA

utilicen estén configuradas con la contraseña que el router trae por defecto, o incluso cometeremos la torpeza de enviar información sensible o confidencial desde redes de acceso público.

Este tipo de agujeros de seguridad son aprovechados por los hacker informáticos para insertarse e interceptar las comunicaciones, teniendo acceso al contenido de las mismas.

Con ello, es decir, conociendo por ejemplo el importe de una Factura, así como el correo electrónico del remitente y el destinatario, les resulta tremendamente sencillo modificar los documentos o el contenido de los propios correos y remitir un nuevo correo con esa Factura modificada, o solicitar que el pago se realice en otro número de cuenta distinto, controlado por el propio delincuente.

El destinatario, que verá el nombre de su remitente conocido en el encabezado, así como un asunto también conocido, no sospechará de que se trata de un correo electrónico fraudulento, salvo que observe con detenimiento la dirección de correo del propio remitente, que suele ser similar (pero no idéntica) a la del remitente original.

Como decimos, este tipo de ataques, que provocan perdidas cuantiosas, así como una merma en la confianza entre empresas.

¿Cómo podemos evitar ser víctimas de este tipo de estafas?

Tal y como señala el Instituto Nacional de Ciberseguridad (INCIBE), a pesar de que resulta difícil detectar cuándo se está sufriendo un ataque informático de esta naturaleza, podemos tomar medidas para tratar de minimizar el riesgo, como por ejemplo:

- Accediendo a sitios web seguros con certificado (HTTPS).

- Modificando la contraseña por defecto de la red wifi, y habilitando una red específica de invitados, si algún tercero tiene que conectarse a nuestra red.

- Actualizando el software de nuestros equipos.

- Activando la autenticación en dos pasos.

- Evitando conectar nuestros equipos a redes wifi abiertas.

- Si nos vemos obligados a hacerlo, evitando remitir información personal, confidencial o sensible.

- Evitando abrir enlaces o documentos de correo electrónico recibidos de desconocidos.

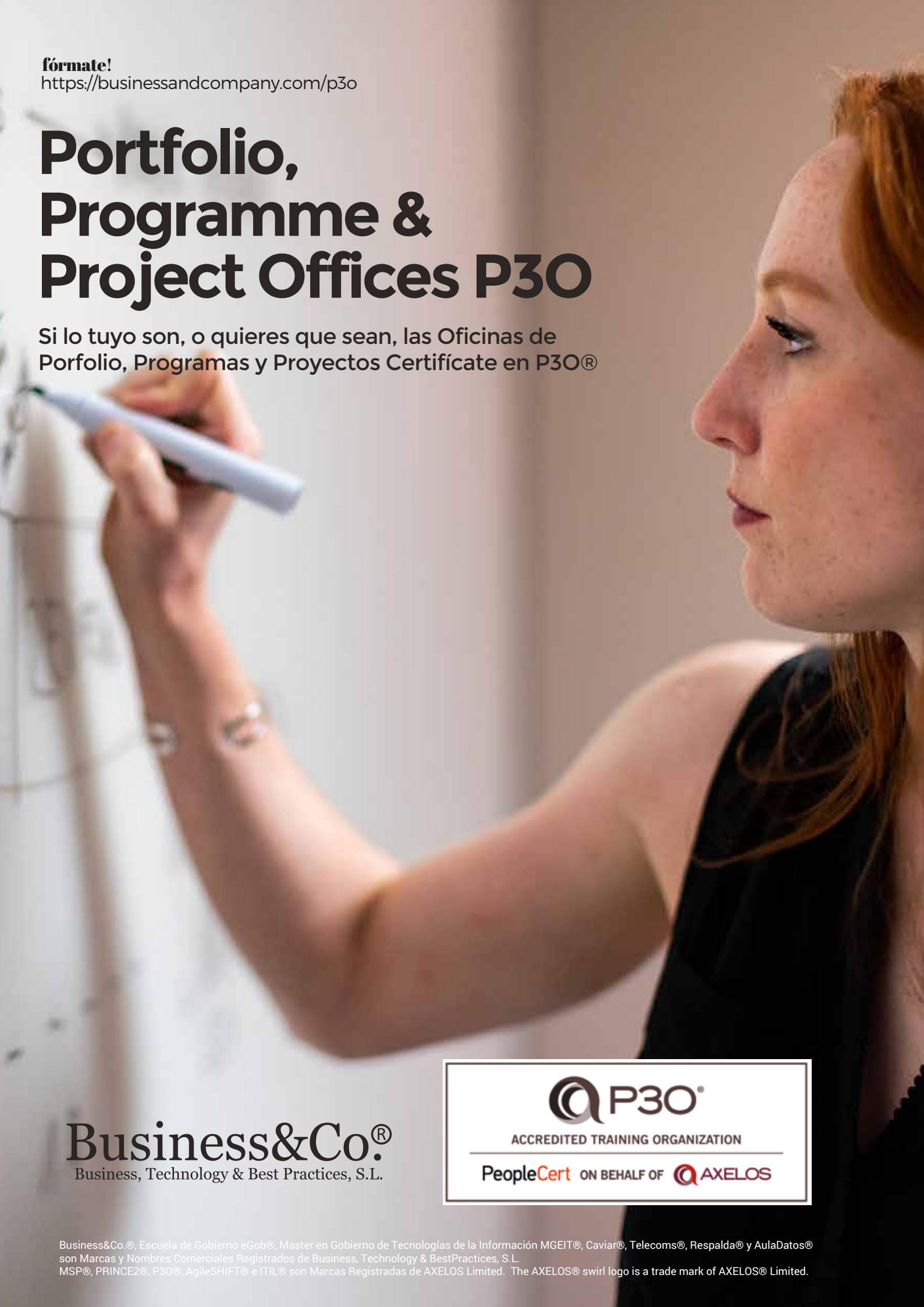
- Comprobando la dirección de correo electrónico del remitente, haciendo caso omiso al nombre del encabezado, confirmando incluso por teléfono que el remitente ha querido enviar ese correo electrónico.

