GRADO EN COMERCIO

TRABAJO FIN DE GRADO

“CIBERSEGURIDAD PARA PYMES”

JAVIER DE LA ROSA PINEÑO

FACULTAD DE COMERCIO

VALLADOLID, JUNIO 2019

FACULTAD DE COMERCIO
Universidad de Valladolid

UNIVERSIDAD DE VALLADOLID
GRADO EN COMERCIO

CURSO ACADÉMICO 2018/19

TRABAJO FIN DE GRADO

“CIBERSEGURIDAD PARA PYMES”

Trabajo presentado por: Javier de la Rosa Pineño

Firma:

Tutor: Francisco Javier Galán Simón

Firma:

FACULTAD DE COMERCIO

Valladolid, 24 de junio de 2019

FACULTAD DE COMERCIO
Universidad de Valladolid

ÍNDICE

Listado de Figuras

1. Introducción

Al comenzar a elaborar este Trabajo Fin de Grado tenía en mente varios objetivos iniciales:

OBJETIVO1. Exponer las amenazas existentes al emplear equipos informáticos, haciendo especial énfasis en aquellos que se vinculan con el uso de internet.

OBJETIVO2. Elaborar una lista de medidas sencillas al alcance de cualquier persona que pueda necesitar de su aplicación para que se convierta en una herramienta útil para pymes preocupadas ante la posibilidad de sufrir un ataque.

OBJETIVO3. Descubrir que dentro de las pymes españolas existen numerosos apartados críticos dentro de la ciberseguridad con una gran capacidad de evolución debido a que las propias empresas se consideran poco o nada atractivas para los atacantes.

OBJETIVO4. Analizar las costumbres dentro de las empresas que provocan una sobreexposición de datos sensibles innecesariamente.

OBJETIVO5. Mostrar la realidad y el rearme que se ha producido en los últimos años en las empresas españolas, debido a la notoriedad que han adquirido ciertos ataques cibernéticos.

En el transcurso de su elaboración, y tras diversas conversaciones con el tutor académico, los objetivos que se han conseguido son los siguientes:

OBJETIVO I. Exponer el concepto de ciberseguridad de modo que sea comprensible para el gran público que, en general, no tiene conocimientos informáticos suficientes para comprender los aspectos claves relacionados con la seguridad en internet.

OBJETIVO II. Desgranar los distintos apartados que conforman las vulnerabilidades a las que nos enfrentamos en el mundo digital día a día.

OBJETIVO III. Mostrar las posibilidades y herramientas reales que tienen las empresas al alcance de su mano para responder a unos altos estándares de seguridad dentro de un entorno cambiante y siempre peligroso.

OBJETIVO IV. Desarrollar la explicación de varias herramientas de nivel medio-avanzado que pueden permitir un uso más seguro de las nuevas tecnologías empleadas en la gestión de nuestro negocio, siempre intentando que el coste adicional sea lo más reducido posible.

OBJETIVO V. Mencionar la existencia de un marco legal que obliga a tomar determinadas acciones para el bienestar de los usuarios y clientes.

OBJETIVO VI. Realizar una serie de entrevistas a empresas operativas con presencia en la web que conocen de primera mano los riesgos a los que están permanentemente expuestas y como defenderse de los mismos.

OBJETIVO VII. Concienciar de que la ciberseguridad tiene un gran interés para todas las empresas, independientemente de su tamaño.

La transformación digital unido a cambios migratorios, culturales y de consumo ha supuesto una gran oportunidad para las empresas de expandirse a nuevos horizontes independientemente de su tamaño. Hemos pasado de un consumo en los barrios con epicentro en las antiguas tiendas de ultramarinos a consumir productos mientras estamos sentados en el sofá de casa o mientras nos trasladamos a nuestro puesto de trabajo haciendo uso del transporte público. Faraónicos centros comerciales plagados de marcas conocidas inundan nuestras ciudades, y en caso de no disponer del producto que deseamos adquirir pueden ponerse en contacto inmediato con otra tienda de la misma marca situada en otra localización para satisfacer nuestra necesidad de compra.

Como puede apreciarse, se han producido (y están produciendo) enormes cambios que nos facilitan realizar múltiples tareas. Sin embargo, no todo es color de rosas, ya que la manera de interconectar estos sistemas obsesionados en la búsqueda de la máxima eficiencia es mediante redes cibernéticas.

