DOSSIER:
DERECHO, TECNOLOGÍAS Y PANDEMIA

Tengo el honor de presentarles este dossier especial sobre "Derecho, tecnologías y pandemia", fruto de un arduo trabajo realizado durante estos meses de confinamiento, que implicó un desafío conjunto entre docentes de distintas universidades. El logro obtenido, nos reconforta y esperamos sea de vuestro agrado.

Confiamos en que la temática propuesta concitará vuestro interés, teniendo en cuenta que la nueva normalidad ha demostrado hasta qué punto el mundo digital ya forma parte de nuestra vida cotidiana.

El Derecho no puede permanecer al margen de estos cambios.

Teniendo en cuenta que todos somos por igual ciudadanos del mundo digital, hemos pensado este Dossier, sujeto a referato, con el aporte de producciones de destacados docentes de diferentes nacionalidades: así podrán encontrar artículos de los Profesores españoles Luis López Lema –de la Universidad de Valencia– y Lucana Estevez –de la San Pablo SEU de Madrid–, así como también de Profesores locales, Mauro F. Leturia, Adrián E. Gochicoa Victoria Antonella Mongelos, Facundo Cerdá –de la Universidad Nacional de La Plata–, y Mariano Refi en conjunto con quien escribe estas líneas –ambos docentes de esta alta Casa de Estudios–. Confiamos que los artículos seleccionados abordan temas de indudable vigencia e interés, y les permitirán profundizar en sus conocimientos, incentivando la reflexión, y el debate.

Me permito unas últimas palabras. La magnitud de este aporte hubiera sido imposible sin la participación de varios actores. Mi más sincero agradecimiento a quienes contribuyeron a este feliz término.

Joselina Pastorini
Profesora de Derecho Penal
UCALP

La gestión de la información durante etapas de teletrabajo en la época de la COVID-19

Luis López Lema

Licenciado en Derecho por la Universidad de Valencia. Magister en Sistemas y Servicios en la Sociedad de la Información por la Universidad de Valencia. Delegado de protección de datos por el IVAC-INSTITUTO DE CERTIFICACIÓN S.L. Consultor de Nuevas Leyes y Tecnología, S.L. (LEYNET CONSULTORES). Docente de la Universidad Internacional de Valencia y de la Universidad de Florida de Valencia.

Resumen

La aparición de la COVID-19 ha cambiado nuestras vidas, desde los hábitos de higiene, las interacciones sociales y hasta la forma de trabajar dentro de las organizaciones. El nuevo cambio de paradigma ha obligado a la mayoría de las organizaciones a implantar sistemas de teletrabajo para poder tener continuidad de negocio durante los periodos de confinamiento. Ello ha generado nuevos estilos de trabajo, nuevos problemas de ciberseguridad, y, por tanto, cualquier organización debe replantearse tanto sus sistemas de información como las medidas de seguridad que venían aplicando para reducir los riesgos cibernéticos derivados del trabajo en remoto.

Palabras clave: Ciberseguridad, COVID-19, Teletrabajo, Privacidad, Protección de Datos.

Abstract

The emergence of COVID-19 has changed our lives, from the hygiene habits, social interactions, and even the way of working within organizations. The new paradigm shift has forced most organizations to implement teleworking systems in order to have business continuity during periods of confinement. This has generated new work styles, new cybersecurity problems, and therefore any organization must rethink both its information systems and the security measures that have been applied to reduce the cyber risks derived from remote work.

Keywords: Cibersecurity, COVID-19, Remote Work, Privacy, Data Protection.

1. Binomio formado por la información y la seguridad

La información es un activo vital que, como otros activos comerciales importantes y estratégicos, es esencial para el negocio de una organización y, en consecuencia, necesita ser protegido adecuadamente. En la Figura 1, se muestra de forma gráfica cómo un dato se convierte en un elemento de valor dentro de cualquier organización, tanto a nivel privado como público.

Figura 1. Cadena de valor de la información.

Fuente: elaboración propia.

Según la norma UNE ISO 27002 (2017) «La información es un activo que, al igual que otros activos del negocio, es esencial para la organización, y por lo tanto debe ser protegido de forma adecuada». (p. 9).

Por ello, es vital garantizar su seguridad, pero lograrla no es tarea fácil. Spafford (citado en Dewdney 1989), profesor de ciencias informáticas en la Universidad Purdue (Indiana, EEUU) y experto en seguridad de datos, dijo que:

> El único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aun así, yo no apostaría mi vida por él. (p. 110)

En general, en la actualidad, podemos entender que un sistema de información es seguro si podemos garantizar los tres pilares que se muestran en la Figura 2:

Figura 2. Pilares de la seguridad.

Fuente: Observatorio Tecnológico (2012).

La confidencialidad, la integridad y disponibilidad son los principales pilares de la seguridad porque ayudan a sacarle el máximo rendimiento de la información con el mínimo riesgo. Si alguno de estos pilares se debilita, se perderá seguridad, y, por tanto, la organización queda expuesta a ataques. Para comprender el alcance de cada uno de estos pilares, se debe conocer en detalle cuál es su función:

a) Confidencialidad: hace referencia a la necesidad de mantener el secreto de determinada información o recursos. Su objetivo es prevenir la divulgación no autorizada de la información.

Para garantizar la confidencialidad se pueden implementar, principalmente, las siguientes medidas técnicas:

- Sistemas de autenticación de usuarios
- Gestión de privilegios
- Sistemas de cifrado y encriptación

b) Integridad: hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado.

