CIBERSEGURIDAD EN 9 PASOS

EL MANUAL SOBRE SEGURIDAD DE LA INFORMACIÓN PARA EL GERENTE

DEJAN KOSUTIC

Ciberseguridad en 9 pasos

El manual sobre seguridad de la información para el gerente

Por Dejan Kosutic

Página sobre derechos de autor

Título: Ciberseguridad en 9 pasos

Subtítulo: El manual sobre seguridad de la información para el gerente

Autor: Dejan Kosutic

Publicado por: EPPS Services Ltd, Zagreb

http://www.iso27001standard.com/

ISBN: 978-953-57452-2-8

Primera edición: 2012

Título original: *9 Steps to Cybersecurity*

Traducción del inglés de Germán Trentini

Exención de responsabilidad

El presente libro fue diseñado únicamente para brindar información sobre ciberseguridad. Esta información se suministra y se vende a sabiendas de que el editor y autor no ofrece ningún tipo de asesoramiento legal ni profesional. En caso de necesitar asesoramiento de este tipo, por favor consulte con el profesional que corresponda. Este libro no contiene toda la información disponible sobre el tema. Este libro no ha sido concebido para ninguna situación o necesidad específica de una persona u organización. Se ha hecho todo lo posible por que este libro sea lo más preciso posible. Sin embargo, pueden existir errores tipográficos y/o de contenidos. Por lo tanto, este libro debe ser considerado solamente como una guía general y no como la principal fuente de información sobre el tema. Este libro contiene información que puede tener fechas y solamente pretende educar y entretener. El autor y editor no tendrá ninguna obligación ni responsabilidad hacia ninguna persona o entidad por ningún tipo de pérdida o daño sufrido, o que supuestamente haya sufrido, en forma directa o indirecta, por la información contenida en este libro. A través del presente, el lector acepta las condiciones de esta exención de responsabilidad o puede devolver el libro dentro del período de la garantía contra el reembolso por el total abonado.

Prólogo

Los negocios se han vuelto más vulnerables que nunca debido a diversos motivos que pueden dañar sus datos, sistemas y, sobre todo, sus actividades. Como nos muestra Dejan Kosutic, los riesgos son numerosos y muy reales, y es mucho lo que está en juego. Dejan expone los mitos populares sobre ciberseguridad. Luego, en forma elocuente y simple, explica los aspectos básicos de la ciberseguridad y detalla sus beneficios a través de hechos convincentes que a usted le ayudarán para involucrar a la alta gerencia con la implementación.

Usted descubrirá opciones de marcos referenciales para ciberseguridad y los conocimientos para escoger cuál es el adecuado para su negocio y situación particular. Dejan Kosutic explica la gestión del riesgo y qué capacitación o concienciación necesitarán tanto su gerencia como sus empleados.

Cuando concluya esta amena lectura, usted tendrá claro el concepto de ciberseguridad, como también los beneficios y en qué dirección orientar la planificación para implementar el sistema que protegerá sus negocios. También comprenderá cómo utilizar la ciberseguridad para hacer que su negocio sea más exitoso.

Tabla de contenidos

Introducción

¿Qué es la ciberseguridad? ¿Cómo se relaciona la ciberseguridad con la seguridad de la información? ¿Cómo protejo a mi empresa de los *hackers*? ¿Y ante un incendio o desastre natural?

Si usted fuera un funcionario de una organización diez años atrás, probablemente no se preocuparía demasiado con estas preguntas. Hoy, usted se encuentra en la segunda década del tercer milenio y ya no puede ignorar ese tipo de amenazases más, en el futuro necesitará aún más protección. ¿Por qué? Porque la mayoría de las organizaciones ahora participan en el negocio del procesamiento de información.

La mayoría de nosotros imagina que un banco maneja diariamente grandes sumas de efectivo. Si bien los bancos todavía realizan muchas transacciones en efectivo, la realidad es que las transacciones en dinero electrónico superan ampliamente a las transacciones en efectivo; en algunos casos por más de un millón a uno. Por lo tanto, esto implica que un banco tradicional participa en el negocio de procesamiento de información; es una gran fuente de información. Y adivine una cosa… desde hace ya algún

tiempo, robar un banco a través de la piratería informática es mucho más rentable que entrar con una máscara sobre la cara y asaltar a los cajeros. Y, además, la piratería es mucho menos riesgosa.

Piense en su negocio, ¿también es una fuente de información? Es muy probable que lo sea, si no completamente, al menos en la mayor parte del procesamiento de información. Esto significa que su negocio es más vulnerable. Su información, sus conocimientos teóricos y técnicos y su propiedad intelectual están en riesgo. Y, ahora, la pregunta del millón o, si usted forma parte de un negocio más grande, podría ser la pregunta de los mil millones: ¿Qué necesita hacer para proteger la información de su empresa y por dónde empieza?

Actualmente, el problema es que existe mucha información sobre ciberseguridad; probablemente usted se sienta bombardeado con información sobre nuevos cortafuegos, programas antivirus, metodologías, legislación, etc. Muchas empresas ofrecen servicios promocionados como la solución a todos sus problemas de ciberseguridad. Sin embargo, estas soluciones aisladas no van a proteger completamente su negocio. Por ejemplo, usted no puede solucionar el problema de un empleado disconforme con un cortafuegos; de la misma

forma, no puede resolver el problema de un pirata informático por el hecho de cumplir con las leyes.

Por eso es obvio que necesita algo más, algo integral. Pero el desafío es incluso por dónde comenzar, qué pasos tomar para proteger de la mejor manera a su empresa.

Este libro le definirá los aspectos básicos de la ciberseguridad, le explicará por qué es estratégicamente importante para su organización proteger su información, le contará cómo establecer la estructura de la ciberseguridad en una organización, qué preparativos son necesarios y, por último, cómo planificar su ciberseguridad y cómo obtener resultados cuantificables.

El siguiente texto evitará la jerga técnica y los detalles de la implementación de la ciberseguridad porque no es lo que usted necesita saber para tomar decisiones. El objetivo de este libro es proporcionarle la asistencia necesaria para usted que pueda comprender los componentes básicos de la ciberseguridad; de esta forma, podrá controlar mejor a sus especialistas en ciberseguridad cuando comiencen con la implementación.

Capítulo 1: La ciberseguridad es necesaria

Los cuatro tipos de incidentes de seguridad

1. Desastres naturales
2. Ataques maliciosos (fuente externa)
3. Ataque interno
4. Fallas y errores humanos involuntarios

Desastres naturales

En los últimos años, el mundo ha experimentado varios desastres naturales que acapararon la atención mundial. Huracanes como el Katrina y el Sandy, el desastre de Fukushima, tsunamis y terremotos como el de Haití, han sido devastadores y destruyeron negocios y bancos de datos completos. Además, otros desastres como tornados, inundaciones y tormentas, pueden ser suficientes para eliminar una empresa casi en cualquier lugar. Incluso un incendio localizado puede destruir todos sus datos si usted no

realizó la relocalización de sus copias de seguridad en una ubicación remota.

Ataques maliciosos

Los ataques cibernéticos y las violaciones de seguridad se suceden a cada minuto y son demasiado generalizadas como para localizarlas. Algunas son pequeñas, otras más grandes; algunas logran su cometido y otras no.

Estos son algunos de los principales incidentes de la historia reciente[1].

En mayo de 2006 los nombres, números de la Seguridad Social, fechas de nacimiento y algunas clasificaciones de incapacidad de 26,5 millones de veteranos y personal militar activo y sus cónyuges, fueron tomados del Departamento de Asuntos de Veteranos (VA) de los Estados Unidos.

La información estaba en un ordenador portátil y en un disco de almacenamiento externo obtenidos en un robo. Aunque esos elementos

[1]http://www.csoonline.com/article/700263/the-15-worst-data-security-breaches-of-the-21st-century

luego fueron recuperados, el Departamento de VA estimó que las pérdidas y costos por prevención podrían llegar a 500 millones de dólares.

Fecha: 6 de agosto de 2006. Ataque a AOL; los datos de más de 650.000 usuarios, incluida información bancaria y de compras, fueron revelados públicamente en un sitio web.

En marzo de 2008, fue atacada una base de datos de Heartland Payment Systems, que produjo la exposición de 134 millones de tarjetas de débito y crédito. Más tarde, Albert Gonzalez fue condenado por el delito y sentenciado a 20 años en una prisión federal.

En 2009 el gobierno Chino lanzó un ataque masivo sin precedentes contra Google, Yahoo y docenas de otras compañías de Silicon Valley. Google confesó que algunos datos de su propiedad intelectual fueron sustraídos.

En 2011, RSA Security reportó que unos 40 millones de registros de empleados fueron robados. Este incidente se relaciona con ataques posteriores sobre Lockheed-Martin, L3 y otros. Esta violación de seguridad ha sido considerada como completamente masiva desde una perspectiva de daño táctico potencial, como también desde una perspectiva psicológica.

En 2011, ESTsoft perdió información personal de 35 millones de surcoreanos debido a piratas informáticos

"En algún momento, casi todas las personas serán víctimas de la piratería", declara Jon Callas, CTO de Entrust, en un artículo de Help Net Security.

Ataques internos

En julio de 2007 un empleado de Fidelity National Information Services robó 3,2 millones de registros de clientes, incluidos los datos bancarios y de tarjetas de crédito e información personal. Un administrador de bases de datos llamado William Sullivan luego fue sentenciado a cuatro años y nueve meses de prisión y a pagar una multa de $3,2 millones.

El famoso sitio Wikileaks fue generado a partir de acceso a información interna. El juicio sobre el daño y los efectos de este caso monumental aún permanece abierto.

Fallas y errores humanos involuntarios

Las fallas de equipamiento e infraestructura es algo con lo que nos encontramos a diario: cortes de energía, caídas de vínculos de Internet y de líneas telefónicas, fallas en los dispositivos de almacenamiento y muchas otras.

¿Y cuando un colega suyo sobrescribe sus datos por error? ¿Y cuando se derrama una taza de café sobre su ordenador portátil?

Todas estas situaciones tienen dos cosas en común: primero, la consecuencia es que usted perderá sus datos, o no podrá acceder a ellos; y segundo, este tipo de incidentes suceden bastante a menudo.

Espero no haberlos asustado demasiado con estos ejemplos. Pero uno de los pasos iniciales para crear su ciberseguridad es ser conscientes del entorno en el que vivimos.

En este sentido, creo que la ciberseguridad no difiere mucho en cómo se gestionan otras áreas de su empresa.

Capítulo 2: Los mitos sobre ciberseguridad

Antes de que avancemos con la ciberseguridad, permítame explicarle qué no es la ciberseguridad. Hay varios mitos muy arraigados que podrían obstaculizar su consideración sobre este tema.

Mito n.° 1: Es lo mismo que tecnología de la información (TI)

Imagine el siguiente escenario: un administrador de sistemas disconforme desactiva intencionalmente su aplicación central y borra sus bases de datos más importantes.

¿Es esto un tema de TI? No, difícilmente sea una cuestión de TI; en realidad, es más un asunto de RR.HH. ¿Esto podría haber sido evitado por medidas de seguridad de TI? No. La persona en esta posición necesita tener acceso directo a todos sus sistemas.

Por eso, la forma de prevenir este tipo de escenarios queda afuera del área tecnológica y tiene que ver con cómo seleccionar a sus empleados, cómo supervisarlos, qué clase de documentos legales se les ha hecho firmar, cómo

se trata a esta persona en la empresa, y muchas otras cuestiones.

No me malinterprete, la tecnología de la información y sus medidas de seguridad son extremadamente importantes en ciberseguridad, pero ellas solas no son suficientes. Estas medidas deben estar combinadas con otros tipos de protección para que sean efectivas. Y esto es algo que explicaré más adelante.