De esta manera, iremos “acorazando” nuestras redes, nuestros sistemas y nuestras comunicaciones, pudiendo disfrutar de las bondades de internet de manera mucho más segura.

fórmate!
https://businessandcompany.com/p3o

Portfolio, Programme & Project Offices P3O

Si lo tuyo son, o quieres que sean, las Oficinas de Porfolio, Programas y Proyectos Certifícate en P3O®



Business&Co.®
Business, Technology & Best Practices, S.L.

P3O®
ACCREDITED TRAINING ORGANIZATION
PeopleCert ON BEHALF OF AXELOS

La Covid-19 y el acoso como delito

Recuerda, querido lector, qué estabas haciendo el día 1 de enero de 2020. Suponemos que, quizá con una pequeña resaca, imaginando un nuevo año lleno de proyectos, de ilusiones, de viajes… en fin, de vida.

Imagina ahora, querido lector, que eres un joven adolescente, nacido en pleno Siglo XXI, cuyos valores de grupo pasan por la extrema exhibición de tu imagen, por los planes compartidos en "manada", delante y detrás de una pantalla de un ordenador, de una tableta, de un teléfono móvil…

Siéntate un año después y rememora qué ha sido de tu vida, querido lector, a lo largo del 2020 que ya nos abandonó. Sobre todo desde el mes de marzo.

Quizá nos parezca muy lejano, y ojalá quede en nuestras vidas como una anécdota que contar a nuestros nietos. Estuvimos más de tres meses encerrados en casa; siete días a la semana; veinticuatro horas al día. Saliendo a aplaudir a los héroes sanitarios y a quien se enfrentaba a un virus desconocido en su puesto de trabajo, todos los días puntualmente a las ocho. ¿Y qué hicimos las otras veintitrés horas y cincuenta y cinco minutos?

Hubo quien, afortunado, pudo disfrutar de un patio, un jardín o una terraza en la que poder hacer algo de ejercicio o tomar el sol.

Pero la mayoría de nosotros, con no tanta suerte, nos vimos en la obligación de comunicarnos con el resto a través de las redes sociales y los sistemas de mensajería instantánea. Descubrimos Zoom, Google Meet, Videochat de Whatsapp, Skype…

Y descubrimos que de puertas para dentro, en nuestras propias casas, también le podíamos sacar partido a Facebook, Twitter, Instagram, Tik Tok…

Tres meses de besos y abrazos virtuales. Tres meses de clases virtuales. Tres meses de Juicios y asistencias a detenidos virtuales.

Imagina ahora, querido lector, cómo hubiera sido el confinamiento sin tecnología. Sin poder ver y saber de tus seres queridos de una manera tan natural como la que hemos vivido.

Definitivamente, una vez más, tenemos que llegar a la conclusión de que toda esa programación de unos y ceros, la tecnología sin cables y el fácil acceso a las comunicaciones del Siglo XXI han llegado a nuestras vidas para hacerlas más fáciles.

O no…

Las redes sociales y los sistemas de comunicación a través de internet nos permiten contactar con nuestros seres queridos, pero también con aquéllos a los que no apreciamos tanto. Una pátina de anonimato, incluso al acceso de los más legos en tecnología, que nos dota de una coraza de impunidad ante cualquier comentario, incluso los más reprobables.

Volvamos a esos adolescentes, nativos digitales, y bullentes de hormonas, que se encuentran de la noche a la mañana encerrados en casa, sin poder interactuar de manera directa y personal con sus iguales y que descubren en las redes sociales una manera sencilla de poder "imitar" esa interactuación.

Desafortunadamente a lo largo del último año estamos contando por cientos las consultas que están llegando al Despacho relacionadas con prácticas poco deseables, sobre todo entre alumnos de Secundaria, que consisten en atacar al más débil de grupo o de la clase; una especie de "caza" que queda plasmada por escrito, con insultos, menosprecios, incluso amenazas. Algo que se vive en el día a día de en muchas aulas de nuestro país, pero que en plena pandemia ha dado el salto a internet.

Ante este tipo de comportamientos, la panoplia de delitos recogidos por el Código Penal, y es algo que deberían conocer nuestros jóvenes, actúa en defensa de las víctimas; víctimas que en muchas ocasiones se encuentran sin salida o no conocen las posibles ayudas que pueden recibir, y llevan a cabo intentos autolíticos.

CONTINÚA EN PRÓXIMA PÁGINA

Imagina, querido lector, que es tu hijo el que a través de sus redes sociales insulta, veja, amenaza o coacciona a otro joven. Desde la "inocencia" de un menor de edad (autores en la mayoría de las ocasiones) estos son los delitos que prevé el Código Penal, para el "ciberacoso" o "ciberbuylling".

Artículo 172.ter.1.
Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:

1.ª La vigile, la persiga o busque su cercanía física.

2.ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.

3.ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.

4.ª Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella.

Artículo 169.
El que amenazare a otro con causarle a él, a su familia o a otras personas con las que esté íntimamente vinculado un mal que constituya delitos de homicidio, lesiones, aborto, contra la libertad, torturas y contra la integridad moral, la libertad sexual, la intimidad, el honor, el patrimonio y el orden socioeconómico.

Artículo 172.1.
El que, sin estar legítimamente autorizado, impidiere a otro con violencia hacer lo que la ley no prohíbe, o le compeliere a efectuar lo que no quiere, sea justo o injusto, será castigado con la pena de prisión de seis meses a tres años o con multa de 12 a 24 meses, según la gravedad de la coacción o de los medios empleados.