El objetivo de la integridad es prevenir modificaciones no autorizadas de la información; por ende, la integridad abarca tanto la propia información como su origen. Es importante hacer hincapié en la integridad del origen, ya que puede afectar su exactitud, su credibilidad y la confianza que las personas ponen en la información.

Para garantizar la integridad, se deben considerar las siguientes actividades:

- Sistemas de monitorización del tráfico de red para descubrir posibles intrusiones
- Sistemas de control de registros
- Sistemas de control de cambios

c) Disponibilidad**:** hace referencia a la accesibilidad del sistema y de los recursos del sistema de información. El objetivo de la disponibilidad es prevenir interrupciones no autorizadas/controladas de los recursos informáticos.

Para garantizar la disponibilidad, se pueden implementan las siguientes medidas:

- Firmar un acuerdo de nivel de servicio (o SLA por su acrónimo en inglés: *Service Level Agreement*).
- Balanceadores de carga.
- Sistemas de copias de seguridad.
- Disponer de recursos alternativos a los primarios.

Toda organización debe mantener el equilibrio entre estos tres pilares, debiendo ponderar las medidas de seguridad para que se consigan los tres sin que alguno de ellos sufra. Por ejemplo, no tiene sentido conseguir la confidencialidad a toda costa para un

archivo si después ni siquiera el usuario administrador puede acceder a él, ya que, en ese caso, se está negando la disponibilidad.

La propia UNE ISO 27002 (2017) determina que existen tres fuentes donde obtener los requisitos de seguridad que nos ayuden a velar por la integridad de estos tres pilares:

- Primera fuente: es el análisis de riesgo realizado por la propia organización. Como veremos en el capítulo siguiente, a través de una evaluación interna, se podrán averiguar las amenazas y su probabilidad de materialización, lo que ayudará a identificar las medidas de seguridad idóneas.
- Segunda fuente: es el cumplimiento de requisitos legales, estatutarios, reglamentarios y contractuales a los que la organización se encuentre sometida. Por ejemplo, la normativa de protección de datos de carácter personal, que se explicará más adelante.
- Tercera fuente: son los propios objetivos y requisitos del negocio que la organización se ha establecido como necesarios para dar soporte al tratamiento de la información. Es decir, las medidas internas que la organización se haya autoimpuesto.

1.1. Aproximación al concepto de seguridad de la información

Antes de la aparición de la COVID-19 en nuestras vidas, la tecnología ya había transformado nuestro día a día. De hecho, nadie concibe un día sin enviar un correo electrónico, conectarse a una red social, escuchar música o ver una serie a través de plataformas en línea. Y, por otra parte, en el mundo de la empresa, no se podría trabajar sin transacciones electrónicas o la utilización de servicios *cloud* para reducir costes y mejorar la productividad. Pero, indistintamente de un uso corporativo o personal, la utilización de la tecnología lleva aparejado un uso responsable y seguro de ella.

Voutssas Marquez (2010) expone que, para poder comprender el concepto integral de la seguridad informática, es indispensable entender los diversos conceptos básicos que la rigen. Se relacionan a continuación:

- Recursos informáticos: el equipo de cómputo y telecomunicaciones; los sistemas, programas y aplicaciones, así como los datos e información de una organización. También se les conoce como «activos informáticos».
- Amenaza: fuente o causa potencial de eventos o incidentes no deseados que pueden resultar en daño a los recursos informáticos de la organización.
- Impacto: la medida del efecto nocivo de un evento.
- Vulnerabilidad: característica o circunstancia de debilidad de un recurso informático la cual es susceptible de ser explotada por una amenaza.

- Riesgo: la probabilidad de que un evento nocivo ocurra combinado con su impacto en la organización.
- Principio básico de la seguridad informática: la seguridad informática no es un producto, es un proceso.

La seguridad informática se encarga de la seguridad del medio informático. Según Aguilera (2011), se puede definir a la seguridad informática como la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y, sobre todo, que tenga disponibilidad. La seguridad de la información no se preocupa solo por el medio informático, se preocupa por todo aquello que pueda contener información, por ejemplo, todos los soportes físicos.

Actualmente, la informática está siendo inundada por toda la información posible, pero la información por sí sola sigue siendo un universo más grande y, en muchos casos, más complejo de manejar, ya que los procesos, en ocasiones, no son tan visibles para los involucrados.

La principal tarea de la seguridad informática es la de minimizar los riesgos, que, en este caso, provienen de muchas partes: puede ser de la entrada de datos, del medio que transporta la información, del *hardware* que es usado para transmitir y recibir, de los mismos usuarios y hasta de los protocolos que se están implementando; pero siempre la tarea principal es minimizar los riesgos para obtener mejor y mayor seguridad.

Lo que debe contemplar la seguridad se puede clasificar en tres partes:

- Usuarios: considerados el eslabón más débil de la cadena, ya que las personas pueden cometer un error y olvidar algo o tener un accidente, y este suceso puede comprometer la información y que terceros puedan acceder a ella.
- Información: compuesta por la interpretación de todos los datos introducidos en el sistema, es el principal objetivo de la seguridad informática, ya que es lo que se desea proteger y lo que tiene que estar a salvo; en otras palabras, se dice que es el principal activo.
- Infraestructura: entendiéndose como todos los recursos necesarios para albergar, tratar y transmitir la información; puede ser uno de los medios más controlados para segurizar todos los procesos.