Mito n.° 2: La alta gerencia no tiene nada que ver con la ciberseguridad

Seguramente usted es consciente de que las medidas de seguridad no pueden ser implementadas sin dinero ni tiempo de trabajo de los empleados. Pero si los ejecutivos de su empresa no están convencidos de que esta protección justifica la inversión, no le proporcionarán los recursos necesarios. Por lo tanto, el proyecto fracasará.

Además, si los altos ejecutivos no cumplen las normas de seguridad y, por ejemplo, dejan un ordenador portátil (con una lista de sus mejores clientes junto con datos de ventas y correspondencia que pueda estar relacionada) sin protección en el aeropuerto, todos los demás esfuerzos de seguridad serán en vano.

Por lo tanto, sus gerentes de alto rango son una parte importante de la ciberseguridad.

Mito n.° 3: La mayor inversión será en tecnología

Falso. La mayoría de las empresas con las que he trabajado ya contaban con casi toda la tecnología necesaria. Lo que *no* tenían eran reglas sobre cómo usar esa tecnología en forma segura. Esto es como comprar un lujoso automóvil BMW nuevo y usarlo solamente para repartir pizzas.

La información estará protegida si todas las personas que tienen acceso saben qué está permitido y qué no y quién es responsable por cada pieza de información o de equipamiento. Esto se logra definiendo reglas claras; generalmente bajo la forma de políticas y procedimientos.

Como norma general, yo diría que la inversión en tecnología generalmente es menos de la mitad de la inversión necesaria. En algunos casos, hasta puede ser menor al 10%. El grueso de la inversión habitualmente se destina al desarrollo de políticas y procedimientos, capacitación y concienciación, etc.

Mito n.° 4: En seguridad no existe el rendimiento de la inversión (ROI)

Sí, la seguridad cuesta dinero y, en general, esta protección no le reportará ingresos adicionales.

Toda la idea de ciberseguridad es disminuir los costos relacionados con problemas de seguridad; es decir, incidentes. Si usted logra disminuir la cantidad y/o la duración de los incidentes de seguridad, ahorrará dinero. En muchos casos, los ahorros conseguidos son mucho mayores que el costo de las medidas de seguridad implementadas; es por eso que usted "ganará dinero" con la ciberseguridad.

Un poco más adelante vamos a ampliar sobre el Retorno sobre la inversión en seguridad.

Mito n.° 5: La ciberseguridad es un proyecto de una única vez

Falso. La ciberseguridad es un proceso permanente. Por ejemplo, si usted desarrolla un procedimiento de respuesta a los incidentes que requiere que sus empleados notifiquen al Jefe de seguridad de la información en su teléfono celular cada vez que se produce un incidente, pero luego esta persona deja de trabajar en su empresa, es obvio que usted no querrá que estas

llamadas sigan siendo dirigidas a ese teléfono si desea que el sistema sea funcional. Debe actualizar sus procedimientos y políticas, pero también el software, el equipamiento, los acuerdos, etc. Y este es el trabajo que nunca acaba.

Mito n.° 6: El mito de la documentación

El hecho de redactar una pila de políticas y procedimientos no significa que sus empleados automáticamente comenzarán a cumplirlos.

La seguridad, generalmente, implica un gran cambio y, para ser francos, a nadie le gusta modificar las prácticas ya establecidas. Por ejemplo, en lugar de su vieja y querida contraseña “1234”, de repente, usted se encuentra con que tiene que cambiarla cada 90 días y que tiene que ser de ocho caracteres, de los cuales al menos uno debe ser un número y uno un carácter especial.

¿Qué significa esto? Que sus empleados se resistirán al cambio y que tratarán de encontrar formas para eludir estas nuevas normas. Yo le diré más adelante qué puede hacer para ayudarlos a superar esta resistencia.

Ahora que ya sabe qué está mal, veamos lo bueno.

Capítulo 3: Aspectos básicos de la ciberseguridad

Entonces, ¿qué es exactamente la ciberseguridad y cómo encaja con todos los otros términos tecnológicos de moda que escuchamos habitualmente?

Primero avancemos sobre algunas definiciones básicas:

Se define a la **seguridad de la información** (también conocida como ***infosec***, por la forma abreviada de su nombre en inglés) como la "preservación de la confidencialidad, integridad y disponibilidad de la información" (ISO/IEC 27001:2005), donde **confidencialidad** es "la propiedad de que la información no sea puesta a disposición de, o se divulgue a, individuos, entidades o procesos no autorizados", **integridad** es "la propiedad de mantener la exactitud y completitud de los activos" y **disponibilidad** es "la propiedad de ser accesibles y utilizables ante la demanda de una entidad autorizada".

En este punto debemos hacer una pequeña advertencia: cuando escuche a sus empleados del área de seguridad hablar sobre CIA, probablemente no se refieran al organismo de

seguridad internacionalmente conocido, sino a los tres conceptos mencionados anteriormente por sus nombres en inglés (*confidentiality, integrity, availability*).

En otras palabras, la seguridad de la información sería lo siguiente: si voy al banco y deposito $10.000, en primer lugar, quiero que nadie más sepa sobre este dinero, solamente el banco y yo. (Esto es **confidencialidad**)

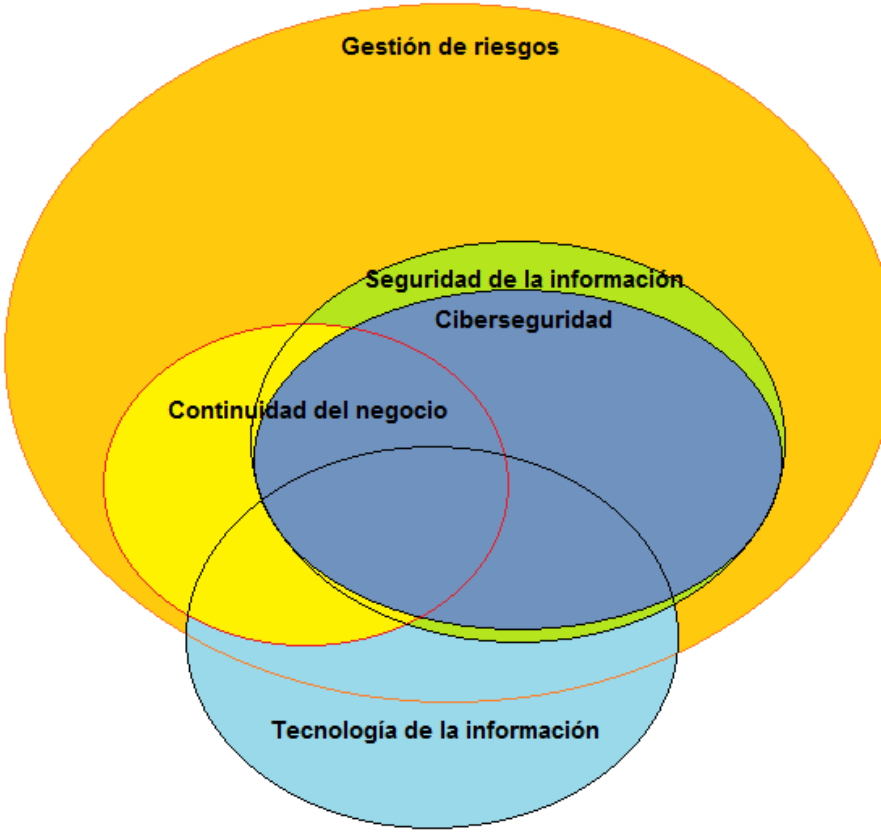
Luego de unos meses, cuando vaya a retirar mi depósito, quiero que el importe sean los $10.000 más los intereses que correspondan; no quiero que me entreguen $1.000 porque alguien estuvo jugando con mi cuenta. (Esto es **integridad**)

Por último, cuando vaya a retirar mi dinero, no quiero que el cajero me diga que el sistema del banco está caído y que tengo que regresar al día siguiente. (Esto es **disponibilidad**)

La definición de ciberseguridad no es muy distinta a la de seguridad de la información: “La ciberseguridad debe estar libre de peligros y daños ocasionados por interrupciones, caídas de los servicios o abusos de las TIC. El peligro o daño debido al abuso, interrupción o caída de los servicios puede estar constituido por una limitación de la disponibilidad y confiabilidad de

las TIC, una violación a la confidencialidad de la información almacenada en las TIC o un daño a la integridad de esa información"(Estrategia nacional de ciberseguridad 2011, Ministerio Holandés de Seguridad y Justicia).

Como probablemente ya hayan notado, esos dos términos son bastante similares. Veamos en la siguiente imagen cómo se relacionan:



Seguridad de la información vs. Ciberseguridad

A pesar de que no hay una posición oficial sobre las diferencias entre seguridad de la información y ciberseguridad, a mí me gusta interpretarlas de la siguiente manera: ciberseguridad es 95% seguridad de la información; la única diferencia es que esta última incluye la seguridad en medios no digitales (por ejemplo, papel), mientras que la ciberseguridad se enfoca solamente en la información en formato digital. En la actualidad, los medios no digitales representan una pequeña porción del total de información disponible; generalmente, mucho menos del 5% de toda la información.

En muchos casos, *seguridad de la información* y *ciberseguridad* se usan indistintamente, como sinónimos. Parecería ser que *ciberseguridad* es el término preferido en círculos gubernamentales en los Estados Unidos, mientras que *seguridad de la información* generalmente es más utilizada en bancos y organizaciones de salud.

Lo importante aquí es que el uso de “seguridad de la información” y “ciberseguridad” habitualmente son intercambiables. Usted puede utilizar ambos términos que no se equivocará. Notará que yo los utilizo indistintamente.

Continuidad del negocio y Gestión del riesgo

Continuidad del negocio es la "capacidad estratégica y táctica de la organización para planificar y ejecutar la respuesta ante incidentes e interrupciones en el negocio con el fin de permitir la continuidad de las actividades comerciales en un nivel aceptable previamente definido" (BS 25999-2:2007).Menciono esto como un concepto distinto porque es aquí donde, habitualmente, se necesita la mayor parte de la inversión en tecnología, y la continuidad del negocio también es indispensable en casos de desastres naturales.

Como tal vez ya ha observado en la imagen anterior, la ciberseguridad se superpone en gran medida con la continuidad del negocio; esto se debe a que una de las características más importantes de la ciberseguridad es mantener la disponibilidad de la información, aquí es donde la continuidad del negocio juega un papel importante.

El objetivo de todas (ciberseguridad, seguridad de la información y continuidad del negocio) es básicamente disminuir los riesgos de hacer negocios o gestionar el riesgo. En el mundo bancario, esto se denomina gestión del riesgo operativo. A pesar de que usted puede no utilizar este término o tener una unidad en la

organización para gestionar riesgos, cuando trabaja para proteger su información para que no sea robada o comprometida, esencialmente está disminuyendo sus riesgos comerciales.

Es posible que sea una sorpresa enterarse de que la tecnología de la información es una parte tan pequeña de la ciberseguridad. Como mencionamos anteriormente, la tecnología no es la solución para todos los riesgos porque las medidas de seguridad de TI normalmente representan el 50% de la ciberseguridad.

Lo que usted hace para disminuir riesgos es, obviamente, el principal esfuerzo de su ciberseguridad. Desde un punto de vista terminológico, es importante saber que las **medidas correctivas** y las **medidas y controles de seguridad**, o simplemente, los **controles**, significan lo mismo: "formas de gestionar el riesgo, incluidas las políticas, procedimientos, directrices, prácticas o estructuras organizacionales, que pueden ser administrativas, técnicas, gerenciales o legales por naturaleza" (ISO/IEC 27000:2009).