Hace ya varias décadas que la introducción y rápida expansión de Internet en nuestras vidas nos permitió realizar tareas de forma rápida, eficiente y barata. No obstante, toda novedad acarrea unos riesgos, y, en el caso de Internet, éstos son que los expertos informáticos maliciosos hagan uso de su inteligencia para hacer el mal, lo que unido a nuestra nula precaución en acciones cotidianas en las que no conocemos el peligro pueden suponer robos de datos por valor de decenas de miles de euros.

Y volviendo a los datos, como he mencionado anteriormente, la forma de comprar de los consumidores ha cambiado muchísimo, por lo que es lógico pensar que la forma de vender de las empresas también se haya visto afectada. Por ello, debemos de echar

un vistazo a los datos, pues vivimos en la era de la información, la cual vale su peso en oro.

La necesidad de regular el acceso, almacenamiento y uso de la información viene precedida por una lista casi interminable de imprudencias y malas prácticas que nos fuerza a formarnos en el uso responsable de los sistemas informáticos que la contienen.

La única forma de dormir tranquilos cuando regentamos un negocio online pasa por seguir las recomendaciones en ciberseguridad de las agencias más prestigiosas del mundo, así como de empresas dedicadas a dicho negocio.

Sirviéndome de diversas fuentes de información, y con una metodología que consistía en leer para comprender tanto los conceptos como las implicaciones de aquello que estaba leyendo, he estructurado mi proyecto de la siguiente manera:

Para comenzar, se explica la realidad existente en el mundo cibernético en lo que respecta a la ciberseguridad. He querido plasmar los puntos críticos a los que se enfrentan las pymes en su día a día, donde son más vulnerables.

A continuación se indican los peligros consustanciales a la herramienta del correo electrónico, advirtiendo de los fraudes más comunes.

Después, nos hemos centrado en el almacenamiento seguro y trabajo en la nube, ya que suponen una revolución que nos abre todo un nuevo abanico de posibilidades de trabajo y nuevas posibilidades de gestionar los costes. Del mismo modo, supone una oportunidad de negocio enorme para empresas que suministren servicios de nube. Además es importante conocer los tipos de la información con los que la empresa trabaja, para dar un tratamiento distinto a cada uno de ellos, y una vez llegado el caso, conocer el método seguro para deshacernos de la propia información.

Posteriormente, se expone una serie de recomendaciones de seguridad adicionales con el objetivo de completar lo expuesto anteriormente, para que una pyme pueda blindarse de forma lo más eficaz posible, siempre con el horizonte de que una seguridad al 100 % nunca será posible.

Proseguimos con la cultura de ciberseguridad dentro de la empresa, ya que, aunque a menudo sea un apartado ignorado, la protección ha de comenzar por la parte más débil del “muro” que nos protege: los empleados, ya que el factor humano es, paradójicamente, el más vulnerable e importante al mismo tiempo dentro del mundo de las máquinas inteligentes.

Seguidamente, continuamos con otro apartado en el que el factor humano representa la oportunidad y el peligro, como es el BYOD (ver anexo), cuyo uso a lo largo y ancho del globo se ha extendido como una mancha de aceite difícil de parar y por mero desconocimiento muchas empresas y empleados están comprometiendo información confidencial de gran valor por no realizar un uso responsable de la tecnología.

Entonces se da paso a un apartado más técnico, como es el firewall, sistema de los más antiguos y al mismo tiempo de los más eficaces, que en sus versiones más actuales incorpora unas funcionalidades que lo convierten en objeto de deseo de los empresarios que desean gestionar la ciberseguridad de su negocio de forma más eficiente.

A posteriori, trato el control de accesos, ya que no sirve de nada un sistema robusto para proteger la información si con unas simples credenciales apuntadas en la propia mesa del ordenador puede acceder cualquiera que se encuentre en frente del dispositivo.

En relación con el apartado anterior, se explica la importancia de los permisos de los usuarios, ya que es necesario establecer una serie de requisitos para dotar de acceso a cada empleado a un área determinada de la empresa a través de los equipos informáticos de la misma.

Después nos centramos en un aspecto muy enrevesado y complicado: los motores de búsqueda, que son unos grandes desconocidos para el usuario medio de Internet; situación que no mejora para muchas pymes. A través de un uso inteligente de los mismos podemos lograr destacar entre las demás webs de la competencia cuando nos interese logrando llegar a más público. A su vez, un mal uso de los mismos nos puede ser muy perjudicial para nuestro posicionamiento en Internet.