Cuando la coacción ejercida tuviera como objeto impedir el ejercicio de un derecho fundamental se le impondrán las penas en su mitad superior, salvo que el hecho tuviera señalada mayor pena en otro precepto de este Código.

Artículo 143.
El que induzca al suicidio de otro será castigado con la pena de prisión de cuatro a ocho años.

Artículo 173.
El que infligiera a otra persona un trato degradante, menoscabando gravemente su integridad moral, será castigado con la pena de prisión de seis meses a dos años.

Como siempre, desde Abogado Amigo tratamos de concienciar respecto del buen uso de las tecnologías y del control parental de las mismas, sobre todo en la época que nos está tocando vivir.

Expansión en LegalTech

LegalTech es la palabra de moda para el futuro de la abogacía. El nuevo entorno económico nacido en la era post COVID ha hecho que la tecnología se vea como salvadora de las cuentas de muchos bufetes. Sin embargo en Abogado Amigo llevamos trabajando en la creación de proyectos tecnológicos innovadores desde hace años, cuando en lugar de LegalTech se llamaba "ser rarito".

El sector jurídico es uno de los últimos en llegar a la transformación digital. En el marco de un mercado en constante evolución en el que las nuevas tecnologías de la información han transformado muchos de los procesos productivos, la abogacía sin embargo aun conserva muchas barreras al desarrollo de nuevas formas de desarrollar el negocio jurídico.

Sin embargo las necesidades de los clientes y el entorno económico cambiante de los últimos meses obligan a las firmas de abogados a responder de forma ágil y eficaz a los retos planteados o agravados por la pandemia.

Los proyectos de aplicación de tecnología al ámbito legal se desarrollan fundamentalmente en dos lineas o niveles: los que abarcan la digitalización de un proceso o servicio y los que formulan una transformación digital o modifican la forma de entender la gestión de un proceso o servicio. En la adaptación tecnológica no podemos considerar ni mejor ni peor procesos por el grado de transformación que impliquen, si no por la utilidad que reporten al profesional. Existen procesos tecnológicos que justamente por ser sencillos, de fácil implementación y que no suponen modificación de procesos que aportan una utilidad cierta y real respecto de las vías utilizadas con anterioridad. Es por ello que LegalTech puede estar en todas las partes del proceso productivo legal, desde lo más complejo, como la gestión jurídica de expedientes realizada por inteligencia artificial, hasta los más sencillo como la inclusión de profesionales en directorios de abogados.

¿EN QUÉ CONSISTEN LOS PROYECTOS DE DIGITALIZACIÓN EN LEGALTECH?

La digitalización se define como la transformación de un producto analógico en formato digital. Así por ejemplo, la digitalización de los documentos aportados a una demanda nos da como resultado el expediente digital que en sí mismo es el mismo producto y responde a las mismas necesidades que el expediente analógico. Implantar los expedientes judiciales digitales en nuestra administración de Justicia no ofrece ninguna transformación, sólo digitaliza un proceso previo. Ahora bien, la digitalización puede ser el trampolín para iniciar procedimientos nuevos que impliquen la transformación de nuestros procesos. En el ejemplo del expediente digital, podremos transformar las notificaciones automatizándolas, creando procesos como la citación a vista telemática de forma automática, o generando estadísticas sobre los conflictos solventados por un determinado juzgado.

CONTINÚA EN PRÓXIMA PÁGINA

La digitalización en términos generales, no sólo puede suponer un ahorro en los costes de gestión, si no que permite (y esto es lo más importante) tener datos. Cualquier documento en formato digital permite que los datos que contiene sean objeto de un tratamiento más rápido y con mayor volumen que en los documentos analógicos. Y cuando tenemos datos comienza la magia.

Lo datos, convenientemente tratados nos darán información. La información adecuadamente estudiada nos dará conocimiento. Si del conocimiento conseguimos adelantar conclusiones llegaremos a la sabiduría, y eso nos dará una posición de ventaja frente a nuestros competidores.

Cualquier base de datos sirve para tomar una decisión empresarial en base a los datos que en ella se almacenan. El valor de esa base será igual al valor de la decisión que soporta. Si la digitalización nos permite tratar los datos a mayor velocidad, nuestras decisiones podrán ser más rápidas, más flexibles y más acertadas, permitiendo que obtengamos mayor aprovechamiento de los datos de que dispone nuestra organización.

¿EN QUÉ CONSISTEN LOS PROYECTOS DE TRANSFORMACIÓN DIGITAL EN LEGALTECH?

La Transformación Digital es la adaptación de los procesos y recursos legales al entorno digital. La Transformación implica el conocimiento de los procedimientos en los que se basa el servicio jurídicos, con una adecuada definición de todos ellos, encontrando aquellos procesos que pueden ser modificados mediante la utilización de tecnología.

Transformación Digital es por lo tanto un cambio en lo que se hace (no sólo en cómo se hace, como sucedía en la Digitalización). La Transformación Digital implica el cambio de la cultura del sector jurídico.

Es por esto que las soluciones tecnológicas nacidas del LegalTech serán (o no) herramientas útiles para la transformación del sector legal, pero necesariamente deberán estar alineadas con nuestra estrategia a largo plazo de cambio de cultura.

En el momento de planificar la Transformación Digital debemos contar con todos los recursos de nuestra organización legal. Existen recursos tangibles y consumibles como son los recursos económicos, los datos, las aplicaciones, y los bienes muebles e inmuebles. Pero hay recursos que son mucho más decisivos en cuanto a habilidades, como son la cultura de la dirección y de la organización, el nivel de madurez de los procesos, y el conocimiento.

En la era digital la existencia de procesos, seguir dichos procesos y acumular conocimiento puede resultar de mayor valor para competir que los recursos financieros. El mismo principio aplica para los profesionales, el conocimiento, el seguimiento de procesos, y la flexibilidad ante el cambio son los activos más valorados.