Básicamente, los controles son lo que usted hace para proteger la información de su empresa.

Ahora que ya conoce algunos aspectos básicos de la ciberseguridad, avancemos con los 9 pasos de la implementación.

Capítulo 4: 9 pasos básicos para establecer la ciberseguridad en su empresa

¿Cuáles son los pasos necesarios para lograr este famoso triángulo CIA; es decir, la protección de la confidencialidad, integridad y disponibilidad de la información en la empresa?

Como ya mencionamos en la introducción, no vamos a centrarnos en los detalles de cada paso, sino que le voy a ofrecer un resumen de qué pasos son necesarios, y el objetivo de cada uno, para que usted pueda iniciar el proyecto en su empresa. Además, también podrá comprender qué necesita para tener éxito. Todo esto en términos fáciles de entender, sin detalles técnicos, para que usted pueda hacer la planificación y luego delegar la implementación en los especialistas.

Paso 1: Investigar sobre la legislación y demás requisitos

Esta puede parecer una forma extraña de comenzar su plan para la implementación de la ciberseguridad, pero también es la más efectiva. Si usted es o representa a una institución financiera, un organismo oficial o una organización de salud, lo más probable es que existan leyes o normas en su país que lo obliguen a implementar medidas de protección de seguridad de la información. Para obtener una lista de leyes y normas relacionadas con seguridad de la información en Argentina, Chile, México, Perú y España, por favor consulte el Apéndice.

En algunos casos, incluso los proveedores y socios comerciales de instituciones financieras y oficinas gubernamentales están regulados; por ejemplo, en algunos países, los proveedores de servicios de tecnología de la información de los bancos se encuentran bajo supervisión del organismo oficial que supervisa a los bancos. Lo importante aquí es que el regulador ha comprendido que el sistema de TI de un banco es tan seguro como la empresa que desarrolla sus aplicaciones o provee los servicios de mantenimiento a los sistemas del banco; si

alguien se infiltra en los servidores de esa empresa de TI, es muy probable que también tenga acceso a los sistemas informáticos del banco.

En la mayoría de los casos, será necesario que su empresa deba cumplir al menos con las leyes de protección de datos personales. Aún si usted no maneja ningún tipo de datos personales de sus clientes, es muy probable que sí tenga registros con datos personales de sus empleados.

De cualquier forma, seguramente se sorprenderá de la cantidad de leyes y normativas que existen. Comience por hacer una lista, y asegúrese de conocer los plazos exactos ya que el no cumplimiento de esas leyes y normas generalmente viene acompañado de elevadas multas.

También es necesario que revise sus obligaciones contractuales. Por ejemplo, si usted es una empresa de TI que provee servicios críticos a un organismo gubernamental, es muy probable que haya firmado con ellos un contrato que exige reglas estrictas de confidencialidad, definiciones del nivel de servicio, cláusulas de derechos de propiedad intelectual, reglas para control de acceso y muchas otras cuestiones a tener en cuenta. Otros contratos con clientes y proveedores también tienen requisitos que se

deben cumplir de una forma establecida, y usted no querrá arriesgarse a perder sus clientes o a ser pasible de recibir multas.

Paso 2: Definir los beneficios y obtener el apoyo de la alta gerencia

De acuerdo a mi experiencia, este es el principal motivo por el cual fracasan las iniciativas y/o proyectos de ciberseguridad.

¿Por qué es tan importante este paso?

La respuesta es bastante simple pero, sin embargo, el apoyo de la alta gerencia demasiadas veces es subestimado. No existe proyecto o iniciativa (de ciberseguridad o de lo que sea) que pueda tener éxito sin el dinero ni la mano de obra necesarios para la implementación. Y las únicas personas que pueden proporcionar esos recursos pertenecen a la alta gerencia; aún si usted es el presidente de una empresa necesitará el compromiso, o al menos el acuerdo, de otros miembros de su equipo de dirección. Si ellos no apoyan el proyecto, pueden demorarlo, o incluso frenarlo, aunque usted lo respalde al 100%.

Ahora, la pregunta es ¿cómo obtiene el apoyo y compromiso de la alta gerencia? Como con todo lo demás en el ámbito de los negocios (y de la vida privada), usted debe encontrar algunos puntos de interés en común; es decir, algunos beneficios que traerá el proyecto no sólo para la

empresa sino también para las personas que trabajan allí.

Por eso, avancemos sobre los cuatro potenciales beneficios que podría obtener su empresa con el proyecto de ciberseguridad. No todos estos beneficios potenciales podrían aplicarse a su situación; lo importante es que usted encuentra al menos uno que marque la diferencia para su empresa.

Cumplimiento

Si en el Paso 1 usted detectó algún tipo de ley, norma o requisito contractual relacionado con la seguridad de la información, puede respaldar su proyecto de ciberseguridad por la importancia en el cumplimiento de todos los requisitos detectados. Entonces, el principal beneficio con este proyecto sería que tendrán la tranquilidad y la certeza de no estar omitiendo ninguna parte del rompecabezas, para que no tengan que pagar ningún tipo de multas. Además, si escoge con buen criterio un marco referencial para la implementación de la ciberseguridad (vea el Paso 4), implementar todos los controles de seguridad le demandará mucho menos tiempo que si no tuviera ese enfoque sistemático.

Ventaja de comercialización

A menos que usted venda alguna clase de herramienta para seguridad de la información o servicios de consultoría, a primera vista parecería que la ciberseguridad y la comercialización no tienen mucho en común. Sin embargo, es necesario que usted les muestre a las otras partes involucradas (por ejemplo, los clientes) que puede administrar en forma segura la información que ellos le confían. Esto se puede hacer a través del proceso de certificación; los certificados más difundidos para las organizaciones son ISO 27001 y PCI DSS (en el Paso 4 explicaré qué son). En algunas situaciones no es necesario un certificado; por ejemplo, si tiene clientes muy grandes, simplemente puede pedirles que envíen un equipo de auditoría para que verifique si su nivel de seguridad es satisfactorio.

Esto puede ser una herramienta de venta para ayudar a su empresa a ganar nuevos clientes porque usted puede demostrarles a sus potenciales clientes que protegerá mejor que la competencia la información que ellos le deleguen. Esto, además, implica que sus posibilidades de retener clientes actuales serán mayores ya que puede probarles que usted es una opción más segura que otras empresas que

intentan conseguir su negocio. Y la inversión en ciberseguridad generalmente es mucho menor que la ganancia potencial que se puede obtener de esos clientes.

Disminuir los costos

La filosofía fundamental de la ciberseguridad es la prevención; usted invierte ahora para ahorrar dinero más adelante. También puede tomarla como su póliza de seguro; paga ahora para evitar posteriormente las consecuencias de algún incidente que ocasione daños.

El argumento principal es cómo garantizar que la inversión en controles de seguridad no superarán los costos de los potenciales incidentes que se evitan. En otras palabras, la pregunta es cómo asegurarse que va a tener un rendimiento sobre la inversión en ciberseguridad. Aquí es donde se utiliza el concepto de gestión de riesgos. Aunque en el Paso 6 ampliaré sobre gestión de riesgos, estos son algunos aspectos básicos: imaginemos que usted desea calcular el ROI para mitigar el riesgo de incendio en su centro de datos; por ejemplo, si su centro de datos se destruye en un incendio, el costo para volver a dejarlo operativo se estima en $2 millones, incluyendo todos los costos y

daños relacionados, y teniendo en cuenta que la posibilidad de que ocurra un incidente de este tipo se considera de una en 100 años, su riesgo anualizado es de $20.000 ($2 millones por 1%). Esto significa que mientras su inversión en sistemas de protección contra incendios sea menor a $20.000 por año, debería obtener una ganancia.

Ahora bien, usted puede estar pensando que predecir la probabilidad y el costo total del daño es imposible, y tiene razón. A menos que tenga datos estadísticos precisos, puede ser difícil calcular este tipo de riesgos, pero el punto es que usted puede demostrar por qué una inversión en ciberseguridad es rentable cuando se hace sensatamente y con una buena medida (Puede utilizar este Calculador del Retorno sobre Inversión en Seguridad como ayuda para estimar riesgos, daños y costos de mitigación).

Optimización de los procesos comerciales

Encontrar una organización en la que todo funcione a la perfección es muy raro, incluso si así fuera, la situación generalmente es temporaria. De hecho, es muy probable que las empresas que no determinaron claramente su organización interna tengan mayores riesgos

relacionados con la ciberseguridad. Por ejemplo, en las empresas de TI que crecen rápidamente el principal problema es que no encontraron tiempo para sentarse y pensar cómo optimizar sus procesos internos. Como consecuencia, no está muy bien determinado quién necesita hacer qué, quién está autorizado a tomar determinadas decisiones, quién es responsable de qué, y muchas otras definiciones. Comúnmente, el efecto que tiene este tipo de situaciones es que los empleados pierden tiempo tapando lagunas en la organización y pierden tiempo para concentrarse en su propio trabajo.

Como mencionamos anteriormente, la ciberseguridad muchas veces no es más que la definición clara de los procedimientos laborales; por ello, como ventaja adicional en la implementación de la ciberseguridad obtendrá una empresa mucho más organizada. La seguridad es principalmente el producto de procesos bien definidos, y debido a que la seguridad está presente en todas las áreas de su organización, este ordenamiento de su negocio abarcará un aspecto mucho más amplio que únicamente los procesos de seguridad.

¿Cómo determinar los beneficios?

La mejor opción sería incluir uno o más de estos beneficios en la estrategia de su empresa; si pudiera encontrar una relación entre los beneficios de la ciberseguridad y sus objetivos estratégicos, daría en el blanco. Esto puede parecer demasiado a primera vista, pero evaluándolo detenidamente, no es una tarea imposible. Muchas veces, una sesión de tormenta de ideas puede generar este tipo de relaciones.

Por el lado personal, es vital definir beneficios que se ajusten a determinados jugadores clave de una empresa. Por ejemplo, su gerente comercial puede, en principio, oponerse a la idea de la seguridad de la información por una posible disminución de las ventas. Sin embargo, si le explica que un mayor nivel de seguridad de la información implicará que la competencia no podrá acceder a información confidencial (por ejemplo, detalles de sus propuestas) mientras esté negociando con un nuevo cliente, probablemente obtenga su compromiso activo.

Pero permítame también mencionar aquí que no podrá usted solo encontrar beneficios para todos. En esta tarea probablemente tenga que incluir a otros miembros de su alta gerencia, como también a empleados de diversas partes de

su organización y de distintos niveles jerárquicos. Este es un proceso continuo, no una decisión que se hace en algún momento.

Esto es más evidente cuando tiene que ver con la actividad “diplomática” dentro de su empresa; usted no puede simplemente pretender que todos los miembros de la gerencia compartan su entusiasmo simplemente a partir de una presentación de 30 minutos con ellos. Descubrir los beneficios y persuadir a todos puede ser un gran trabajo.

Paso 3: Establecer los objetivos para la ciberseguridad

"Lo que se mide se puede mejorar", una clásica cita de Peter Drucker.

Por lo visto hasta ahora, probablemente se haya dado cuenta de que tiene que tratar la ciberseguridad como un caso de negocios: usted desea invertir determinados recursos y obtener resultados positivos para su empresa. Si logra lo que pretende, sabrá que su inversión en ciberseguridad tenía sentido; por otro lado, lo contrario también es cierto, si no alcanzó los objetivos planteados, algo no está bien con su ciberseguridad.