Entonces, nos enfocamos en las fugas de información y otros riesgos relacionados. Quedan enfocados desde el punto de pérdida de información de las empresas que puede acabar en las manos equivocadas y cómo evitar que eso ocurra.

Para finalizar con la parte técnica, se tienen en cuenta los sellos de confianza. Se trata de una serie de certificados y sellos digitales que se emplean para aumentar la confianza en nuestros clientes potenciales mostrando de forma clara que somos una empresa rigurosa que se toma en serio el tratamiento de sus datos y que dispone de métodos de pago seguros.

Entrando en aspectos legales, se hace referencia al recientemente aprobado RGPD, que es la nueva normativa europea de protección de datos, obligatoria en todo el territorio de la Unión Europea. Y, lógicamente, también se hace referencia a la nueva LOPDGDD, normativa española basada en el RGPD, que concreta los requisitos legales dentro del territorio nacional.

Concluyendo mi aportación personal, se incluye una parte práctica que consta de cinco breves entrevistas a empresas españolas para conocer de forma sencilla las medidas que han implementado en el apartado de la ciberseguridad y sus prácticas diarias.

Para finalizar el trabajo, se incorpora una breve bibliografía, así como un sencillo diccionario con términos útiles para comprender mejor la parte más técnica de este trabajo.

2. Medidas de seguridad que debe tomar una pyme

Las empresas de mayor tamaño, volumen de negocio y más internacionalizadas fueron las primeras en concienciarse (debido a los ataques sufridos) sobre la importancia de protegerse de los peligros cibernéticos, mientras que las pymes necesitaron de más tiempo, en gran parte porque pensaron, en un primer momento, que carecían de atractivo para los hackers maliciosos. Hoy día sabemos que en torno al 50 % de los ataques se producen a pymes. (González, 2018).

Las grandes empresas pueden destinar enormes recursos a ciberseguridad mientras que las pymes tienen que hacer uso de herramientas personalizadas, mucho más sencillas y baratas pero muy efectivas y robustas.

Numerosos organismos públicos y privados hacen recomendaciones en la materia a la vez que nos aportan datos de interés:

- El Instituto Nacional de Ciberseguridad (INCIBE) hace hincapié en la necesidad de tener un buen protocolo que todos sepan ejecutar.
- Sophos se centra en vigilar los controles de acceso, permisos de usuario, red de la empresa, puertos abiertos y las conexiones y recursos compartidos. Por último, desaconseja descargar archivos de web no seguras.
- Kaspersky se centra en el phishing y en evitar pendrives y discos duros de origen desconocido.
- Randed explica que el coste medio para una empresa de un ataque cibernético exitoso es de 35.000 €, cantidad inasumible para muchas pymes, dato que explica que el 60 % de las empresas no consigan recuperarse después de sufrir un ataque digital.
- Con datos recogidos del Centro Criptológico Nacional (CCN), en 2017 se produjeron en España más de 25.000 incidencias.

Debemos ser conscientes de que los ciberatacantes emplean vulnerabilidades de nuestra propia red, porque debemos garantizar su seguridad por encima de todo. Programas anti-malware y completos antivirus con firewall resultan fundamentales para dificultar la ilícita labor.

De este modo, interesa que los empleados no sean desconocedores de las ciencias informáticas y sus peligros, pues gran parte del riesgo existirá debido a negligencias cometidas por ellos mismos.

La amenaza de los malware guarda una gran relación con el apartado anterior. Se trata de programas disponibles en internet que son en apariencia legítimos. Sin embargo, esconden un gran peligro, puesto que crean una "puerta trasera" en nuestro equipo que será utilizada por alguna persona con fines ilícitos para acceder a la información recogida en el ordenador. Para prevenirlos debemos de evitar su instalación, pero existen empleados no concienciados con ello que acaban pagando muy caro su temeridad.

Es necesario que los negocios se tomen muy en serio estas recomendaciones, de forma especial aquellos que operen con información económica y estratégica, que deben de llevar a cabo una encriptación segura, especialmente en los datos más sensibles. Depositar nuestra confianza en aquellas plataformas que se han labrado una buena reputación por medio de sus buenas prácticas ayudará a enviar el mensaje al resto de que están fuera del mercado si no se lo toman en serio y repercutirá en mejores servicios globales de ciberseguridad.