Tanto en una línea como en otra, los próximos años van a suponer una transformación profunda de la profesión de abogado tal y como la hemos conocido en los últimos 2.000 años. El cambio de paradigma y la entrada imparable de la tecnología en la profesión, así como la adopción de cambios tecnológicos por las administraciones, llevarán a la necesidad de adaptación de todos los profesionales implicados.

Toca ser como el bambú.

fórmate!
https://businessandcompany.com/cobit

Tu vida puede depender de la tecnología

COBIT® 2019 Marco de Gobierno y Gestión de la Tecnología

La Implementación de un Marco de Gobierno y Gestión de Tecnologías de la Información permite conocer la salud global de los Sistemas de Información de los que depende los procesos habituales de una organización, sin un adecuado Marco de Gobierno y Gestión se podrá trabajar la seguridad, privacidad y otros aspectos de manera disociada tampoco se podrá garantizar que se estén teniendo en cuenta todos los factores necesarios para una adecuada operación. COBIT® aporta confianza.

Business&Co.®
Business, Technology & Best Practices, S.L.

Nace el Legal Project Management

El Project Management son un conjunto de conocimientos, herramientas y técnicas con las que se procura gestionar racionalmente un proyecto, los riesgos que son inherentes al mismo y las excepciones que pueden surgir en su desarrollo. Pero… ¿tienen proyectos los abogados? Siguiendo a PRINCE2 puede definirse un proyecto como "una organización temporal que se crea con el propósito de entregar uno o más productos comerciales de acuerdo a un Business Case convenido". Y si nos fijamos un poco, cualquier encargo que recibe un abogado en su carrera es el compromiso adquirido de entregar en un plazo determinado un determinado "producto" (dictamen, demanda, contrato, propuesta…) conforme a un objetivo perseguido (reclamar una cantidad, tener seguridad en una relación comercial, valorar riesgos de una operación…).

De esta forma la gestión jurídica puede ser entendida como una gestión de proyectos. Cuando un encargo se trata como un proyecto nos permite definir, gestionar, valorar y mejorar la forma de trabajo utilizando las metodologías creadas con la finalidad de gestionar proyectos.
Pues la persona que implanta y hace el seguimiento de la metodología dentro del despacho es a quien conocemos como Legal Project Manager, es decir, el especialista en aplicar los conocimientos del Project Management al desarrollo de servicios del ámbito jurídico.

El Project Management no es una única metodología si no que incluye una multitud de metodologías diversas que buscan la gestión del proyecto con matices o singularidades:

- **Gestión del proyecto o encargo profesional** orientado a resultados como puede ser SCRUM, Kanban, Lean Startup o PRINCE2 Agile. En el ámbito jurídico puede ser indicado para entornos de alta volatilidad como la gestión de crisis de empresa, ERES o expansiones internacionales de compañías.
- **Gestión de proyectos adaptándolos a la mejora continua como PRINCE2**. En el ámbito jurídico es increíblemente práctico contar con una gestión de proyectos para organización de actividad contenciosa del despacho.

Las metodologías de Project Management nos permiten tratar con seriedad y profundidad cualquier proyectos sin importar la cuantía del mismo o su ámbito temporal. Además ofrecen herramientas que son básicas en el entorno jurídico como puede ser el caso de definición de beneficios y contrabeneficios, y resultan fundamentales para la programación del trabajo y de la carga de cada uno de los profesionales que forman parte de la estructura del Bufete.

CONTINÚA EN PRÓXIMA PÁGINA

El Legal Project Manager implanta una o varias metodologías en el funcionamiento de la actividad ordinaria del bufete para:

- Lograr mejorar la eficacia de su trabajo, al saber cada uno de los operadores la información que debe recibir, las tareas que debe ejecutar y el resultado que debe entregar.
- Definir adecuadamente los roles evitando vacíos de toma de decisión o tomas de decisión por personas no adecuadas. Gracias a una adecuada gestión de proyectos legales podemos garantizar la trazabilidad de la tramitación de un asunto con conocimiento de los responsables del mismo, incluso cuando se impliquen otros compañeros en la ejecución de alguna tarea. Siendo siempre la distribución de roles tremendamente importante en cualquier estructura empresarial, en el ámbito legal en el que el abogado es responsable directamente de la gestión realizada (incluso patrimonialmente) esta es aún más relevante.
- Obtener mejores resultados mediante la implantación de mejoras continuas que faciliten la identificación de errores o ineficiencias y la corrección de las mismas.
- Ordenar los conocimientos adquiridos por la estructura jurídica y poder ponerlos a disposición de otros miembros de bufete cuando sea necesario.

Por último el Legal Project Manager debe ser adaptable, de forma que no puede pretender la implantación de una metodología concreta en todos los supuestos ni para todos los proyectos, si no que en muchos casos deberá simplificar, en otros ampliar y en todos adaptar, los conocimientos de la metodología a lo requerido por la situación concreta.