Y aquí es donde las cosas se pueden complicar un poco. ¿Cómo sabrá si logró una "ventaja comercial" o el "cumplimiento"? La respuesta a esta pregunta es que usted debe establecer objetivos claros y cuantificables. Por ejemplo, un objetivo que diga "queremos tener seguridad" no le proporciona nada de dónde sostenerse; en cambio, piense en objetivos en la línea de "retener a todos los clientes actuales" o "vincular un 2% de nuevos clientes que se interesan por la ciberseguridad durante los próximos 12 meses" o, por ejemplo, "dar pleno cumplimiento a todas

las leyes y normativas dentro de los próximos cuatro meses" o, mejor aún, "disminuir los costos de incidentes de seguridad en un 50% durante los próximos dos años".

Si determina este tipo de objetivos para su ciberseguridad, podrá evaluar si todos los pasos planificados en la implementación tienen sentido. No solamente esto, luego de uno o dos años podrá mirar hacia atrás y sacar conclusiones precisas sobre si todo este esfuerzo valió la pena; simplemente compare dónde está hoy en relación con lo que escribió en sus objetivos.

Redactar objetivos claros también es importante para los demás integrantes de la organización. Todos los demás miembros de su cuerpo directivo sabrán exactamente por qué usted impulsa este proyecto; los niveles gerenciales intermedios y todos los empleados también tendrán un panorama mucho más claro de por qué es importante este esfuerzo. Y si ellos comprenden por qué esto es importante y útil, usted tiene muchas más posibilidades de que el proyecto tenga éxito. Si ellos no aceptan su visión sobre ciberseguridad, lo más probable es que traten de evitar todo lo que esté relacionado con ella.

Cuando intente pensar en los objetivos para la ciberseguridad, siempre comience por los beneficios que ya ha definido en los pasos previos; cuando tenga en claro estos beneficios, la definición de los objetivos será mucho más sencilla. Si ya tiene algún tipo de sistema para establecer objetivos y medir si se cumplieron; por ejemplo, un sistema de resultados compensados, definitivamente debe incorporar los objetivos de ciberseguridad en este sistema. Cuantas más actividades de ciberseguridad incluya en sus actividades diarias, mejor.

Paso 4: Escoger el marco referencial para la implementación de la ciberseguridad

Una vez que tenga claro qué desea conseguir, el siguiente paso es definir cómo lo va a ejecutarla ciberseguridad es algo que, ciertamente, no podrá terminar en una o dos semanas. El proyecto involucrará a muchas personas de su empresa, a sus proveedores, socios comerciales y clientes, como también implicará cambios en los procedimientos y responsabilidades laborales vigentes, en tecnología, en prácticas de recursos humanos, etc. Es mucho trabajo.

Y es por esto que lo mejor es utilizar experiencias de otras organizaciones que ya han implementado con éxito la ciberseguridad; esos marcos referenciales son de acceso público y aquí detallamos una lista de los más reconocidos:

ISO 27001

ISO/IEC 27001 es una norma internacional publicada por ISO (*International Organization for Standardization*) que define cómo implementar y administrar el Sistema de gestión de seguridad

de la información. Esta norma proporciona una buena base para construir la ciberseguridad porque ofrece un catálogo de 133 controles de seguridad y la flexibilidad de aplicar solo aquellos que son realmente necesarios (según la evaluación de riesgos).Pero lo mejor que tiene es que define un marco referencial de gestión para controlar y abordar los asuntos de seguridad logrando, de esta forma, que la gestión de la seguridad sea parte de la gestión general de una organización. Es una de las principales normas en seguridad de la información y, al momento de escribir este libro, había aproximadamente 20.000 empresas certificadas por esta norma en todo el mundo (la certificación es realizada por organismos de certificación acreditados).Para consultar cómo dar cumplimiento a esta norma, descargue este diagrama de implementación gratuito.

COBIT

COBIT es un marco referencial publicado por ISACA (*Information Systems Audit and Control Association*) que se centra en la gestión de TI corporativa. Es diferente porque refleja el rol central que tiene la tecnología de la información en las organizaciones modernas. Como sucede con otros marcos referenciales, también se basa

en el concepto de gestión de riesgos y en mantener dentro de un nivel aceptable los riesgos relacionados con TI; pero, tal vez, su mejor característica es que proporciona una relación directa entre los objetivos estratégicos de una empresa y el uso de TI. Muchos auditores de seguridad de la información y TI prefieren este marco como base para ejecutar su trabajo de auditoría.

Serie NIST SP 800

NIST SP 800 es una serie de más de cien publicaciones sobre seguridad de TI realizada por el Instituto Nacional de Normas y Tecnología de los Estados Unidos. Es, probablemente, la biblioteca de acceso público más completa sobre buenas prácticas y, de la misma forma que la PCI DSS, está orientada, en mayor medida, a temas técnicos de seguridad. Como la SP 800 no es un documento único sino una serie de documentos no muy relacionados, no sería adecuado utilizarla como un marco referencial único para la implementación; sin embargo, las publicaciones de NIST SP 800 son indispensables para controles individuales o para determinadas áreas de la seguridad de la información.

PCI DSS

PCI DSS es una serie de normas emitida por el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC) que se centra en mejorar la seguridad de los datos de tarjetas de pago. Este marco está conformado por especificaciones, herramientas, medidas y demás recursos muy específicos y detallados para la seguridad de datos y la protección técnica de los sistemas de pago. El cumplimiento de estas normas es prácticamente obligatorio para cualquier empresa que trabaja con pagos de tarjetas de crédito y otros tipos de transacciones en línea, algunos estados de Estados Unidos directamente estimulan la implementación de esas normas. En cuanto a la certificación, solamente determinados tipos de organizaciones que participan de las transacciones de pago con tarjetas deben ser evaluadas por consultores calificados.

ITIL© e ISO 20000

La ITIL, anteriormente conocida como Biblioteca de Infraestructura de TI, fue publicada por la Oficina Gubernamental de Comercio (OGC) del Reino Unido. Es un marco referencial para identificar, planificar, suministrar y dar soporte

a servicios de TI de la parte comercial de una organización y es, sin dudas, el enfoque de mayor aceptación a nivel mundial para la gestión de servicios de TI. Aunque sí cuenta con elementos de gestión de seguridad de la información y continuidad del servicio (es decir, continuidad del negocio), el principal interés de ITIL no está en estas áreas. La certificación ITIL para individuos está muy difundida; sin embargo, las empresas no se pueden certificar con este marco referencial. Las organizaciones se pueden certificar con la norma internacional ISO/IEC 20000-1, que se basa en la ITIL.

ISO 22301 y BS 25999-2

ISO 22301 es una norma internacional también publicada por ISO que se enfoca en el desarrollo del Sistema de Gestión de la Continuidad del Negocio y fue publicada muy recientemente; sin embargo, es una versión nueva y mejorada de la norma británica BS 25999-2, que ya se ha convertido en una de las principales normas a nivel mundial sobre continuidad del negocio. ISO 22301 es totalmente compatible con ISO 27001 y es posible implementarlas conjuntamente de forma muy sencilla, obteniendo así un muy buen marco referencial para la protección integrada de seguridad de la información y continuidad del

negocio. Como con otras normas ISO, las empresas también pueden obtener la certificación bajo esta norma de continuidad del negocio. Para consultar cómo dar cumplimiento a esta norma, descargue este diagrama de implementación gratuito.

NFPA 1600

NFPA 1600 es una norma publicada por la Asociación Nacional de Protección contra Incendios de los Estados Unidos y se centra en la gestión de desastres y emergencias y en continuidad del negocio. Es muy popular en los Estados Unidos y también está reconocida como la norma nacional de preparación por la Comisión Nacional sobre Ataques Terroristas en los Estados Unidos. En comparación con la ISO 22301 es más detallada en el área de gestión de crisis; no obstante, al ser una norma propia de los EE. UU., no es tan popular fuera de este país. Todavía hay que ver cuál de estas dos normas prevalecerá en los EE. UU.

ISO 27032

ISO/IEC 27032 contiene los lineamientos para la implementación de la ciberseguridad; es una

norma internacional realmente nueva publicada por ISO que abarca las prácticas sobre seguridad que son el punto de referencia para todos los involucrados en el ciberespacio. Todavía hay que ver cómo se pondrá en práctica esta norma y qué aceptación logrará, pero, en principio, parece que funcionará mucho mejor como una norma de apoyo para la implementación de ISO 27001 que como un marco referencial independiente. No es posible certificar una organización contra ISO 27032 porque ésta no es una norma que describa un sistema de gestión.

¿Cómo escoger el marco referencial adecuado?

Al evaluar todos estos marcos referenciales, usted debe tener presentes las siguientes preguntas:

- ¿Cuáles son los requisitos legales?
- ¿Cuáles son los requisitos contractuales?
- ¿Qué beneficios le gustaría obtener?
- ¿Cuáles son los objetivos que desearía lograr?

Por ejemplo, si usted ha firmado un contrato de nivel de servicio requerido con algunos de sus clientes que lo obliga a garantizar un

determinado nivel mínimo de disponibilidad de servicio, la norma ISO 22301 (o, tal vez, NFPA 1600 si se encuentra en los EE. UU.) probablemente sea la mejor opción. Esto se debe a que necesitará enfocarse en aspectos de continuidad del negocio, mientras que los aspectos de seguridad no serán el principal interés.

Por otro lado, si su objetivo es definir claramente procesos y procedimientos en su departamento de TI, entonces ITIL sería probablemente la mejor solución ya que ese es el principal enfoque de esta norma.

Sin embargo, si, por ejemplo, la legislación lo obliga a implementar medidas de seguridad organizacionales y técnicas que sean integrales, probablemente deba orientar su mirada hacia ISO 27001, la serie NIST SP 800 y COBIT. Personalmente, yo preferiría la ISO 27001 porque creo que es la más fácil de implementar. Pero, nuevamente, tal vez yo esté muy influenciado en este punto.

Cualquiera sea su elección, siempre será mejor que nada. Implementar la ciberseguridad sin conocimientos, muy probablemente termine en un fracaso.

Paso 5: Organizar la implementación

Independientemente del marco referencial que decida utilizar, el proceso de implementación de su ciberseguridad será, probablemente, un trabajo complejo. Por lo tanto, no puede simplemente asignárselo a su administrador de sistemas para que lo realice como parte de su trabajo habitual por varias razones: (1) es demasiado complejo para que una sola persona lo maneje sin un plan claro, (2) porque no se trata principalmente de una tarea de TI y (3) porque cualquier persona que esté muy abajo en la estructura organizacional y que no tenga experiencia en el manejo de personas, probablemente no esté debidamente capacitada para este trabajo.

Entonces, ¿cómo inicia la implementación desde un punto de vista organizacional?

Determinar la gestión del proyecto

Este tipo de implementaciones complejas nunca se podrán terminar sin una estructura del proyecto. Esto no significa que usted deba aplicar alguna sofisticada metodología para gestión de proyectos, pero sí, al menos, que tiene que determinar lo siguiente:(1) qué desea lograr

con este proyecto; (2) quién es el responsable del proyecto, por ejemplo, un gerente de proyectos que coordinará todos los esfuerzos y será responsable de los plazos y resultados del mismo; (3) quién será el promotor del proyecto, es decir, una persona de la alta gerencia que intervendrá cuando el proyecto se estanque (y créame que esto sucederá con mucha frecuencia); y (4) cuáles son los pasos, resultados, plazos y logros del proyecto. A menos que se trate de una organización pequeña, también puede (5) formar un equipo del proyecto que ayudará en la coordinación con diferentes unidades organizacionales. Lo mejor es que los miembros del equipo del proyecto sean seleccionados tanto desde el sector comercial como del de TI de la organización.

Obtener los conocimientos

El marco referencial o la norma que haya seleccionado en los pasos previos le proporcionará una excelente base sobre la cual construirá su ciberseguridad; sin embargo, esto no le otorgará todo el conocimiento y teórico y práctico necesario para su implementación.