2.1. El correo electrónico

El correo electrónico forma parte del día a día de las empresas por ser la mejor alternativa para múltiples usos. Siendo tan útil se ha convertido en un recurso para aquellos que se dedican al fraude y a los ataques informáticos.

Existen diferentes fraudes mediante el correo electrónico que deberíamos conocer y sobre los que deberíamos enseñar a nuestros empleados:

2.1.1. Phishing

Consiste en la suplantación de identidad a través del correo electrónico para obtener datos (generalmente bancarios) de la víctima.

Las medidas de prevención que debemos llevar a cabo son:

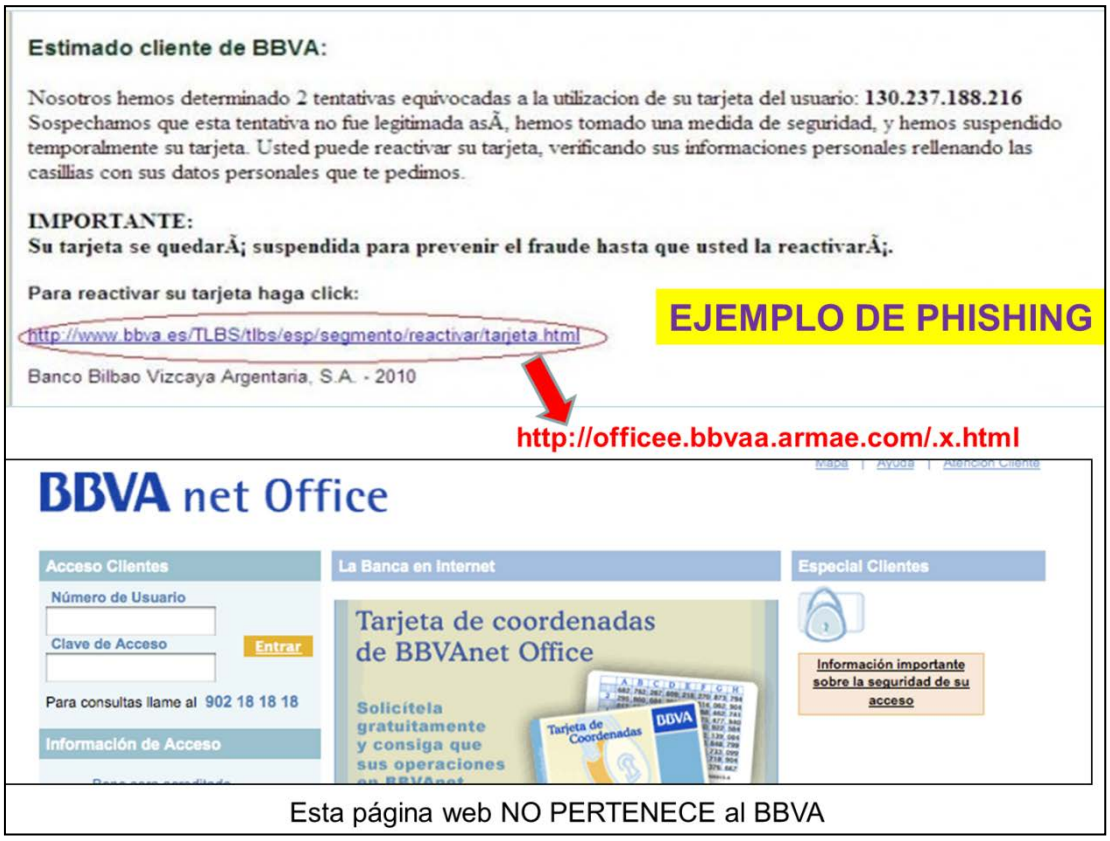
MEDIDA1. Verificar las URL en las que estemos operando.

MEDIDA2. Recelar de correos electrónicos procedentes de bancos que soliciten el envío de información personal.

MEDIDA3. Verificar las URL a las que nos redireccionen los enlaces contenidos en los emails.

MEDIDA4. Ignorar aquellos correos electrónicos (o incluso SMS) sospechosos que nos pidan datos personales.

Figura 1. Ejemplo de phishing



Fuente: Elaboración propia

2.1.2. Scam

Consiste en hacer creer a la víctima que ha sido ganadora de algún premio, concurso o herencia con el fin de cobrarle una tasa para desbloquear el pago. También se puede emplear para sustraer información confidencial.