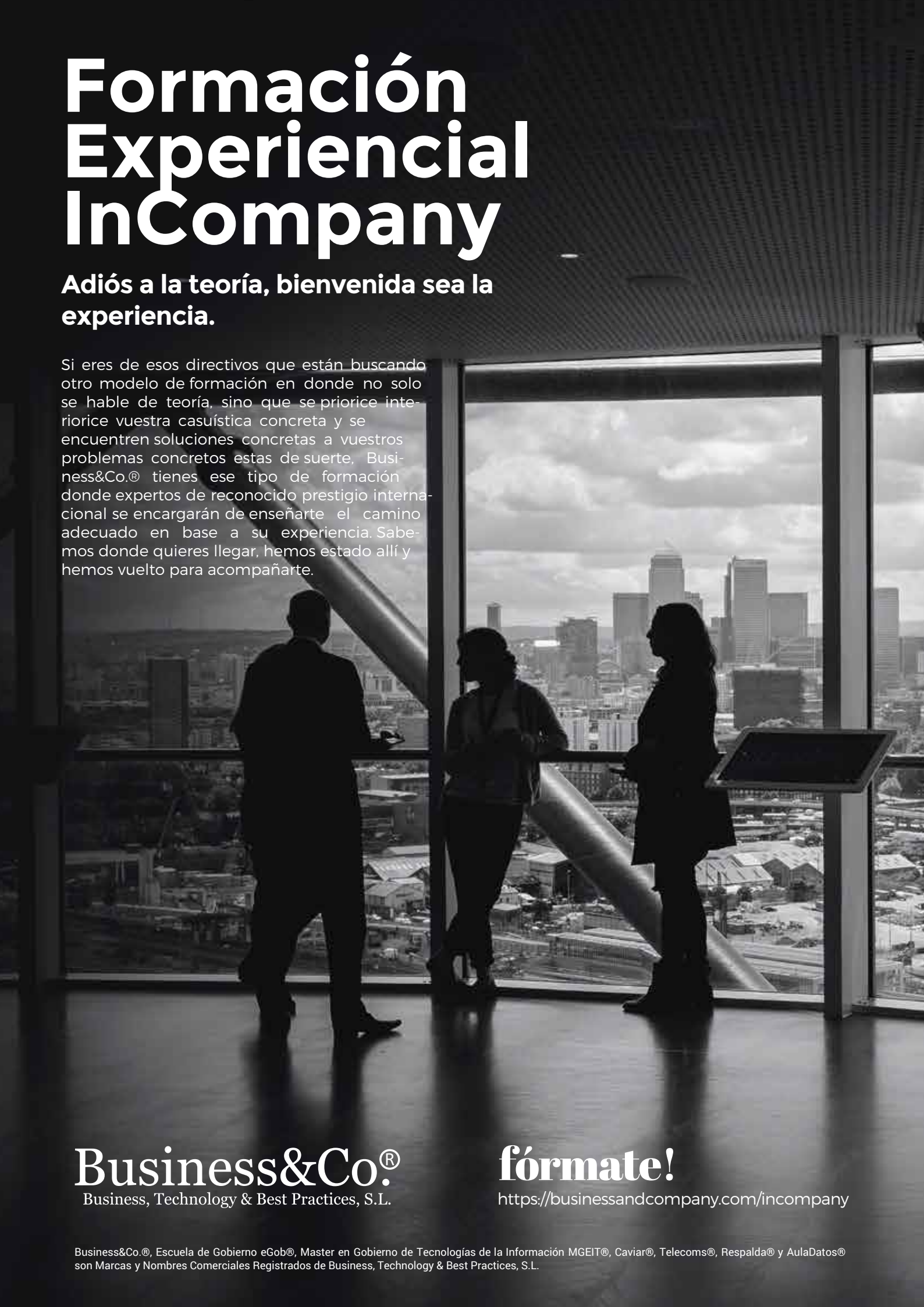
A diferencia de lo que sucede en muchos entornos empresariales en los que se implanta un modelo de Project Management, en el caso del ámbito legal el Legal Project Manager debe contar con que su trabajo no sea entendido o comprendido por los abogados que reciban las nuevas formas de gestión. Aunque todas metodologías buscan la implicación del personal, la resistencia al cambio es una de las características propias de esta profesión por lo que un buen Manager necesitará una increiblemente desarrollada capacidad de gestionar los recursos humanos dentro del proyecto, creando vínculos con cada uno de los implicados para sientan todos los beneficios de la transformación.

Los despachos de abogados ya han comenzado su gestión empresarial y, y como tales estructuras empresariales, requerirán cada vez de más profesionales especializados en el Legal Management en los próximos años. ¿estás listo para certificarte en metodologías de gestión?

Formación Experiencial InCompany

Adiós a la teoría, bienvenida sea la experiencia.

Si eres de esos directivos que están buscando otro modelo de formación en donde no solo se hable de teoría, sino que se priorice interiorice vuestra casuística concreta y se encuentren soluciones concretas a vuestros problemas concretos estas de suerte, Business&Co.® tienes ese tipo de formación donde expertos de reconocido prestigio internacional se encargarán de enseñarte el camino adecuado en base a su experiencia. Sabemos donde quieres llegar, hemos estado allí y hemos vuelto para acompañarte.



Business&Co.®
Business, Technology & Best Practices, S.L.

fórmate!
https://businessandcompany.com/incompany

Vamos a poner el Derecho del revés

Mucho tiempo ha pasado desde que la Lex Cincia de la República Romana prohibía a los abogados cobrar estipendio alguno por sus servicios puesto que defender la Justicia y aplicar el derecho era un honor de todo ciudadano. De hecho, las minutas aún las seguimos denominando "HONORarios". Desde entonces, han cambiado las leyes, los legisladores, la forma de estudiar, la forma de compilar la legislación… pero poco ha cambiado respecto a la forma de ofrecer los servicios jurídicos. Igual que en el foro romano el acusado elegía entre los abogados que se encontraban allí en el momento del juicio según las recomendaciones que había recibido y la fama de cada uno de los jurisconsultos, hasta hace pocos años el cliente elegía entre los abogados por su placa, la ubicación de su despacho o las referencias.

Sin embargo la tecnología lo cambia todo y el mundo de los servicios jurídicos no podía estar al margen de ello. Llegó internet, se democratizó la publicidad, se acercó al abogado, se escriben cientos de blogs y se compartieron las fuentes legislativas, pero la función del abogado seguía siendo hasta cierto punto "oscura". Lo que dice la ley y lo que se interpreta no siempre coinciden, hay un conocimiento en la defensa de la legalidad que hace que el cliente no entienda qué o porqué está pagando, y si el cliente no sabe el motivo del precio (por muy justo que sea) siempre lo considerará caro.