Por lo tanto, deberá decidir cuál de estas opciones escogerá:

a) Implementar la ciberseguridad únicamente con sus empleados.
b) Implementar la ciberseguridad con sus empleados utilizando el asesoramiento de un especialista externo.
c) Implementar la ciberseguridad utilizando principalmente ayuda externa (es decir, consultores).

La opción a) al principio será la más económica, pero también demandará mayor cantidad de tiempo porque deberá capacitar a sus empleados o buscar contratar en el mercado alguien que posea los conocimientos necesarios. No obstante, durante la implementación usted podría darse cuenta de que equivocó algunos pasos que, al fin de cuentas, le costaron más que lo que habría pagado por asesoramiento externo. Tal vez esta opción sea la mejor si usted tiene cuestiones de alta confidencialidad, ya que no querrá dejar que nadie externo conozca por dentro a su empresa.

La opción b) ciertamente será más rápida que la opción a), pero no tanto como la c).Pero lo que a mí me gusta de esta alternativa es que logra un buen equilibrio entre no cometer demasiados errores y, al mismo tiempo, la posibilidad de obtener la mayor transferencia posible de conocimiento hacia sus propios empleados. Esto no se genera únicamente a través de las capacitaciones, que seguirán siendo necesarias,

sino también mediante el aprendizaje a partir del especialista que contrate y de su propia experiencia durante la implementación.

La opción c) es la más rápida y, probablemente, la mejor si usted tiene plazos muy cortos. De todos modos, debe ser consciente de que los consultores no son económicos (al menos los buenos, y contratar a los malos le costará aún más) pero, además, si un tercero redacta todos sus procedimientos y políticas, sin importar qué tan bueno sea este consultor, usted podría enfrentar dos problemas: primero, sus empleados pueden sentir que esas políticas y procedimientos no son algo que han producido ellos mismos y podrían resistirse a la implementación; segundo, la transferencia de conocimientos no será tan amplia como en la opción b), entonces podría encontrarse con que le faltan empleados capacitados para mantener su ciberseguridad una vez que el consultor se ha ido.

Determinar los recursos necesarios

El solo hecho de crear un plan no significa que su proyecto tendrá éxito. También necesita dinero y horas hombre para terminar el proyecto satisfactoriamente.

Normalmente, esto es lo que usted debe planificar en su presupuesto y en otras planificaciones comerciales:

1) **Tiempo y costo de sus empleados:** el tiempo que ellos deberán invertir en capacitación, desarrollo de documentación, coordinación del proyecto, adaptación a las nuevas reglas, etc. Además, tampoco podrán desarrollar sus tareas habituales. Es muy probable que este sea su mayor gasto.

2) **Costo de tecnología:** tal vez necesite invertir algo de dinero en nuevas tecnologías a medida que vaya detectando mayores riesgos. Sin embargo, como observamos anteriormente, es muy probable que usted ya cuente con la mayor parte de la tecnología. En general, la principal inversión necesaria es en "recuperación ante desastres". Esta recuperación es una solución técnica en la que sus datos y tecnología están

disponibles no sólo en su ubicación habitual (denominada “ubicación principal”), sino además en un lugar alternativo (denominado "ubicación secundaria") que se utiliza en caso que ocurra un desastre. En la actualidad, con el avance de la “computación en la nube” y demás alternativas, su ubicación secundaria no es necesario que sea demasiado costosa (a menos que tenga datos muy confidenciales que no quiera almacenar en la nube; por ejemplo, si se trata de un banco).

3) **Costo de asistencia externa:** Aquí se incluyen los consultores (si los contrata), capacitación, diversas herramientas que podría utilizar, plantillas de documentación, etc. Asegúrese de que cada uno de estos elementos disminuirá su costo total y/o duración de la implementación en lugar de incrementarlo.

4) **Costos de certificación:** Si decide ir por la certificación, también habrá un costo. De todos modos, estos costos serán los menores de todos los mencionados anteriormente. Por supuesto que primero

deberá decidir si encuentra algún beneficio en la certificación.

Podrá calcular sus costos de forma mucho más precisa una vez que termine su proceso de evaluación y tratamiento de riesgos.

Paso 6: Evaluación y mitigación de riesgos

Los detalles de su proyecto de implementación de ciberseguridad dependerán de sus objetivos y del marco referencial que escoja. Sin importar cuál de los enfoques adopte, tendrá que basarse en gestionar sus riesgos en seguridad de la información.

El objetivo de la gestión de riesgos

¿Por qué son importantes la evaluación y el tratamiento de riesgos? Permítame darle un ejemplo.

Digamos que habitualmente usted deja su ordenador personal en el asiento trasero de su automóvil. Es muy probable que, tarde o temprano, se lo roben. ¿Qué puede hacer para disminuir el riesgo de comprometer la confidencialidad, integridad y disponibilidad de la información almacenada en su ordenador personal?

Ante todo, puede crear una regla (redactando un procedimiento o una política) que establezca que los ordenadores personales no pueden ser dejados desatendidos en un vehículo; o que se debe estacionar el vehículo en un lugar que

tenga algún tipo de protección física. Segundo, puede proteger su información configurando una clave segura y encriptado sus datos. Además, puede exigirles a los empleados que firmen una declaración por medio de la cual se hacen legalmente responsables por el daño que pueda producirse. Pero ninguna de estas medidas tendrá efecto si no se las explica a sus empleados a través de una capacitación.

Ahora, ¿qué conclusiones puede sacar de este ejemplo? La seguridad de la información nunca es un único control de seguridad. Esto se logra con una combinación de medidas de protección que no deben estar relacionadas únicamente con TI, también deben contemplar cuestiones organizacionales, gestión de recursos humanos, seguridad física y protección legal.

El problema es que esto fue sólo un ejemplo de un único ordenador personal, sin amenazas internas. Ahora piense qué complejo es proteger la información en su empresa, donde la información se archiva no solamente en sus ordenadores sino también en diversos servidores, en los cajones de escritorios, en sus teléfonos móviles, en unidades de memoria USB y también en la cabeza de todos los empleados. ¿Y qué pasaría si tuviera algún empleado muy disconforme?

Asegurar toda esta información puede parecer una tarea imposible. ¿Difícil? Sí. Pero no imposible. La respuesta es evaluación y tratamiento de riesgos (es decir, mitigación) en forma sistemática.

Elementos de la gestión de riesgos

Las metodologías para la gestión de riesgos varían pero, en esencia, se trata de encontrar qué tipo de cosas malas puede ocurrirle a cada pieza de información de su empresa. El tratamiento del riesgo es encontrar las mejores formas (y las más económicas, como se explicó en el Paso 2) para mitigar los riesgos más importantes.

Por lo tanto, la evaluación y el tratamiento de riesgos debería ser la pieza central de su ciberseguridad, y todas las medidas de protección (o, al menos, la mayoría de ellas) deberían ser implementadas en función de la gestión del riesgo. De otra forma, se puede encontrar invirtiendo enormes cantidades de dinero en determinadas medidas de protección que, en realidad, no son necesarias (es decir, no hay riesgos o son muy bajos), mientras que otros riesgos más importantes quedan desatendidos.

No confíe en el instinto de alguien para tomar consciencia de todos los riesgos. En mi

experiencia, las personas que trabajan en TI generalmente son conscientes solamente del 40% de los riesgos que hay en su sector, mientras que quienes pertenecen a la parte comercial de la organización están incluso menos enterados, conocen alrededor de un 25% de los riesgos. Para tener una mejor visión sobre qué riesgos puede haber en su empresa, consulte esta Lista de amenazas y vulnerabilidades.

Paso 7: Implementar las medidas de protección

Una vez que haya terminado con la evaluación y tratamiento de riesgos, asegúrese de redactar un plan de acción bien preciso. Aquí debería indicar específicamente qué se debe implementar, cuáles son los plazos, quién es responsable, cuál es el presupuesto y a quién se debe informar sobre la implementación. Este plan de acción debe ser incorporado a su plan del proyecto.

La implementación de la ciberseguridad se realiza, generalmente, de la siguiente forma:

1) **Definiendo nuevas reglas:** las reglas son documentadas a través de políticas, procedimientos, instrucciones y otras formas; aunque no será necesario documentar algunos procesos menos complejos. Es de suma importancia adaptar su documentación en función de sus necesidades reales. Por ejemplo: si usted es una empresa pequeña con 50 empleados, obviamente no querrá 150 nuevas políticas y procedimientos de 20 o más páginas cada uno. Además, es recomendable identificar las reglas vigentes que funcionan correctamente en su empresa; no tiene que

cambiar todo simplemente porque está implementando la norma ISO 27001. Recuerde el mito de la documentación que mencionamos en la Sección 2: redactar los documentos no es suficiente; es mucho más importante vivir esas reglas en las actividades diarias.

2) **Implementando nueva tecnología:** como dijimos anteriormente, piense mucho antes de comprar nuevos sistemas que demanden gran inversión. Seguramente existirán alternativas igual de efectivas y mucho más económicas. Además, tenga presente que la mayoría de los riesgos existen por conductas humanas, no por las máquinas. Entonces, la pregunta es si una máquina sería la solución a ese tipo de problemas.
3) **Cambiando la estructura organizacional:** en algunos casos necesitará introducir un nuevo cargo o modificar las responsabilidades de un puesto existente. Un ejemplo típico es agregar el puesto de Jefe de seguridad de la información que reporte directamente al Directorio. Generalmente, esta persona proviene del departamento de TI, pero para evitar un conflicto de intereses, el puesto tiene que ser cubierto con alguien que no sea de ese sector. La implementación de la

ciberseguridad también podría implicar que necesite contratar una persona a tiempo completo. En empresas más pequeñas trate de evitar estos incrementos de costos asignando tareas y responsabilidades adicionales al personal existente.

Desde una perspectiva gerencial, es importante que usted pueda verificar no solo si las medidas de protección se implementaron según lo planificado, sino, fundamentalmente, si lograron su objetivo.

Para poder hacer un seguimiento de sus medidas de protección necesita pedirle tres cosas a su equipo del proyecto:

(1) Que defina objetivos cuantificables para cada medida de protección implementada.

(2) Que defina un método con el cual su empresa medirá periódicamente el logro de los objetivos.

(3) Que establezca responsabilidades para medir y reportar los resultados.

No confunda estos objetivos y mediciones con los objetivos del Paso 3. En esa etapa yo me refería a los objetivos de toda la ciberseguridad, que permitirían evaluar si tenía sentido el proyecto en sí. En cambio, aquí hablamos de objetivos de menor nivel, para cada elemento de su

ciberseguridad, cuya finalidad es ajustar la sintonía fina de cada parte del sistema.

Esta es la única forma de crear una base para mejoras (siempre necesarias).

Paso 8: Capacitación y concienciación

La falta de capacitación y concienciación es el segundo motivo de fracaso de los proyectos de ciberseguridad. ¿Por qué?

La seguridad generalmente es una carga. Como mencionamos anteriormente, a nadie le gusta cambiar las contraseñas con mayor frecuencia que antes, además de tener que recordar las nuevas que son más complejas. Y esa actitud se presenta con todas las demás reglas de seguridad. Por eso, si no les explica a sus empleados por qué es necesario, probablemente ellos busquen formas de eludir esas reglas. La forma de abordar este tema es explicándoles los beneficios que tendrá su empresa con estas medidas de protección. También es igual de importante explicarles qué beneficios tendrán los empleados con esos cambios. Por ejemplo, si se utilizan contraseñas de alta seguridad, es mucho menos probable que alguien acceda sin permiso a sus cuentas; ya que, en caso que esto ocurra, tendría que ser el mismo empleado quien debería hacerse cargo de los daños que pudiera producir este incidente.