Y es en este punto donde los proveedores de servicios y tecnología relacionados con la ciberseguridad están cambiando las prioridades para respaldar las necesidades actuales: continuidad del negocio, trabajo remoto y planificación para la transición a la siguiente normalidad.

1.2 Los elementos vulnerables de un sistema de información

Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Conviene aclarar que, no siendo posible la certeza absoluta, el elemento de riesgo está siempre presente, independientemente de las medidas que tomemos, por lo que debemos hablar de niveles de seguridad, ya que la seguridad absoluta no es posible. En adelante, entenderemos que la seguridad informática es un conjunto de técnicas encaminadas a obtener niveles altos de seguridad.

La seguridad es un problema integral; los problemas de seguridad informática no pueden ser tratados aisladamente, ya que la seguridad de todo el sistema es igual a su punto más débil. El uso de sofisticados algoritmos y métodos es inútil si no garantizamos la confidencialidad de las estaciones de trabajo. Por otra parte, existe algo que los *hackers* llaman *ingeniería asociada*, que consiste simplemente en conseguir, mediante un engaño, que los usuarios autorizados revelen sus contraseñas. Por lo tanto, la educación de los usuarios es fundamental para que la tecnología de seguridad pueda funcionar.

En vista de estas manifestaciones, hay tres elementos principales que proteger en cualquier sistema informático: el *software*, el *hardware* y los datos.

- Por *hardware* entendemos el conjunto de todos los elementos físicos de un sistema informático, como CPU, terminales, cableados, medios de almacenamiento secundarios, tarjeta de red, etc.
- Por *software* entendemos el conjunto de programas lógicos que hacen funcionar el *hardware*, tanto sistemas operativos como aplicaciones.
- Por datos, el conjunto de información lógica que maneja el *software* y el hardware, por ejemplo, paquetes que circulan por un cable de red o entradas de una base de datos.

Por ende, y en conclusión, tenemos que ser conscientes de que las medidas de seguridad que deberán establecerse en cualquier sistema de información comprenderán y tendrán repercusión sobre el *hardware*, el sistema operativo, las comunicaciones y los soportes físicos.

2. Riesgos en la seguridad de la información

Debemos entender como riesgo cualquier posibilidad de que se materialice una amenaza o situación que provoque un ataque a los sistemas de información y produzca el quebrantamiento de alguno de los pilares comentados anteriormente.

Según Voutssas Marquez (2010), el riesgo es la probabilidad de que un evento nocivo ocurra combinado con su impacto o efecto perjudicial en la organización. Se materializa cuando una amenaza actúa sobre una vulnerabilidad y causa un impacto.

La dependencia informática tan fuerte a la que las organizaciones se encuentran sometidas, junto con la inexorable evolución de las telecomunicaciones para interactuar en Internet y compartir información, ya había cambiado el paradigma de la seguridad y la expectativa de privacidad de la información de las organizaciones, pero, a raíz de la aparición de la COVID-19, dicho paradigma se ha visto incrementado.

La pandemia no solo ha supuesto un riesgo y peligro para la salud de los humanos, sino que también resulta un riesgo para la seguridad de los sistemas informáticos, ya que han aumento los ataques de *phishing*, *malspams* y de *ransomware,* utilizando precisamente el reclamo de la COVID-19 como cebo para hacerse pasar por marcas de productos de protección individual frente al virus a fin de infectar el terminal.

También las aplicaciones relacionadas con ayuda sobre la COVID-19, o incluso las mismas aplicaciones gubernamentales publicadas para controlar a nivel nacional el virus, están siendo suplantadas para infectar de *ransomware* a los usuarios.

Y es que, con el solo hecho de abrir un correo electrónico o realizar una transacción en línea, podemos poner en riesgo la seguridad corporativa de toda la organización. Por ello, todo usuario debe concienciarse sobre la importancia de la seguridad informática, ya que el factor humano es el eslabón más débil en lo que respecta la integridad de la información.

2.1. La incidencia de la COVID-19 en la seguridad de la información

La estimación de Cybersecurity Ventures en su informe de 2020 establece que los costes de daños por delitos cibernéticos podrían potencialmente duplicarse durante el período del brote de coronavirus y no solo por las estafas de *phishing*, sino también por los ataques de *ransomware*, debido al acceso remoto inseguro a las redes corporativas, por la falta de formación de los trabajadores remotos que exponen las credenciales de inicio de sesión de sus terminales con el resto de miembros de su núcleo familiar, así como por la utilización de los equipos informáticos por parte de todos los miembros de su núcleo familiar y, por ello, comprometer los archivos e informaciones de la compañía.

Actualmente, las principales situaciones que comprometen la seguridad de la información donde el factor humano es determinante son las siguientes:

a) El trabajo remoto

La COVID-19 ha llevado a que una gran cantidad de empleados en todo el mundo sean enviados a casa para trabajar de forma remota. La gran mayoría de ellos, al trabajar desde fuera de su entorno empresarial o institucional, tienen recursos mínimos de seguridad informática en comparación con los que normalmente tienen a su disposición cuando trabajan en su puesto de trabajo habitual.