2.1.3. Malware

Correos electrónicos que adjuntan algún tipo de archivo malicioso que se introduce en el ordenador y lo infecta. Es fácil enviarlos masivamente y que algún trabajador de la empresa caiga en la trampa.

Las medidas de prevención consisten en formar adecuadamente a los empleados y emplear un buen antimalware.

2.1.4. Spam

Se basa en el envío masivo de correo electrónico con fines publicitarios o fraudulentos, generalmente por parte de usuarios no conocidos.

Por suerte, actualmente existen filtros antispam muy sofisticados que nos evitan la incomodidad de eliminarlo por nosotros mismos.

2.1.5. Fake

Se trata de la difusión masiva de noticias falsas a través de correo electrónico, WhatsApp o Telegram principalmente. Suelen venir acompañados de enlaces potencialmente peligrosos.

En conclusión, para estar convenientemente protegido es vital contar con un equipo humano bien entrenado en ciberseguridad y comprometido con la causa, así como con antivirus y anti-malware de calidad.

2.1.6. Correo electrónico desechable

En numerosas ocasiones en las que naveguemos por Internet comprobaremos que muchas webs nos pedirán que introduzcamos nuestro correo electrónico para hacer uso de alguno de sus servicios. Eventualmente, veremos que nuestro email se llena de publicidad no deseada que, generalmente, acaba en la bandeja de spam. Sin embargo, en ocasiones, el filtro anti-spam falla.

En el caso de las empresas, aprendemos enseguida que “tiempo es dinero” y no nos podemos permitir una laboriosa gestión manual de mensajes no deseados en el correo electrónico.

Por suerte, existen las cuentas de correo temporales, las cuales son generadas en cuestión de segundos y de forma gratuita por programas de la red. Según Alemán (2017), estas cuentas serán destruidas automáticamente después de cierto tiempo o cuando se realice una acción determinada (por ejemplo, cerrar la pestaña en la que esté abierta).

Su utilidad para nosotros como empresa es muy interesante, pues nos permite:

VENTAJA1. Esquivar a los hackers maliciosos que traten de hacerse con nuestros datos.

VENTAJA2. Registrarnos en una red WiFi pública que pida nuestra cuenta de correo.

VENTAJA3. Esquivar bases de datos de correo electrónico.

VENTAJA4. Obtener algún tipo de beneficio en un determinado sitio web al registrar nuestro email, eliminando la molestia de recibir correos publicitarios indiscriminadamente.

VENTAJA5. Hacer pruebas con numerosos correos electrónicos en nuestra nueva web antes de lanzarla definitivamente al público.

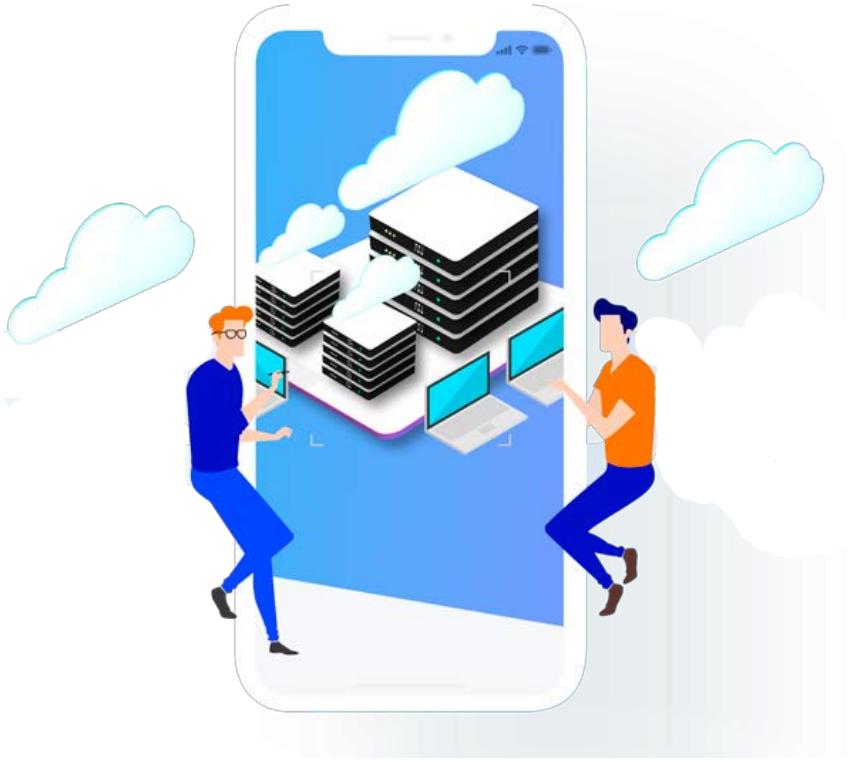
VENTAJA6. Posibilidad de enviar un email totalmente anónimo.