La seguridad, habitualmente, requiere nuevas habilidades. Si usted implementó un nuevo tipo de software (complicado), no puede esperar que

todos los empleados comiencen a utilizarlo simplemente a partir de la lectura del manual. Necesitan capacitación si quiere evitar errores.

Al planificar sus programas de capacitación y concienciación, hay tres cosas que debe tener en mente:

1) Debido a que la ciberseguridad no es el único trabajo de la gente de TI, deberá **implementar esos programas para toda la empresa**. Es más, deberá concentrarse en los empleados del sector comercial de la organización ya que, en general, ellos perciben la seguridad de la información como el trabajo de otro, no suyo.
2) Cuando implemente las nuevas medidas de protección, **al mismo tiempo deberá planificar sesiones de capacitación y concienciación**. No puede pretender que todos acepten una nueva regla con entusiasmo si el procedimiento fue publicado seis meses atrás y usted ahora está intentando generar conciencia.
3) No es suficiente hacer una sola vez las sesiones de capacitación y concienciación. Habrá nuevas personas en la empresa, los que ya estaban se olvidarán lo que escucharon, las medidas de protección

cambiarán, etc. Entonces, la **capacitación y concienciación es un proceso permanente**; por eso, su Jefe de seguridad de la información y/o su departamento de recursos humanos tendrán que trabajar en consecuencia.

(Paso 9): La ciberseguridad es una historia sin fin

Este no es, en realidad, un paso más sino una serie de actividades que debería realizar permanentemente si desea que su ciberseguridad sea efectiva.

Lamentablemente, muchas veces he visto empresas invertir mucho esfuerzo y recursos y luego, una vez terminada la implementación, dejan de lado todas las políticas, procedimientos y tecnología porque quedaron desactualizadas y ya no sirven. ¿Ya mencioné que este es el tercer motivo de los fracasos más comunes de la ciberseguridad?

Si usted quiere evitar esto, tendrá que concentrarse en las siguientes actividades para mantener y mejorar su sistema:

Supervisión: Los empleados responsables de determinadas medidas de protección deberán controlar su funcionamiento. Generalmente, esto se hace en forma regular. Por ejemplo, un administrador de sistema puede verificar todos los días si las copias de seguridad se generaron correctamente. Cuando se realizan los controles, es vital registrar todos los incidentes para saber

por qué se produjeron y cómo evitar que vuelvan a ocurrir.

Medición: Al contrario de la supervisión, la medición se efectúa con menor periodicidad (por ej., trimestral o anualmente) y su finalidad es determinar si se cumplieron los objetivos. Existen al menos dos niveles de objetivos: los objetivos generales establecidos para todo el sistema de ciberseguridad (ver el Paso 3) y objetivos determinados para cada control individual (ver Paso 7).

Escuchar sugerencias: Todas las partes involucradas (empleados, socios, clientes, organismos oficiales, etc.) probablemente sepan dónde puede estar fallando su seguridad. Usted necesita asegurarse de mantener abiertos los canales de comunicación y que toda la información llegue a las personas indicadas dentro de su empresa.

Auditoría interna: A pesar de que muchas empresas perciben a una auditoría como una pérdida de dinero, en realidad, esto puede ser bastante útil si se realiza correctamente. La realidad es que muchos empleados buscarán sortear estas reglas para dedicarles el menor tiempo posible a las tareas que ellos consideran irrelevantes. En algunos casos, los empleados están convencidos de estar haciendo las cosas

correctamente, para luego descubrir que es todo lo contrario. Es muy difícil descubrir estos desvíos a menos que alguien (objetivo y minucioso) controle si todo el mundo cumple con las normas.

También debería realizar auditorías a sus proveedores y asociados que tengan acceso a su información crítica y sistemas. En última instancia, una auditoría interna puede ser el mayor aporte para mejorar la seguridad de su información.

Revisión de la alta gerencia: Cada tanto, por ejemplo, trimestralmente, miembros de su alta gerencia deberían dedicarle un tiempo a la ciberseguridad. En general, esto se realiza en las reuniones gerenciales periódicas, en las que un tema es la ciberseguridad. Para esa reunión, la persona a cargo de la ciberseguridad debería preparar material que incluya: resultados de mediciones, de auditorías internas, lista de incidentes, nuevas amenazas identificadas, inversiones necesarias, propuestas de cambio en políticas, etc. En función de estos datos, los altos ejecutivos deberían tomar decisiones importantes, como ser: modificar los objetivos de la ciberseguridad, proporcionar recursos, hacer cambios organizacionales, eliminar obstáculos en la implementación, etc.

Auditorías de certificación: Estas auditorías pueden no ser obligatorias, pero podrían ser útiles con fines comerciales. También pueden ayudar para mejorar el nivel de seguridad, porque si todo el mundo dentro de la empresa sabe que habrá una auditoría de certificación programada para una determinada fecha, se pondrá mayor esfuerzo para hacer que todo esté perfecto.

Mejora continua: Todas las actividades mencionadas crearán una especie de lista de "cosas por hacer" que deben ser implementadas. Las normas ISO tienen una forma práctica de abordar esas listas en forma sistemática: este concepto es el de *medidas correctivas y preventivas*. Estas medidas deben ser enumeradas en forma transparente, con plazos y responsabilidades bien definidos y una vez implementadas todas deben ser verificadas para garantizar que el problema realmente fue eliminado.

Y ahí están los 9 pasos que necesita seguir. Si bien esto puede parecer que demande tiempo y que sea un desafío, permítame preguntarle algo: si omite alguno de estos pasos, ¿le parece que su ciberseguridad funcionará?

La respuesta probablemente sea que no.

Es por esto que pienso que es extremadamente importante que conozca cuáles son los elementos de su ciberseguridad, para que cuando delegue la implementación en sus especialistas, no olviden ningún paso importante.

Capítulo 5: Conclusión

Trabajando con muchas empresas y ayudándolas a implementar proyectos de seguridad de la información o ciberseguridad, me he dado cuenta de un hecho esencial: la gerencia de la mayoría de las empresas tenía conceptos erróneos sobre lo que realmente es la ciberseguridad.

Es más, demasiado pocos de ellos tenían una idea real sobre cómo la ciberseguridad podía ser de ayuda para su negocio principal.

Por eso, espero que este libro le haya ayudado a comprender todos estos temas y le haya explicado cómo utilizar la ciberseguridad como una herramienta para hacer que su negocio sea más exitoso.

Apéndice

Legislación relacionada con seguridad de la información y continuidad del negocio

Para consultar un listado no oficial de leyes y normas en todo el mundo, haga clic aquí.

A continuación encontrará la lista de leyes y normas que tienen requisitos relacionados con seguridad de la información y continuidad del negocio.

Argentina

DATOS PERSONALES Y PRIVACIDAD

1. Ley 25.326 Protección de los Datos Personales, Boletín Oficial: Noviembre 2 de 2000, 2000.
2. Decreto 1558/2001 Reglamentación de la Ley N° 25.326, Boletín Oficial:03.12.2001, 2001.
3. Ley N° 24.766 de confidencialidad sobre información y productos que estén legítimamente bajo control de una persona

y se divulgue indebidamente de manera contraria a los usos comerciales honestos, 1996.
4. Ley N° 26.529 Derechos del Paciente en su Relación con los Profesionales e Instituciones de la Salud, 2009.
5. Ley N° 26.529 de Actos Discriminatorios , Boletín Oficial 8/7/2002, 1988.
6. Ley N° 23.511 Banco Nacional de Datos Genéticos (BNDG), 1987.
7. Decreto 38/2013 que reglamenta la Ley 26.548 sobre el Registro Nacional de Datos Genéticos (BNDG), 2013.
8. Ley N° 1.472 Código Contravención de la Ciudad Autónoma de Buenos Aires, BOCBA N° 2055 del 28/10/2004, 2004.
9. Ley N° 2.602 de la Ciudad Autónoma de Buenos Aires sanciona con fuerza de Ley, BOCBA N° 2852 del 17/01/2008, 2008.
10. Ley N° 3.130 de la Ciudad Autónoma de Buenos Aires sanciona con fuerza de Ley, BOCBA N° 3251 del 04/09/2009, 2009.
11. Ley 21.173 Código Civil el art. 1071 bis, Boletín Oficial del 22-oct-1975, 1975.

DISPOSICIONES DE LA DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES (DNPDP)

1. DISPOSICION Nº 2/2003, de la Dirección Nacional de Protección de Datos Personales (DNPDP), 2003.
2. DISPOSICION Nº 1/2004, de la Dirección Nacional de Protección de Datos Personales (DNPDP), 2004.
3. DISPOSICION Nº 4/2004, de la Dirección Nacional de Protección de Datos Personales (DNPDP), 2004.
4. DISPOSICION Nº 2/2005, de la Dirección Nacional de Protección de Datos Personales (DNPDP), 2005.
5. DISPOSICION Nº 7/2005, de la Dirección Nacional de Protección de Datos Personales (DNPDP), 2005.
6. DISPOSICION Nº 2/2006, de la Dirección Nacional de Protección de Datos Personales (DNPDP), 2006.
7. DISPOSICION Nº 11/2006, de la Dirección Nacional de Protección de Datos Personales (DNPDP), 2006.
8. DISPOSICION Nº 2/2008, de la Dirección Nacional de Protección de Datos Personales (DNPDP), 2008.
9. DISPOSICION Nº 3/2008, de la Dirección Nacional de Protección de Datos Personales (DNPDP), 2008.

10. DISPOSICION Nº 3/2012, de la Dirección Nacional de Protección de Datos Personales (DNPDP), 2012.
11. DISPOSICION Nº 6/2008, de la Dirección Nacional de Protección de Datos Personales (DNPDP), 2008.
12. DISPOSICION Nº 7/2008, de la Dirección Nacional de Protección de Datos Personales (DNPDP), 2008.
13. DISPOSICION Nº 10/2008, de la Dirección Nacional de Protección de Datos Personales (DNPDP), 2008.
14. DISPOSICION Nº 4/2009, de la Dirección Nacional de Protección de Datos Personales (DNPDP), 2009.
15. DISPOSICION Nº 12/2010, de la Dirección Nacional de Protección de Datos Personales (DNPDP), 2010.
16. DISPOSICION Nº 17/2010, de la Dirección Nacional de Protección de Datos Personales (DNPDP), 2010.
17. DISPOSICION Nº 24/2010, de la Dirección Nacional de Protección de Datos Personales (DNPDP), 2010.
18. DISPOSICION Nº 3/2012, de la Dirección Nacional de Protección de Datos Personales (DNPDP), 2012.

19. DISPOSICION Nº 4/2012, de la Dirección Nacional de Protección de Datos Personales (DNPDP), 2012.

DELITOS INFORMÁTICOS Y CIBERSEGURIDAD

1. Código Penal De La Nación Argentina, Nº Ley 11.179, 1984.
2. Ley 26.388 De Ley De Delitos Informáticos, 2008.
3. Convención de Budapest sobre Ciberdelincuencia, Serie de Tratados Europeos- n° 185, 2001.
4. Declaración “Fortalecimiento de la Seguridad Cibernética en las Américas”, 2012.
5. Declaración de Panamá sobre “La Protección de la Infraestructura Crítica en el Hemisferio frente al Terrorismo”, 2007.
6. Ley 2.257 Del Gobierno De La Ciudad De Buenos Aires, BOCBA N° 2609 del 22/01/2007, 2007.
7. Resolución 501/fg/12 De La Fiscalía General De La Ciudad Autónoma De Buenos Aires, 2012.
8. Resolución 580/2011 De La Jefatura De Gabinete De Ministros, 2011.
9. Decreto 1766/2011, 2011.