Por otra parte, la forma tan repentina y precipitada con las que las organizaciones han optado por el teletrabajo no ha permitido capacitar a los empleados remotos

sobre cómo detectar y reaccionar ante estafas de *phishing* y otros tipos de ataques cibernéticos.

b) Uso incorrecto de la tecnología

Hemos pasado de tener solo el ordenador en el puesto de trabajo dentro de la oficina a llevarlo en el bolsillo y estar constantemente conectados a él. Y es que, aunque no lo parezca, los teléfonos móviles son pequeños ordenadores. Los dispositivos que nos rodean y que se utilizan de forma cotidiana para el desempeño de las tareas empresariales permiten tener la conectividad total de tal forma que, actualmente, se puede estar controlando una empresa desde cualquier parte del mundo sin necesidad de estar conectado en un puesto fijo dentro de una oficina. Pero el uso inadecuado de estas características también puede poner en riesgo nuestra información. Por ejemplo, conectarse a una red wifi no segura puede permitir que terceros accedan al contenido del dispositivo; instalar *software* ilegal puede facilitar un ataque informático; no tener actualizados los sistemas operativos podría derivar en una brecha de seguridad por no tener los últimos parches de seguridad instalados, etc.

Además, la falta de conciencia de seguridad puede implicar también el no realizar copias de respaldo o de seguridad. O realizarlas de forma poco segura, como almacenarla en el propio ordenador, con lo que, al final, si este resultara afectado, la copia de respaldo también quedaría afectada.

En definitiva, ser prudentes con la tecnología y hacer un uso consciente siempre garantizará un nivel de seguridad de la información.

c) Virus, códigos maliciosos y engaños

La información está expuesta constantemente a virus, códigos maliciosos, troyanos, etc., bien porque llegan a través de correo electrónico, por la descarga e instalación de *software* ilegal, por la navegación por sitios poco seguros, por la introducción de dispositivos de almacenamiento externo, etc.

Sin ir más lejos, un troyano se puede autoinstalar en un ordenador gracias a una memoria extraíble USB. Las memorias extraíbles pueden ser útiles, pero también son una gran fuente de contagio, por lo que siempre que sea posible, en una organización, no deberían aceptarse dispositivos ajenos para el traslado de información.

Este tipo de amenazas pueden provocar la pérdida definitiva de la información, su secuestro o incluso que monitoreen la actividad realizada por el usuario para descubrir contraseñas, números de tarjeta de crédito o cualquier otra información sensible para la comisión de alguna actuación cibercriminal.

Gran parte de estas amenazas se pueden evitar o incluso se podrían eliminar a través de un buen *software* antivirus y sistemas de cortafuego. Pero tener un antivirus no

es garantía total de no ser infectado, ya que, dependiendo de las actividades que realicemos, vamos a estar más o menos expuestos ante este tipo de amenazas.

Por ello, y al hilo del punto anterior, hace falta tener un buen criterio analítico a la hora de gestionar el correo electrónico, debiendo evitar descargar archivos adjuntos de correos electrónicos de personas o entidades desconocidas. Pero, sobre todo, asegurarse de que el emisor es quien dice ser, ya que, en muchos casos, se reciben correos electrónicos supuestamente de la entidad bancaria con la única finalidad de engañar al usuario para conocer sus claves personales con fines delictivos.

Sin embargo, no solo se debe tener cuidado con los correos electrónicos, sino también con las redes sociales, ya que, en ocasiones, se puede recibir un mensaje directo de un desconocido, que indique el acceso a un determinado enlace. Ese *link* puede conducir a un portal web infectado con *malware* que termine infectando el ordenador o el teléfono móvil.

Todos los días, Gmail[1] bloquea más de 100 millones de correos electrónicos de *phishing*; ha llegado a detectar 18 millones de correos electrónicos de *phishing* y *malware* diarios relacionados con COVID-19. Esto se suma a más de 240 millones de mensajes de *spam* diarios relacionados con COVID. Ante esta situación, el servicio de correo electrónico de Google ha evolucionado sus sistemas para comprender y filtrar estas amenazas, y, con ello, poder lograr el bloqueo de más del 99,9 % del *spam*, el *phishing* y el *malware* para que no lleguen a sus usuarios.

d) Externalización de gestiones

Las soluciones *cloud computing* han propiciado el desarrollo de plataformas que permiten mejorar el almacenamiento de la información de las organizaciones, bien teniendo más capacidad para guardar información, bien teniendo herramientas que mejoran su tratamiento. A pesar de las potenciales ventajas que supone la tecnología en la nube, es evidente que delegar la gestión de la información en terceros entraña cierto riesgo, puesto que deja de estar bajo la propia gestión.

A veces, en la contratación de estos proveedores, prima más la oferta económica que la seguridad. Por ejemplo, pongamos el caso de servicios de alojamiento de datos, donde, en la mayoría de las situaciones, se puede optar por un servicio gratuito. No debemos dejar de lado el hecho de que muchos de estos proveedores, a cambio de sus servicios, utilizan los datos proporcionados por los propios usuarios para compartirlos con terceros y, de esta forma, ofrecer productos y servicios de acuerdo a sus hábitos.

Además, en la mayoría de las situaciones en las que se contrata este tipo de servicios, no se realiza una lectura detenida de los términos y condiciones publicados en el

[1] https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond

portal web del potencial proveedor para conocer de forma detallada cómo se van a manejan los datos y las medidas de seguridad que aplican.

e) Robo, pérdida y extravío de dispositivos

De todas las situaciones descritas anteriormente, esta puede ser la más difícil de controlar, ya que muchas veces dependerá del azar. Por ese mismo motivo, se deben de adoptar medidas preventivas, por ejemplo, un sistema de bloqueo remoto para que ningún tercero pueda ver la información o implantar medidas de rastreo y geolocalización para poder localizar los dispositivos.