Con este panorama hace ya algunos años la Universidad de Stanford lanzó la idea de aplicar los conceptos del "Design Thinking" al Derecho y a los servicios jurídicos. Design Thinking es una metodología que propugna aplicar procesos creativos al diseño de productos y servicios enfocados principalmente a la forma en la que el usuario usa o desea usar los mismos. De esta forma el servicio no es creado por el diseñador (de dentro a fuera) si no que el diseño viene marcado por la interacción del usuario y el diseñador debe soportar ese resultado (de fuera a dentro).

CONTINÚA EN PRÓXIMA PÁGINA

Si aplicamos el Design Thinking a los servicios jurídicos nace el Legal Design. Legal Design es el paradigma que procura rediseñar el derecho para hacerlo comprensible y aplicable de forma amigable para el usuario y sin tener puntos oscuros o interpretables.

Quizá la aplicación más conocida de esta metodología sea la privacy by design que ha sido acogida por el propio Reglamento General de Protección de Datos. Pero las aplicaciones de esta nueva forma de pensar los servicios jurídicos son mucho más profundas y disruptivas.

Frente a la imagen tradicional de un abogado que dice conceptos de no se entienden, que habla un lenguaje oscuro, y por ese motivo es buen abogado o buen profesional, el Legal Design ha abierto una corriente que facilita y acerca los servicios y productos legales para facilitar la contratación de los mismos.

Legal Design quiere crear productos jurídicos fáciles de entender para los usuarios. Por lo tanto los servicios jurídicos deberán centrarse en cumplir con determinadas características:

TRANSPARENCIA: en qué consiste el servicio que se contrata y que resultado se va a obtener del mismo. La descripción del servicio que se presta permite ajustar las expectativas del cliente y la oferta del profesional.

PRECIO CONOCIDO: Los honorarios deben ser conocidos de antemano, sin letra pequeña, sin condicionantes. no necesariamente un servicio "design" debe ser más barato, aunque el conocimiento de procesos, servicios y resultados sin duda permitirá aplicar mejoras que impliquen rebaja en el precio para el usuario final.

INNOVACIÓN: repensar el servicio deseado por el cliente (en lugar del ofrecido por el abogado) nos lleva a conseguir lanzar nuevos servicios o nuevos "paquetes" de servicios que ayuden al cliente a identificar sus necesidades.

FLEXIBILIDAD: Los servicios diseñados desde el cliente permiten al cliente adaptarlos a sus necesidades.

Cuando todos estos enunciados los trasladamos a los productos jurídicos nos encontramos con documentos legales más comprensibles y etiquetados adecuadamente con enunciados claros que permiten entender el contenido de cada regulación. Los contratos, las condiciones legales de un sitio web, los consentimientos a efectos de LOPD o incluso, ¿porqué no?, las demandas se organizan de forma simplificada, con anotaciones y enunciados claros que permiten identificar qué se regula en cada apartado, sin olvidar los aspectos más técnicos y precisos que se redactarán con un lenguaje que impida (o dificulte) las dobles interpretaciones.

Legal Design no es únicamente útil y preciada en la relación del servicio jurídico con el cliente final. La simplificación de procesos y la estandarización de los mismos abre puertas muy importantes al sector jurídico combinadas con el uso de big data y machine learning. La aplicación del legal design a las estructuras de procesos, servicios y comunicación facilita la implantación y desarrollo de nuevos productos y servicios y el desarrollo de tecnologías como la Inteligencia Artificial.

fórmate!
https://businessandcompany.com/itil

El Sistema de Valor del Servicio de ITIL®4

...o todavía andas pensando en el ciclo de vida del Servicio.

Business&Co®
Business, Technology & Best Practices, S.L.

ITIL®
ACCREDITED TRAINING ORGANIZATION
PeopleCert ON BEHALF OF AXELOS

Digitalización de un Bufete... o Transformación Digital del Derecho

O dicho con otras palabras, ¿cómo me puede hacer ganar dinero a un Bufete de Abogados la Digitalización y Transformación Digital?

En los últimos números de Tecnología y Sentido Común hemos repasado aspectos fundamentales para la transformación de los servicios jurídicos tales como la llegada del Legal Project Management o el replanteamiento de la forma de vender los servicios mediante el Legal Design. En muchas ocasiones los negocios ven la tecnología como tabla de salvación para vender más, para vender más caro, para captar más clientes, para gastar menos… Y en la coyuntura actual, los despachos de abogados no son la excepción.
Pero debemos decirlo muy clarito: la tecnología no es la solución de ningún problema y mucho menos el de no ser rentables.
La tecnología es la herramienta para implantar soluciones definidas por nuestro Bufete.

Para entender qué es Digitalización y Transformación Digital, y cómo pueden ayudarnos en un despacho de abogados, primero debemos saber qué es lo que no son: No es Digitalización ni Transformación Digital la implantación de nuevas tecnologías (puede o no ser necesario cambiar nuestra tecnología para digitalizarnos); tampoco lo es gastar más en tecnología (aunque en algunos casos será necesario); no lo será vender on line (puesto que no es un mero cambio de canal); no tiene que ver con la gestión de redes sociales;

Es en esta encrucijada cuando las soluciones de Legaltech y el desarrollo de nuestra propia visión de ver la tecnología cobra sentido.
¿Tiene tu bufete una forma particular de ver el Derecho? Pues ahora aplica esa personalidad a la forma de relacionarse con la tecnología y deja que el negocio fluya.