10. Decisión Administrativa 669/2004 De La Jefatura De Gabinete De Ministros, 2004.
11. Disposición 6/2005 De La Oficina Nacional De Tecnologías De Información (ONTI), 2005.
12. Ley 863 De La Legislatura De La Ciudad Autónoma De Buenos Aires, BOCBA N° 1526 del 16/09/2002, 2002.
13. Código Contravencional De La Ciudad De Buenos Aires, Ley N° 1.472, BOCBA N° 2055 del 28/10/2004, 2004.
14. Comunicación "b" 9042 Del Banco Central De La República Argentina (BCRA), 2007.

COMERCIO ELECTRÓNICO Y CONTRATACIÓN ELECTRÓNICA

1. Resolución 412/99 Del Ministerio De Economía y Obras y Servicios Públicos, B.O.:09/04/99, 1999.
2. Resolución 104/2005 De La Secretaría De Coordinación Técnica, 2005.
3. Decreto 1023/2001, 2001.
4. Ley 2.244 De La Ciudad Autónoma De Buenos Aires, Boletín Oficial Nº 2612, 2007.
5. Ley 2.817 De La Ciudad Autónoma De Buenos Aires, BOCBA N° 3022 del 25/09/2008, 2008.

6. Resolución 412/99 Del Ministerio De Economía, Obras Y Servicios Públicos, B.O.:09/04/99, 1999.
7. Ley 26.104, Publicidad Con Fines Turísticos, 2006.
8. Ley 24.240 De Defensa Al Consumidor, 1993.
9. Resolución 33.463/08 De La Superintendencia De Seguros De La Nación, 2008.
10. Resolución 7/2002 De La Secretaría De La Competencia, La Desregulación Y La Defensa Del Consumidor, 2002.
11. Resolución 53/2003 De La Secretaría De La Competencia, La Desregulación Y La Defensa Del Consumidor, 2003.
12. Resolución 26/2003 De La Secretaría De Coordinación Técnica

NOMBRES DE DOMINIO

1. Decreto 189/2011, 2011.
2. Decreto 2085/2011, 2011.
3. Resolución 654/2009 Del Ministerio De Relaciones Exteriores, Comercio Internacional Y Culto, 2009.
4. Resolución 203/2009 Del Ministerio De Relaciones Exteriores, Comercio Internacional Y Culto, 2009.

5. Resolución 616/2008 Del Ministerio De Relaciones Exteriores, Comercio Internacional Y Culto, 2008.
6. Resolución 2226/2000 Del Ministerio De Relaciones Exteriores, Comercio Internacional Y Culto, 2000.

MARCAS COMERCIALES

1. Ley 22.362 De Marcas Y Designaciones, 1980.
2. Resolución Inpi 266/2012, 2012.

DERECHOS DE AUTOR

1. Ley 25.036 Propiedad Intelectual, B.O.: 11/11/98, 1998.
2. Ley 25.140 Apruébense el Convenio de Berna para la Protección de las Obras Literarias y Artísticas, el Tratado de la Organización Mundial de la Propiedad Intelectual —OMPI— sobre Interpretación o Ejecución y Fonogramas y el Tratado de la Organización Mundial de la Propiedad Intelectual, estos dos últimos, abiertos a la firma en Ginebra, 1999.
3. Decreto 165/94, 1994.
4. Ley Nº 24.425 Apruébese el Acta Final en que se incorporan los resultados de la

Ronda Uruguay de Negociaciones Comerciales Multilaterales; las Decisiones, Declaraciones y Entendimiento Ministeriales y el Acuerdo de Marrakesh, 1994.
5. Decreto 5.146/69 que reglamenta la Ley 17.648 de SADAIC, 1969.
6. Decreto 1670/74 sobre el Régimen de Uso de las reproducciones y grabaciones fonográficas, 1974.
7. Decreto 1671/74 que establece las normas para la utilización pública de las reproducciones fonográficas. Representación legal de AADI y CAPIF, régimen de reparto de las retribuciones, 1974.
8. Decreto 746/73 que enumera a quién se considera interprete y los medios aptos para difundir sus trabajos, 1973.
9. Ley 25.446 Ley Del Fomento Del Libro Y La Lectura, 2001.

DOCUMENTO ELECTRÓNICO

1. Ley 24.624 de Presupuesto General de la Administración Nacional (1996), 1995.
2. Ley 26.685 de Expediente Electrónico, 2011.

FIRMA DIGITAL Y ELECTRÓNICA

1. Ley 25.506 de Firma Digital, 2011.
2. Decreto 2.628/02 que reglamenta la Ley Nº 25.506 de Firma Digital, 2002.
3. Resolución 45/97 De La Secretaría De La Función Pública, 1997.
4. Resolución 194/98 De La Secretaría De La Función Pública, 1998.
5. Decreto 427/98, implementa el régimen para el empleo de la Firma Digital en actos internos de la Administración Pública Nacional con los mismos efectos de la firma ológrafa, 1998.
6. Decreto 283/2003, autoriza a la Oficina Nacional de Tecnologías Informáticas (ONTI) a proveer certificados digitales para utilizarse en los circuitos de la Administración Pública Nacional que requieran Firma Digital, 2003.
7. Decreto 1028/2003, disuelve el Ente Administrador de Firma Digital creado por el Decreto 2628/2002 y lo reemplaza por la Oficina Nacional de Tecnologías de Información (ONTI) de la Subsecretaría de la Gestión Pública, 2003.
8. Decisión Administrativa 6/2007 de la Jefatura de Gabinete de Ministros, establece el marco normativo de Firma

Digital aplicable al otorgamiento y revocación de las licencias a los certificadores que así lo soliciten, 2007.

RÉGIMEN DE INTERNET

1. Decreto 1431/2001 establece que el acceso a la información contenida en la base de datos INFOJUS del SISTEMA ARGENTINO DE INFORMACIÓN JURÍDICA (SAIJ) será libre y gratuito, 2011.
2. Ley 3784 de la Ciudad Autónoma de Buenos Aires, BOCBA N° 3683 del 13/06/2011, 2011.
3. Decreto 1552/2010 Créase el Plan Nacional de Telecomunicaciones "Argentina Conectada", 2010.
4. Ley 25.873 Modificase la Ley Nº 19.798, en relación con la responsabilidad de los prestadores respecto de la captación y derivación de comunicaciones para su observación remota por parte del Poder Judicial o Ministerio Público, 2003.
5. Ley 25.690 Estableése que las empresas ISP (Internet Service Provider) tendrán la obligación de ofrecer software de protección que impida al acceso a sitios específicos, 2002.

6. Ley 26.032 Estableése que la búsqueda, recepción y difusión de información e ideas por medio del servicio de Internet se considera comprendida dentro de la garantía constitucional que ampara la libertad de expresión, 2005.
7. Decreto 554/97 Declárese de Interés Nacional el acceso de los habitantes de la República Argentina a la red mundial Internet, B.O.: 23/06/97, 1997.
8. Decreto 735/97 Créase la Comisión de Conexión con Internet, B.O: 8/8/97, 1997.
9. Decreto 1279/97 Declárese comprendido en la garantía constitucional que ampara la libertad de expresión al servicio de Internet, B.O: 1/12/97, 1997.
10. Resolución 2132/97 Adóptese el procedimiento de Audiencia Pública, previsto en el Reglamento General de Audiencias Públicas y Documentos de Consulta, para la presentación de inquietudes sobre aspectos relacionados con Internet, B.O.: 15/7/97, 1997.
11. Decreto 1018/98 Créase el Programa para el desarrollo de las comunicaciones telemáticas argentin@internet.todos, B.O: 7/9/98, 1998.
12. Resolución 1235/98 Determínese la inscripción que deberán incluir las facturas

emitidas por los Internet Provider, B.O: 28/5/98, 1998.
13. Decreto 1293/98 Declárese de Interés Nacional el proyecto "Internet 2 Argentina", destinado a la implementación, desarrollo y aplicaciones de una red de alta velocidad de telecomunicaciones, con el fin de interconectar centros académicos, científicos y tecnológicos en todo el territorio nacional, B.O: 10/11/98, 1998.
14. Decreto 1335/1999 Poder Ejecutivo Nacional, Boletín Oficial del 19-nov-1999, 1999.
15. Decreto 252/2000 Créase el Programa Nacional para la Sociedad de la Información, 2000.

GOBIERNO ELECTRÓNICO

1. Decreto 103/2001 Apruébese el Plan Nacional de Modernización, 2001.
2. Decreto 378/2005 Apruébense los Lineamientos Estratégicos para la puesta en marcha de los mencionados Planes, 2005.
3. Resolución 259/2003 De La Subsecretaría General De La Presidencia De La Nación, 2003.

4. Resolución General 1956/2005 De La Administración Federal De Ingresos Públicos (AFIP), 2005.
5. Decreto 1479/2009 Apruébese el Convenio Marco Sistema Unico de Boleto Electrónico suscripto el 16 de marzo de 2009. Modificación del Decreto N° 84/09, 2009.

PROMOCIÓN DE LAS NUEVAS EMPRESAS Y DE LA INDUSTRIA DEL SOFTWARE

1. Ley 4064 del Gobierno de la Ciudad de Buenos Aires de Promoción de Nuevas Empresas Porteñas, 2011.
2. Ley 25.856 de Asimilación de la Producción del Software como Actividad Industrial, 2003.
3. Ley 25.922 de Promoción de la Industria del Software, 2004.
4. Ley 26.692 de Promoción de la Industria del Software, 2011.
5. Decreto 1594/2004 Apruébese la reglamentación de la Ley N° 25.922, 2004.
6. Resolución 177/2010 del Ministerio de Industria y Turismo de Promoción de la Industria del Software, 2010.

Chile

1. Ley N° 17.336 Propiedad Intelectual, Ultima Modificación: 04-MAY-2010 Ley 20435, 1970.
2. Ley N° 19.223 Delitos Informáticos, Tipifica Figuras Penales Relativas A La Informática, 1993.
3. Ley De Propiedad Industrial D.F.L. Nº 3, 2006.
4. Ley N° 19.628 Protección De Datos De Caracter Personal, 1999.
5. Ley N° 19.927 Modifica El Código Penal, El Código De Procedimiento Penal Y El Código Procesal Penal En Materia De Delitos De Pornografía Infantil, 2004.
6. Ley N° 20.009 Limita La Responsabilidad De Los Usuarios De Tarjetas De Crédito Por Operaciones Realizadas Con Tarjetas Extraviadas, Hurtadas O Robadas, 2005.
7. Ley N° 20.575 Establece El Principio De Finalidad En El Tratamiento De Datos Personales, 2012.
8. Ley N° 20.285 Sobre Acceso A La Información Pública, 2008.
9. Ley N° 20.393 Establece La Responsabilidad Penal De Las Personas Jurídicas En Los Delitos De Lavado De Activos, Financiamiento Del Terrorismo Y Delitos De Cohecho Que Indica, 2009.

10. Decreto 83 Aprueba Norma Técnica Para Los Organos De La Administración Del Estado Sobre Seguridad Y Confidencialidad De Los Documentos Electrónicos, 2004.
11. Ley N° 19.799 Sobre Documentos Electrónicos, Firma Electrónica Y Servicios De Certificación De Dicha Firma, 2002.