2.2 Análisis de vulnerabilidades y metodología

Para la correcta conjugación de los elementos anteriores, se requiere implementar una metodología de análisis de vulnerabilidades con la finalidad de tratar de mitigar o reducir los riesgos detectados dentro de los sistemas de información. Todo ello, bajo un proceso que el INCIBE (2017) —siglas del Instituto Nacional de Ciberseguridad de España— plantea en las fases ilustradas en la Figura 4.

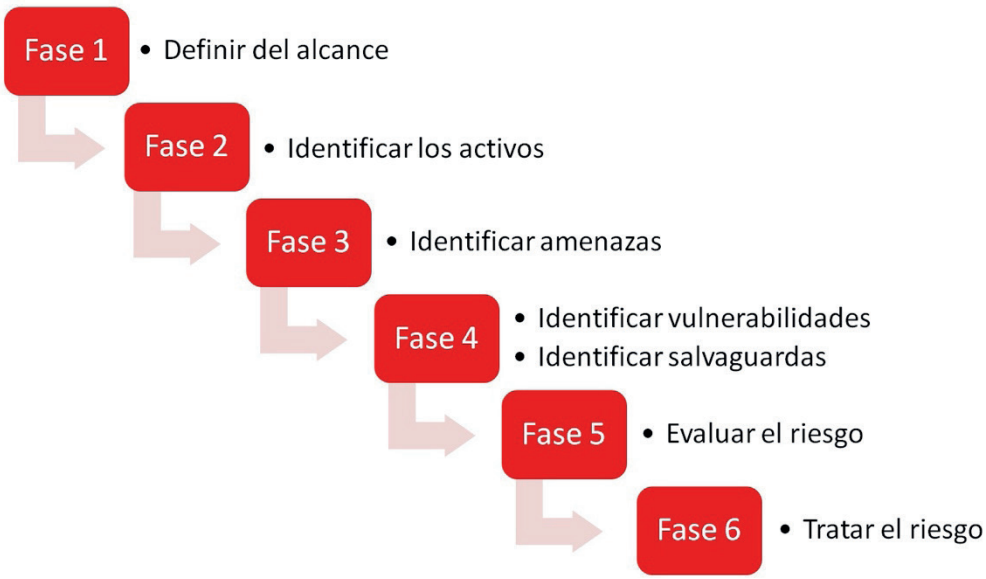

Figura 4. Fases de un sistema de gestión de riesgos.

Fuente: INCIBE (2017).

Fase 1. Concreción de que se quiere analizar

El punto de partida para un correcto análisis de riesgo es saber sobre qué parte de la organización se va a realizar, es decir, si afecta a la seguridad de la información de un determinado departamento, de un determinado proceso, de un sistema en particular, etc.

Fase 2. Identificar los activos

Teniendo claro qué se quiere analizar, se deben identificar los recursos que conforman ese sistema de información que guardan relación con el departamento, proceso o sistema objeto del estudio. Para mantener un inventario de activos sencillo, puede ser suficiente con hacer uso de una hoja de cálculo o tabla, como la que se muestra a continuación en la Figura 5.

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
ID_01	Servidor 01	Servidor de contabilidad.	Director Financiero	Servidor (Físico)	Sala de CPD1	Sí
ID_02	RouterWifi	Router para la red WiFi de cortesía a los clientes.	Dept. Informática	Router (Físico)	Sala de CPD1	No
ID_03	Servidor 02	Servidor para la página web corporativa.	Dept. Informática	Servidor (Físico)	CPD externo	Sí
...						

Figura 5. Modelo de inventario de recursos.

Fuente: INCIBE (2017).

Fase 3. Identificación de las amenazas

Habiendo identificado los principales activos, el siguiente paso consiste en identificar las amenazas a las que estos están expuestos. Como se puede imaginar, el conjunto de amenazas es amplio y diverso, ya que pueden producirse por diferentes elementos tantos externos como internos de la organización, por lo que se debe realizar un exhaustivo esfuerzo en poder identificar todas las amenazas.

Siguiendo la terminología de la normativa ISO 31000, la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) responde a lo que se denomina *proceso de gestión de los riesgos* y lo implementa dentro de un marco de trabajo para que las organizaciones tomen las decisiones oportunas, teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. De forma ilustrativa, se muestra en la Figura 6 cómo se integra esta metodología dentro del proceso de gestión de riesgos.