Existen múltiples plataformas que nos permiten crear cuentas de correo temporal o desechable, como 10minutemail, nowmymal, guerrillamail y yopmail entre otras. En caso de requerir de alguna plataforma específica por su funcionalidad no nos será ardua tarea el encontrarla con varias búsquedas en la barra de búsqueda de nuestro buscador habitual.

2.2. Almacenamiento seguro y trabajo en la nube

Los servicios de almacenamiento en la nube se han vuelto muy populares desde hace unos años, especialmente para las empresas. Las ventajas que éstos ofrecen son importantes -acceso a la información desde cualquier parte que tenga conexión a Internet, menor necesidad de recursos propios de la empresa para el almacenamiento, etc.- pero existen riesgos que merecen ser considerados, especialmente el de tener la información de la empresa custodiada por un tercero.

Figura 2. Computación en la nube



Fuente: Imágenes de Google

Para aquellos que decidan incorporar este tipo de servicios a su empresa es necesario desarrollar una política de almacenamiento en la nube, la cual ha de guiarse por los siguientes apartados:

2.2.1. Contrato a Nivel de Servicio (SLA)

Un "Service Level Agreement" es un contrato entre la empresa que presta el servicio de almacenamiento y su cliente. Se trata de un pacto que fija el tipo de servicio contratado y la calidad del mismo, así como las compensaciones a percibir en caso de que no cumplir el contrato.

2.2.2. Elección del tipo de servicio

Existen diferentes alternativas en el mercado en base a diversos aspectos: servicio gratuito y servicio Premium.

Podemos optar por un servicio gratuito que normalmente es muy limitado en cuanto a herramientas que nos faciliten administrar nuestra información y en cuanto al almacenamiento máximo disponible.

Sin embargo, existe la posibilidad de mejorar el servicio aportando una cantidad de dinero, por lo que lograremos un servicio Premium, más completo, que además nos suele permitir un Contrato a nivel de Servicio o Service Level Agreement (SLA).

2.2.3. Disponibilidad y trazabilidad

Resulta fundamental estudiar detenidamente las diferentes alternativas ofrecidas en el mercado, pues dependiendo del tipo de información que vayamos a almacenar nos puede ser más conveniente una opción u otra. Si necesitamos almacenar datos con los que trabajamos a diario que requieran de disponibilidad inmediata, es necesario asegurarnos de que escogemos una empresa que no tenga patrones en sus servidores, pues en caso contrario podría paralizar nuestra producción. Si por el contrario, vamos a almacenar copias de seguridad, esta característica no sería (a priori) tan importante.

En cuanto a la trazabilidad, resulta una gran ventaja poder conocer los accesos de cada usuario a los datos almacenados, así como herramientas que nos permitan conocer la evolución y cambios de un archivo a lo largo del tiempo.

2.2.4. Copias de seguridad y requisitos legales

Dependiendo de nuestras necesidades puede ser muy interesante emplear este tipo de servicios para el almacenamiento de copias de seguridad, por lo que nos resulta atractivo conocer el tipo de políticas y protocolos de seguridad que tienen al respecto.

En referencia a los requisitos legales es primordial conocer que dependiendo de la ubicación de un archivo se aplicará una u otra legislación. La legislación aplicable es una u otra dependiendo del país de origen de los datos. Para información de empresas españolas hemos de contratar un servicio que opere en Europa aplicando la ley vigente.

2.2.5. ¿Qué tipo de información almacenar y cómo administrarla?

El primer paso es realizar un protocolo de gestión de datos que nos permita clasificar la información en función de su confidencialidad para la empresa. Esta clasificación ha de hacerse teniendo en cuenta los efectos que podría tener para la empresa que alguien accediese a la información de forma no consentida. Distinguimos tres tipos de información atendiendo a su nivel de confidencialidad:

INFO1. Confidencial: aquella información a la que tendrá acceso la junta directiva así como algunos empleados involucrados en determinadas tareas.