España

1. Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la ley de propiedad intelectual.
2. Ley Orgánica 15/1999, de 13 de diciembre, de protección de los datos de carácter personal.
3. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
4. Ley 59/2003, de 19 de diciembre, de firma electrónica.
5. Ley 56/ 2007 o Ley para el Impulso de la Sociedad de la Información.
6. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos

7. Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
8. Real Decreto 3/2010, de 8 de enero (BOE de 29 de enero), por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
9. Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
10. Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
11. Magerit - versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
12. Guías CCN-STIC para la seguridad de los sistemas de la Administración Pública

México

1. Código Penal Federal, 2013.
2. Ley de Firma Electrónica del Distrito Federal, 2009.

3. Ley Para El Uso De Medios Electrónicos Del Estado De México, Decreto Número 142, 2010.
4. Ley de Protección de Datos Personales del Estado de México, Decreto Número 516, 2010.
5. Ley Federal De Protección Al Consumidor, Nueva Ley publicada en el Diario Oficial de la Federación el 24 de diciembre de 1992, 2012.
6. Ley Federal Del Derecho De Autor, Nueva Ley publicada en el Diario Oficial de la Federación el 24 de diciembre de 1996, 2012.
7. Ley Federal De Telecomunicaciones, Nueva Ley publicada en el Diario Oficial de la Federación el 7 de junio de 1995, 2013.
8. Código Federal De Procedimientos Civiles, 2013.
9. Código De Comercio, Nuevo Código publicado en el Diario Oficial de la Federación del 7 de octubre al 13 de diciembre de 1889, 2012.
10. Ley Döring, 2011.
11. Ley Federal De Transparencia Y Acceso A La Información Pública Gubernamental, Nueva Ley publicada en el Diario Oficial de la Federación el 11 de junio de 2002, 2012.

12. Acuerdo publicado en el Diario Oficial de la Federación el 12 de julio de 2010, Última reforma publicada DOF 22 de agosto de 2012, 2012.
13. Ley De Firma Electrónica Avanzada, Nueva Ley publicada en el Diario Oficial de la Federación el 11 de enero de 2012, 2012.
14. Manual Administrativo de Aplicación General en Materia de Tecnologías de Información y Comunicaciones, 2010.

Perú

NORMA QUE GARANTIZA LA LIBERTAD DE INFORMACIÓN

1. Ley No. 26301 Acción Constitucional de Habeas Dana, 1994.

NORMAS DE PROTECCIÓN AL DERECHO DE AUTOR

1. Decreto Legislativo No. 822 Ley sobre el Derecho de Autor (Protección Jurídica del Software), 1996.
2. Decisión No. 351 Régimen Común sobre Derecho de Autor y Derechos Conexos, 1993.

3. Resolución No. 0121-1998/ODA-INDECOPI aprueban lineamientos de la Oficina de Derechos de Autor sobre uso legal de los programas de ordenador (software), 1998.

NORMAS SOBRE DELITOS INFORMÁTICOS

1. Código Penal, 1991.
2. Ley No. 27309 Ley que incorpora los Delitos Informáticos al Código Penal, 2000.

NORMAS DE FIRMA Y CERTIFICADOS DIGITALES

1. Ley No. 27269 Ley de Firmas y Certificados Digitales, 2001.
2. Resolución Suprema No. 098-2000-JUS designan Comisión Multisectorial encargada de elaborar el reglamento de la ley de firmas y certificados digitales, 2002.
3. Resolución Ministerial No. 074-2000-ITINCI-DM designan representante del Ministerio ante la comisión multisectorial encargada de elaborar el reglamento de la ley de firmas y certificados digitales, 2000.
4. Resolución Ministerial No. 276-2000-MTC-15.01 designan representante del Ministerio ante comisión encargada de elaborar el

reglamento de la ley de firmas y certificados digitales, 2001.
5. Resolución Jefatural Nº 021-2001-INEI designan representantes del INEI ante el Consejo de Supervisión e Fedatarios Juramentados con Especialización en Informática, 2001.
6. Ley No. 27310 Ley que Modifica el Artículo 11º de la Ley 27269, 2000.

NORMAS QUE PERMITEN LA UTILIZACIÓN DE LOS MEDIOS ELECTRÓNICOSPARA LA COMUNICACIÓN PARA LA MANIFESTACIÓN DE VOLUNTAD

1. Ley No 27291 Ley que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica, 2000.

NORMAS QUE REGULAN EL USO DE LAS TECNOLOGÍAS DE INFORMACIÓN EN LA GESTIÓN DE ARCHIVOS Y DOCUMENTOS

1. Decreto Legislativo No. 681 Normas que Regulan el Uso de Tecnologías Avanzadas en Materia de Archivo de Documentos e Información tanto respecto a la Elaborada

en Forma Convencional cuanto la Producida por Procedimientos Informáticos en Computadoras, 1991.
2. Decreto Supremo No. 009-92-JUS Aprueban El Reglamento del Decreto Legislativo No. 681, Sobre el Uso de Tecnologías de Avanzada en Materia de Archivos de las Empresas
3. Decreto Ley No. 25661 Comprenden a la Banca Estatal de Fomento, dentro de los alcances del Decreto Legislativo No. 681, en cuanto al uso de las tecnologías de microformas, microduplicados, micrograbación y otros análogos, 2008.
4. Circular No. B-1922-92-SBS Circular referida a la sustitución de archivos, mediante microformas y plazos de conservación de libros y demás documentos, 1992.
5. Resolución No. 090-93-EF-94.10.0-CONASEV Dictan normas que permitan poner en práctica el uso de tecnologías avanzadas en materia de archivo de documentos, 1993.
6. Ley No. 26612 Ley que modifica el D. LEG. No. 681, mediante el cual se regula el Uso de Tecnologías Avanzadas en Materia de Archivo de Documentos e Información, 1996.

7. Decreto Legislativo No. 827 Amplían los Alcances del D. Leg. No. 681 a las Entidades Públicas a fin de modernizar el Sistema de Archivos Oficiales, 2011.
8. Decreto Supremo No. 002-98-ITINCI Aprueban Requisitos y Procedimiento para Otorgamiento de Certificado de Idoneidad Técnica para la Confección de Microformas, 1998.
9. Decreto Supremo No. 001-2000-JUS Aprueban el Reglamento Sobre la Aplicación de Normas que Regulan el Uso de Tecnologías Avanzadas en Materia de Archivo de Documentos e Información a Entidades Públicas y Privadas, 2000.
10. Resolución Ministerial No. 169-2000-JUS Aprueban Reglamento para supervisión de eventos de capacitación, conducentes al otorgamiento de certificado de idoneidad técnica de fedatario juramentado con especialidad en informática, 2000.
11. Ley No. 27323 Ley que modifica el Decreto Ley No. 26126, 2000.

NORMAS QUE FOMENTA EL USO DE FORMATOS ELECTRÓNICOS EN LAS ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA

1. Decreto Legislativo No 809 Ley General de Aduanas, 1996.
2. Decreto Supremo N° 121-96-EF Reglamento de la Ley General de Aduanas, 1997.
3. Resolución de Intendencia Nacional de Aduanas No 000 Adt/2000-000750 – Aprueban Formatos e Instructivos de la Declaración Unica de Aduanas (DUA) y la Orden de Embarque, 2000.
4. Resolución de Intendencia Nacional No 000 Adt-2000-001272 - Prorrogan entrada en vigencia de Resolución que aprueba Formatos e Instructivos de la Declaración Unica de Aduanas (DUA) y la Orden de Embarque, 2000.
5. Resolución de Intendencia Nacional de Sistemas No 001-2000- Aduanas - Estructura de Datos de la "Declaración Unica de Aduanas - Electrónica" (E-Dua), La "Orden de Embarque" y demás documentos del Despacho Aduanero Electrónico, 2000.
6. Resolución de Intendencia Nacional No 000 ADT-2000-002180 - Aprueban los Instructivos de Trabajo Declaración Unica de Aduanas (DUA) y Orden de Embarque (O/E), 2000.

7. Resolución de Intendencia Nacional de Aduanas Nş 000 ADT-2000-002797 - Modifican el Instructivo de Trabajo “Declaración Unica de Aduanas (DUA) INTA- T.00.04”, 2000.
8. Resolución de Superintendencia de Aduanas No 000103 – Establecen a nivel nacional uso obligatorio del “Formato Electrónico de Documentos Internos” (FEDI) en la tramitación interna de documentos que no estén relacionados con el despacho de mercancías, 2001.
9. Formulación y Tramitación de Documentos Institucionales – ADUANAS, 2001.
10. Resolución de Intendencia Nacional Nş 000 Adt/2001-000277 Aprueban Estructura de Solicitudes Electrónicas y Modifican El Procedimiento “Autorización de Operadores” INTA- E.00.08, 2001.
11. Resolución de Superintendencia No 002-2000/SUNAT – Dictan disposiciones referidas a La utilización de Programas de Declaración Telemática para la presentación de Declaraciones Tributarias, 2000.
12. Resolución de Superintendencia N° 044-2000/ SUNAT - Establecen disposiciones sobre Declaración y Pago de Diversas Obligaciones Tributarias, mediante

Programas de Declaración Telemática, 2000.
13. Resolución del Superintendente Nacional de los Registros Públicos No 124-97-SUNARP, Aprobar la sustitución del archivo Registral existente en la Oficina de Lima y Callao por un Sistema de Microarchivos
14. Ley No 27419 Ley Sobre Notificación por Correo Electrónico, 2001.
15. Decreto Supremo No 012-2001-PCM Texto Unico Ordenado de la Ley de Contrataciones y Adquisiciones del Estado, 2001.
16. Decreto Supremo No 013-2001-Pcm - Reglamento de la Ley de Contrataciones y Adquisiciones del Estado, 2001.

Bibliografía

BS 25999-2:2007, Gestión de la continuidad del negocio. Especificación

COBIT 5, Un marco de referencia para el gobierno y la administración de TI en la empresa

ISO/IEC 20000-1:2011, Tecnología de la información: Gestión del servicio. Parte 1: Requisitos del sistema de Gestión del Servicio

ISO 22301:2012, Seguridad de la sociedad: Sistemas de gestión de continuidad del negocio. Requisitos

ISO/IEC 27000:2009, Tecnología de la información: Técnicas de seguridad. Sistemas de gestión de seguridad de la información: Resumen y terminología

ISO/IEC 27001:2005, Tecnología de la información: Técnicas de seguridad. Sistemas de gestión de seguridad de la información: Requisitos

ISO/IEC 27032:2012, Tecnología de la información: Técnicas de seguridad. Lineamientos sobre ciberseguridad

ITIL©, *Biblioteca de infraestructura de TI*

NFPA 1600, Norma sobre gestión de desastres y emergencias y programas de continuidad del negocio

Publicaciones especiales de NIST (serie 800)

PCI DSS, Norma de seguridad de datos de la industria de tarjetas de pago

http://blog.iso27001standard.com/ ISO 27001 & ISO 22301 Blog

Índice

Sobre el autor

Dejan Kosutic es autor de diversos artículos, tutoriales en vídeo, plantillas de documentación, webinars y cursos sobre gestión de seguridad de la información y continuidad del negocio.

Es el autor del principal blog sobre ISO 27001 – ISO 27001 & ISO 22301 Blog, y ha ayudado a muchas organizaciones, incluidas algunas instituciones financieras, organismos gubernamentales y empresas de TI, a implementar la gestión de seguridad de la información y continuidad del negocio en conformidad con esas normas.

Tiene un Máster en Gestión Empresarial (MBA) de Henley Management College (actualmente Henley Business School).

Haga clic aquí para consultar su perfil en LinkedIn.

Información de contacto

Nombre de la empresa: EPPS Services Ltd.
Autor: Dejan Kosutic
Domicilio: Nazorova 59, 10000 Zagreb, Croacia

Sitio web: http://www.iso27001standard.com/

Correo electrónico: info@iso27001standard.com

Teléfono: +385 98 304 566

Fax: +385 1 556 0711

Twitter: https://twitter.com/Dejan_Kosutic

Facebook:
http://www.facebook.com/pages/Information-Security-Business-Continuity-Academy/119822218040795