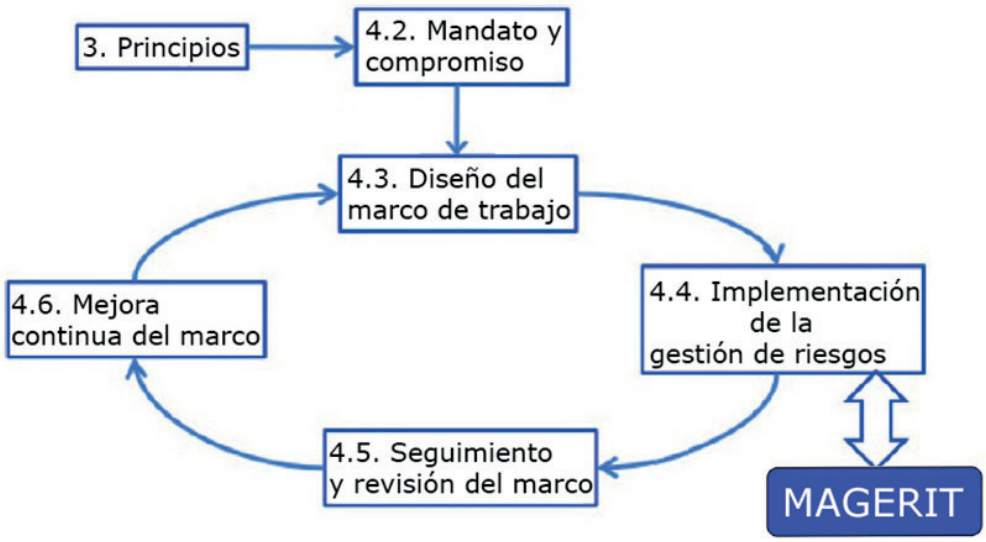

Figura 6. Relación de la metodología MAGERIT en un proceso de gestión de riesgos.

Fuente: adaptado de Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica (2012).

Fase 4. Identificación de las vulnerabilidades

Los recursos inventariados en la primera fase deben ser auditados para identificar sus puntos débiles o vulnerabilidades. Por ejemplo, una posible vulnerabilidad puede ser que los ordenadores no tengan instalados los últimos parches de seguridad o que cuenten con sistemas operativos desactualizados.

Fase 5. Evaluación del riesgo

Con toda la información obtenida hasta el momento, se establecerá la probabilidad de que una amenaza se materialice y el grado de impacto que produciría dentro de la organización. El cálculo de riesgo se puede realizar usando tanto criterios cuantitativos como cualitativos, tal como se aprecia en la Figura 7.

Cualitativo	Cuantitativo	Descripción
Baja	1	La amenaza se materializa a lo sumo una vez cada año.
Media	2	La amenaza se materializa a lo sumo una vez cada mes.
Alta	3	La amenaza se materializa a lo sumo una vez cada semana.

Figura 7. Clasificación cuantitativa y cualitativa de los riesgos.

Fuente: INCIBE (2017).

La elección del criterio cuantitativo o cualitativo definirá el cálculo del riesgo. Cabe destacar que ambos criterios no son excluyentes, sino complementarios. De tal forma que la combinación de ambos criterios aporta mayor valor a la hora de combatir y reducir los riesgos dentro de la organización.

Si hemos optado por hacer el análisis cuantitativo, calcularemos multiplicando los factores de probabilidad e impacto, como se refleja en la Figura 8.

PROBABILIDAD * IMPACTO = RIESGO

Figura 8. Cálculo del riesgo bajo el criterio cuantitativo.

Fuente: elaboración propia.

Si, por el contrario, se quiere optar por un análisis cualitativo del riesgo, se deberá elaborar una matriz de riesgo como la que se muestra en la Figura 9.

		IMPACTO		
		Bajo	Medio	Alto
PROBABILIDAD	Baja	Muy bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy alto

Figura 9. Matriz para clasificar el riesgo de forma cualitativa.

Fuente: INCIBE (2017).

Debemos poner en relación las vulnerabilidades detectadas en la anterior fase y relacionarla con esta matriz. Con ello, se podrá estimar la probabilidad y el impacto teniendo en cuenta las salvaguardas con las que cuenta la organización.

Fase 6. Gestión del riesgo

Para gestionar los riesgos seleccionados, existen cuatro estrategias:

- Transferir el riesgo a un tercero: por ejemplo, contratando un proveedor que tenga mejor capacidad técnica que nuestra organización para realizar un proceso, o bien contratando un seguro que cubra los daños a terceros ocasionados por fugas de información.

- Eliminar el riesgo: por ejemplo, eliminando un proceso o el recurso que está expuesto al riesgo.
- Asumir el riesgo: por motivos de negocio, por ejemplo, porque el coste es desproporcionado o el estado de la técnica aún no es estable, la organización puede asumir el riesgo; sin embargo, dicha decisión siempre deberá estar justificada.
- Mitigar el riesgo: aplicando medidas de seguridad que ayuden a reducir la consideración del riesgo.

En cualquier caso, a la hora de elegir una u otra opción la organización debe mantener el equilibrio entre el costo que tiene una actividad de control, la importancia del recurso y el nivel de criticidad del riesgo.

3. Ciberseguridad y protección de datos de carácter personal

A priori, el marco jurídico más cercano aplicable y afectado por la gestión de la información se compone por el conjunto de normas que regulan el uso y tratamiento de datos personales. Desde el 25 de mayo de 2018, se encuentra en vigor el Reglamento General de Protección de Datos (en adelante, RGPD), aprobado el 18 de abril de 2016, y, por otra parte, en España se encuentra en vigor desde el 5 de diciembre de 2018 y en España la Ley Orgánica de 3/2018 sobre Protección de Datos y Garantía de los Derechos Digitales (conocida también como LOPDGDD).