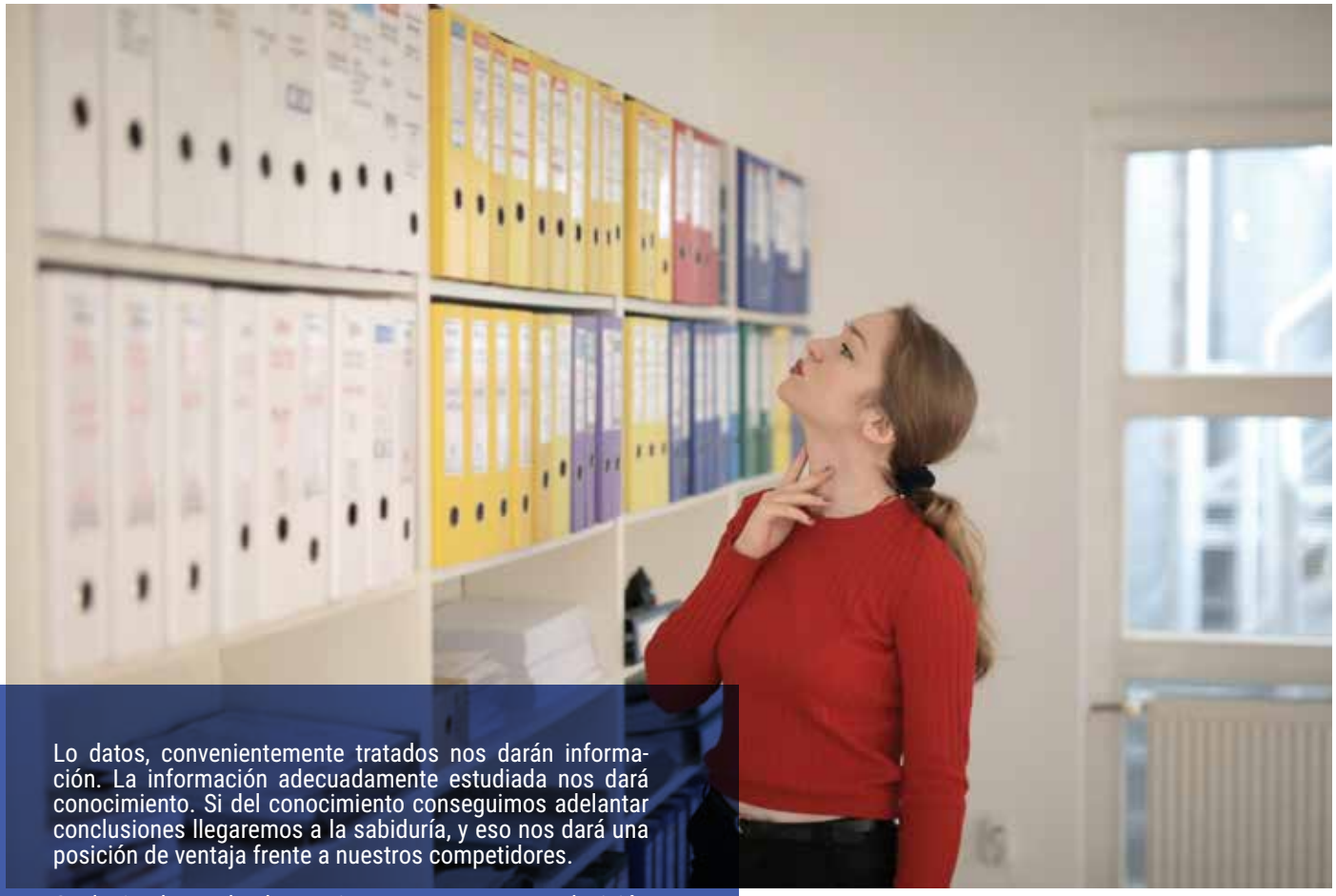
En conclusión: La Tecnología sin control no sirve de nada

¿QUÉ ES DIGITALIZACIÓN DE UN DESPACHO DE ABOGADOS?

La digitalización se define como la transformación de un producto analógico en formato digital. Así por ejemplo, la digitalización de la factura nos da como resultado la factura digital que en sí misma es el mismo producto y responde a las mismas necesidades que la analógica. Implantar las facturas digitales en nuestro despacho no ofrece ninguna transformación, sólo digitaliza un proceso previo. Lo mismo podemos predicar de la implantación de LEXNET.
Ahora bien, la digitalización puede ser el trampolín para iniciar procedimientos nuevos que impliquen la transformación de nuestros procesos. En el ejemplo de la factura digital, una vez digitalizada podremos transformar la entrega de la factura sustituyendo su envío por correo postal por una puesta a disposición del cliente en una plataforma que es un proceso absolutamente diferente: pasar del envío a la descarga.

La digitalización en términos generales, no sólo puede suponer un ahorro en los costes de gestión, si no que permite (y esto es lo más importante) tener datos. Cualquier documento en formato digital permite que los datos que contiene sean objeto de un tratamiento más rápido y con mayor volumen que en los documentos analógicos. Y cuando tenemos datos comienza la magia.

CONTINÚA EN PRÓXIMA PÁGINA



Lo datos, convenientemente tratados nos darán información. La información adecuadamente estudiada nos dará conocimiento. Si del conocimiento conseguimos adelantar conclusiones llegaremos a la sabiduría, y eso nos dará una posición de ventaja frente a nuestros competidores.

Cualquier base de datos sirve para tomar una decisión empresarial en base a los datos que en ella se almacenan. El valor de esa base será igual al valor de la decisión que soporta. Si la digitalización nos permite tratar los datos a mayor velocidad, nuestras decisiones podrán ser más rápidas, más flexibles y más acertadas, permitiendo que obtengamos mayor aprovechamiento de los datos de que dispone nuestra organización.