El art. 5.1.f del RGPD establece que los datos personales serán tratados de tal manera que se garanticen su confidencialidad y seguridad: Lo que implica que se deberán adoptar las medidas de seguridad necesarias acorde al tipo de datos, medios de tratamiento y el estado de la técnica, tal como recoge el art. 32 del RGPD. Es por ello por lo que existe tan estrecha relación entre gestión de datos personales y seguridad de la información, y por ello, la necesidad de aplicar procedimientos de gestión de riesgos para evaluar y definir las medidas más óptimas para garantizar un tratamiento de datos seguros conforme a lo visto en los apartados anteriores.

Por otra parte, en 2013, la Comisión Europea presentó una propuesta de directiva relativa a las medidas para garantizar un elevado nivel común de las redes y la información de seguridad en toda la Unión. En 2015, el Parlamento y el Consejo acordaron en el texto de la Directiva de Red y Seguridad de la Información (conocida como NIS por sus siglas).

Esta directiva tiene como objetivo la mejora de las capacidades de ciberseguridad en los Estados miembros de la Unión Europea; establece el vehículo jurídico para un ciberespacio más abierto, seguro y resiliente. Con ello, se pretende crear una Unión Europea más protegida, y desarrollar recursos tecnológicos e industriales de ciberseguridad e implementar un mercado interno de productos y servicios de ciberseguridad.

Todo ello generará un espacio donde se contará con una mayor colaboración entre los países y las empresas de la Unión Europea, lo que permitirá reducir el cibercrimen, evitar la fragmentación de planes nacionales de ciberseguridad e incrementar la armonización entre Estados miembros en la protección frente a incidentes NIS, riesgos y amenazas. Consecuentemente, se mejorará de forma considerable la protección al consumidor, el negocio y el gobierno en el ámbito de la Unión Europea.

Pero la preocupación legislativa de un tratamiento seguro de datos personales no solo es una cuestión europea. De hecho, en Canadá se promulgó La Ley de Protección de Información Personal y Documentos Electrónicos (también conocida como PIPEDA por sus siglas en inglés), que determina las reglas que cualquier organización debe seguir al recopilar información personal; entre ellas, se establece que se debe tratar de forma segura.

El mismo principio de seguridad se expande por las legislaciones de todo el mundo, como ocurre en normativas tan dispares geográficamente como es la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, Ley n.º 8968 de Costa Rica y la Privacy Act 1988 de Australia.

3. Conclusiones

La aparición de la COVID-19 cambiará nuestras vidas para siempre con nuevos estilos de trabajo, nuevos problemas de ciberseguridad, nuevas políticas propuestas, higiene personal, etc.

Todos los gobiernos del mundo han implantado y potenciado el distanciamiento social y los confinamientos (totales o parciales) como medidas preventivas claves para la propagación y contención de la COVID-19.

Gracias a la tecnología y a la hiperconexión con internet, cualquier persona puede continuar su vida profesional y privada de forma virtual. Sin embargo, con los enormes aumentos en el número de personas que trabajan de forma remota, es de vital importancia cuidar también *la higiene cibernética.*

Una incidencia de seguridad puede terminar en un ataque reputacional, en perdida de la continuidad de negocio, en un coste elevado para restaurar el sistema a un punto anterior, etc.; por todo ello, es imprescindible establecer y analizar los riesgos a los que se encuentra expuesta la organización.

Reducir los riesgos sobre la nueva gestión de la información en los nuevos contextos, como el teletrabajo, no es solo es problema y responsabilidad para la organización, sino un esfuerzo conjunto de todos, tanto de la organización como de los trabajadores y proveedores de tecnología. Porque tan solo con una visión y fuerzas conjuntas, se podrán plantear, diseñar y repensar nuevas medidas de gestión que reduzcan los riesgos cibernéticos y sus consecuencias.

Debido a ello, para mantener un nivel adecuado de seguridad informática en épocas de teletrabajo, se deberían seguir los siguientes consejos:

A) Recomendaciones para las organizaciones: cualquier empleador, bien sea una institución pública o bien sea una institución privada, deberá velar por implantar medidas de seguridad. Para ello, entre otras acciones, deberá:

- Realizar un análisis de riesgo detallado, así como el protocolo pertinente para efectuar análisis periódicos con el fin de detectar nuevas vulneraciones.
- Asegurarse una conexión segura entre el dispositivo del usuario y el sistema de información de la organización. Para ello, es recomendable contar con redes VPN (de sus siglas en inglés Virtual Private Network) corporativas que admitan una gran cantidad de conexiones simultáneas y con la finalidad de conectarse a uno o más ordenadores de una red privada utilizando Internet.
- Establecer un listado de aplicaciones y software autorizado por la organización, para evitar que el personal decida e instale soluciones informáticas que puedan comprometer la información corporativa. Además, es importante que el departamento de informática se encargue de realizar dichas instalaciones.
- Establecer sistemas de acceso con protocolos de identificación y autenticación con claves robustas (mezclando mayúsculas, minúsculas, números y símbolos) para acceder a los sistemas de información corporativos. Y, además, obligar su modificación de forma periódica.
- Proporcionar, cuando sea posible, ordenadores o dispositivos informáticos al personal que lo requiera, asegurándose de que tengan el sistema operativo y *software* de seguridad.
- En el caso de que no sea posible proporcionar dichos recursos, se deberá establecer políticas BYOD (concepto que deriva de sus siglas en inglés Bring Your Own Device) que regulen el uso de los dispositivos particulares de los empleados que se autorizan para un uso corporativo. En dicha política, se establecerá, entre otros aspectos, en qué condiciones se permiten su uso, cómo se accede a la información corporativa, qué configuraciones de seguridad serán necesarias para poder utilizarlos, etc.
- Formar al personal sobre principios básicos y fundamentales de seguridad de la información, así como establecer un programa de formación continua para reforzar e instruir a todo el personal ante los nuevos riesgos y amenazas que aparezcan.
- Definir una política para responder a incidentes y violaciones de seguridad.
- Asignar una dotación presupuestaria para reforzar la seguridad informática de la organización.