¿QUÉ ES TRANSFORMACIÓN DIGITAL?

La Transformación Digital es la adaptación de los procesos y recursos empresariales al entorno digital. La Transformación implica el conocimiento de los procedimientos de tu Bufete de abogados, con una adecuada definición de todos ellos, encontrando aquellos procesos que pueden ser modificados mediante la utilización de tecnología.

Transformación Digital es por lo tanto un cambio en lo que se hace (no sólo en cómo se hace, como sucedía en la Digitalización). La Transformación Digital implica el cambio de la cultura del proveedor de servicios jurídicos.

Es por esto que las soluciones tecnológicas serán (o no) herramientas útiles para nuestra Transformación en Legaltech, pero necesariamente deberán estar alineadas con nuestra estrategia a largo plazo de cambio de cultura en la prestación de servicios jurídicos.

En el momento de planificar la Transformación Digital debemos contar con todos los recursos de nuestro Bufete. Existen recursos tangibles y consumibles como son los recursos económicos, los datos, las aplicaciones, y los bienes muebles e inmuebles. Pero hay recursos que son mucho más decisivos en cuanto a habilidades, como son la cultura de la dirección y de la organización, el nivel de madurez de los procesos, y el conocimiento.

En la era digital la existencia de procesos, seguir dichos procesos y acumular conocimiento puede resultar de mayor valor para competir que los recursos financieros. El mismo principio aplica para los profesionales, el conocimiento, el seguimiento de procesos, y la flexibilidad ante el cambio son los activos más valorados.

ALINEACIÓN ENTRE OBJETIVOS EMPRESARIALES Y USO DE TECNOLOGÍAS

Por lo tanto Legaltech no es la salvación sino una necesidad. Y en primer lugar el Bufete debe ser consciente de que se traducirá en un gasto que debe responder a los objetivos fijados para la prestación de nuestro servicio.
Así, el departamento de tecnología es en realidad un departamento de servicio a los letrados del Bufete. Si consideramos la tecnología como uno de los servicios internos de nuestro despacho podremos evaluar y medir el rendimiento de cada inversión en relación a los objetivos marcados para el desarrollo.

Sólo desde una visión holística del desarrollo de los objetivos del despacho, podremos definir las necesidades tecnológicas de nuestras estructuras y la rentabilidad y conveniencia de cada transformación.

Transformemos nuestro Bufete para que tenga una larga y próspera vida en el mundo digital.

#BestPractices #BetterProfessionals

Cursos oficiales de Certificación

septiembre

GOBIERNO I&T

COBIT® 2019 FUNDAMENTOS

PRIMERA SESIÓN:
Viernes 3 de Septiembre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Sábado 4 de Septiembre de 2021 de 09:00 a 14:00 horas

TERCERA SESIÓN:
Viernes 10 de Septiembre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN:
Sábado 11 de Septiembre de 2021 de 09:00 a 14:00 horas

GESTIÓN DE SERVICIOS

ITIL® 4 FUNDAMENTOS

PRIMERA SESIÓN:
Martes 7 de Septiembre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Jueves 9 de Septiembre de 2021 de 16:00 a 21:00 horas

TERCERA SESIÓN:
Martes 14 de Septiembre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN
Jueves 16 de Septiembre de 2021 de 16:00 a 21:00 horas

GESTIÓN POR PROCESOS

BPM PROFESIONAL ISO/IEC 19510

PRIMERA SESIÓN:
Viernes 17 de Septiembre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Sábado 18 de Septiembre de 2021 de 09:00 a 14:00 horas

TERCERA SESIÓN:
Viernes 24 de Septiembre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN
Sábado 25 de Septiembre de 2021 de 09:00 a 14:00 horas

GESTIÓN DE SERVICIOS

ITIL® 4 STRATEGIST: DIRECT, PLAN & IMPROVE

PRIMERA SESIÓN:
Martes 21 de Septiembre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Jueves 23 de Septiembre de 2021 de 16:00 a 21:00 horas

TERCERA SESIÓN:
Martes 28 de Septiembre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN
Jueves 30 de Septiembre de 2021 de 16:00 a 21:00 horas

octubre

GESTIÓN DE SERVICIOS

ITIL® 4 FUNDAMENTOS

PRIMERA SESIÓN:
Viernes 1 de Octubre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Sábado 2 de Octubre de 2021 de 09:00 a 14:00 horas

TERCERA SESIÓN:
Viernes 8 de Octubre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN
Sábado 9 de Octubre de 2021 de 09:00 a 14:00 horas

GOBIERNO I&T

COBIT® 2019 FUNDAMENTOS + ISO 38500 PROFESIONAL

PRIMERA SESIÓN:
Martes 5 de Octubre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Jueves 7 de Octubre de 2021 de 16:00 a 21:00 horas

TERCERA SESIÓN:
Martes 12 de Octubre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN:
ISO/IEC 38500 a elegir por el Alumno.

GESTIÓN DE PROYECTOS

PRINCE2® FUNDAMENTOS

PRIMERA SESIÓN:
Viernes 15 de Octubre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Sábado 16 de Octubre de 2021 de 09:00 a 14:00 horas

TERCERA SESIÓN:
Viernes 22 de Octubre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN:
Sábado 23 de Octubre de 2021 de 09:00 a 14:00 horas

GESTIÓN OFICINAS DE PROYECTOS

P3O® FUNDAMENTOS

PRIMERA SESIÓN:
Martes 19 de Octubre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Jueves 21 de Octubre de 2021 de 16:00 a 21:00 horas

TERCERA SESIÓN:
Martes 26 de Octubre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN:
Jueves 28 de Octubre de 2021 de 16:00 a 21:00 horas

Business&Co®
Business, Technology & Best Practices, S.L.

Más información en
https://javierperis.com/formacion-oficial/