B) Recomendaciones para el personal para realizar sus funciones fuera de las dependencias de la organización: cualquier trabajador debe aplicar las medidas de seguridad idóneas o sustitutivas a las que aplica durante el desempeño de su trabajo

para garantizar la confidencialidad de la información que maneja. Para ello, entre otras acciones, deberá:

- Utilizar preferiblemente equipos informáticos corporativos, en vez de utilizar equipos personales, a menos que la organización haya establecido una política BYOD. Y, en la medida de lo posible, no mezclar en el mismo dispositivo el trabajo y las actividades de ocio.
- No compartir el dispositivo con el resto de personas que residan en el mismo domicilio.
- Conectarse a Internet a través de redes seguras, evitando las redes abiertas/libres, y mucho menos utilizar de forma fraudulenta redes wifi. Con una conexión insegura, las personas que se encuentren conectadas a la misma red pueden tener acceso al tráfico que se genera allí. Por ello, deberán activar un protocolo seguro o cifrado.
- Evitar el intercambio de información corporativa confidencial (por ejemplo, por correo electrónico) a través de conexiones posiblemente inseguras, como las redes wifi de cafeterías, vecinos del mismo edificio, etc.
- En la medida de lo posible, utilizar los recursos de la intranet corporativa para compartir archivos de trabajo. Por un lado, esto garantiza que los archivos de trabajo estén actualizados y, al mismo tiempo, se evita el intercambio de información confidencial entre dispositivos locales.
- Tener especial cuidado con la apertura de correos electrónicos, sobre todo, aquellos que hacen referencia a productos o comunicaciones referentes a la COVID-19, ya que pueden ser intentos de phishing o estafas. También, mantener especial atención a la dirección completa del emisor del correo electrónico y comprobar la identidad en aquellos casos en los que se requiera un pago o transferencia bancaria. En caso de duda sobre la legitimidad de un correo electrónico, comunicarlo al responsable de la organización.
- Tener el sistema operativo, antivirus y de las aplicaciones utilizadas actualizadas a la última versión disponible para reducir los fallos de seguridad y contar, en la medida de lo posible, con todos los parches de seguridad oportunos.
- Bloquear la pantalla al ausentarse del ordenador si se trabaja en un espacio compartido.
- No compartir las URL de las reuniones virtuales en las redes sociales u otros canales públicos para evitar que personas ajenas a la organización o terceros no autorizados pueden acceder a reuniones privadas.

C) Recomendaciones para los proveedores tecnológicos: cualquier proveedor de tecnología deberá implantar medidas proactivas para anticiparse y detectar los riesgos en una primera fase incipiente.

Bibliografía

Aguilera, P. (2011). *Redes seguras (Seguridad informática)*. Madrid, España: Editex.

Australian Government - Federal Register of Legislation. (n. d.). *Privacy Act 1988*. Recuperado de: https://www.legislation.gov.au/Series/C2004A03712

Cybersecurity Ventures (2020). *Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021*. Recuperado de: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Dewdney, A. (1989). Computer Recreations. *Scientific American, 260*(3), pp. 110-113. Recuperado de: http://www.jstor.org/stable/24987184

INCIBE (2017). *Clasificación cuantitativa y cualitativa de los riesgos*. [Figura]. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

INCIBE (2017). *Fases de un sistema de gestión de riesgos*. [Figura]. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

INCIBE (2017). *Matriz para clasificar el riesgo de forma cualitativa*. [Figura]. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

INCIBE (2017). *Modelo de inventario de recursos*. [Figura]. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

INCIBE (2019). ¡Fácil y sencillo! Análisis de riesgos en 6 pasos. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

INCIBE (2019). *Herramienta de Autodiagnóstico*. Recuperado de: https://adl.incibe.es/

Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales. Ley n.º 8968 Publicada en La Gaceta num. 170. San Jose 7 de julio de 2011.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado núm. 294. Madrid 6 de diciembre de 2018, páginas 119788 a 119857.

Observatorio Tecnológico (2012). *Pilares de la seguridad*. [Figura]. Recuperado de: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?showall=1

Observatorio Tecnológico (2019). *MONOGRÁFICO: Introducción a la seguridad informática*. Recuperado de: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?showall=1

Ramió Aguirre, J. (2006). *Libro electrónico de seguridad Informática y Criptografía*. Madrid, España: Universidad Politécnica de Madrid.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, publicado en el *Diario Oficial de la Unión Europea* núm. 119. Bruselas, 4 de mayo de 2016, pp. 1 a 88.

Personal Information Protection and Electronic Documents Act (2000). S.C. 2000, c. 5. Ontario, 13 de abril de 2000.

UNE (2017). ISO 27001. *Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.* Madrid, España: Aenor.

UNE (2017). ISO 27002. *Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información*. Madrid, España: Aenor.

Voutssas Marquez, J. (2010). Preservación documental digital y seguridad informática. *Investigación bibliotecológica 24*(50), pp.127-155.