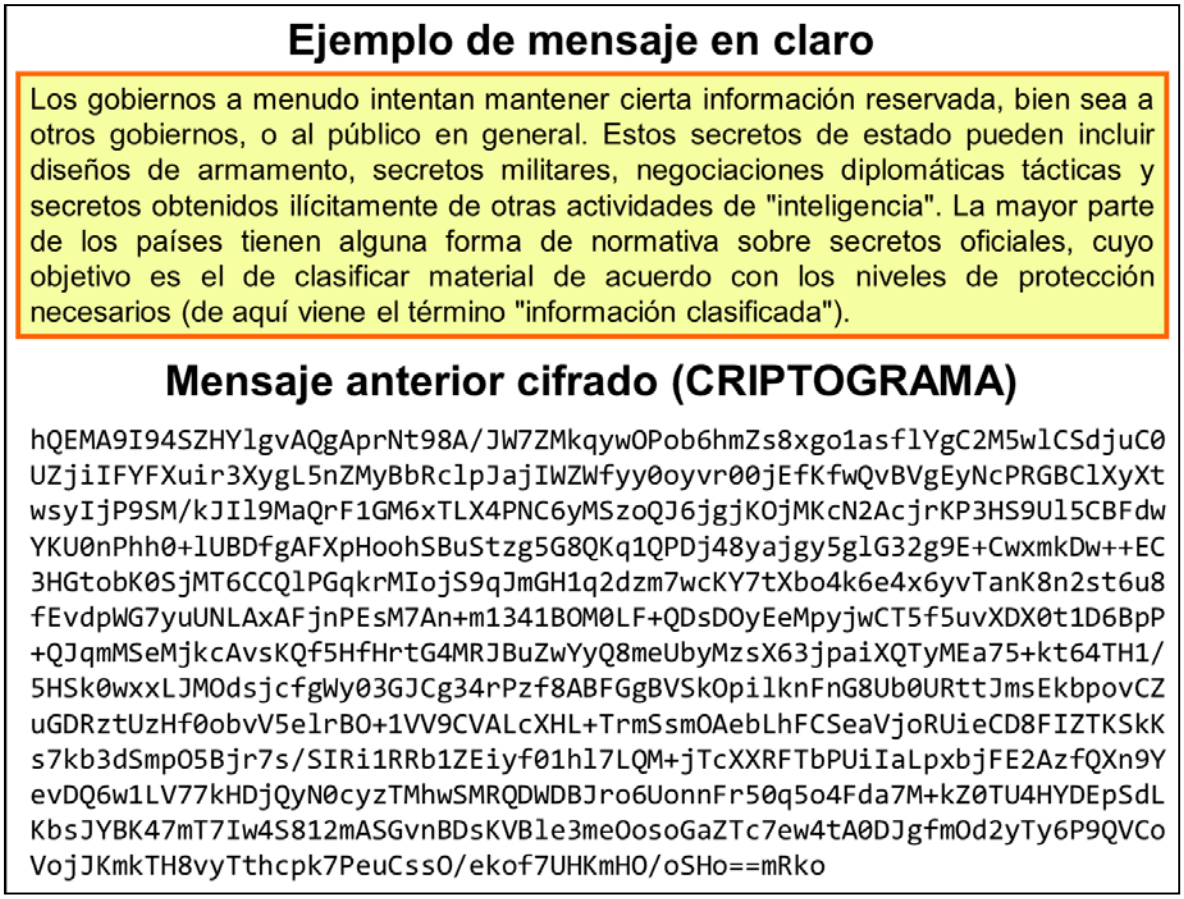
INFO2. Interna: aquella información que estará disponible para los empleados de la empresa. Incluyen protocolos y procedimientos a seguir en caso de que se den determinadas circunstancias.

INFO3. Pública: se trata de información que la empresa comparte abiertamente.

2.2.6. Cifrado y borrado seguro

Al completar la clasificación de la información en las distintas categorías del apartado anterior hemos de proceder a decidir si han de subirse a la nube o no los datos enmarcados en cada categoría y con qué medidas de seguridad.

Figura 3. Ejemplo de mensaje cifrado



Fuente: Elaboración propia

Las medidas de seguridad que se aconsejan basándose en la clasificación del apartado anterior son las siguientes:

SEG 1. Confidencial: se recomienda evitar subir esta información a la nube, pues supone correr un riesgo innecesario. Es aconsejable que la organización guarde estos archivos en sus propios servidores.

SEG 2. Interna: ha de asegurarse un sistema de credenciales para que únicamente tengan acceso aquellas personas autorizadas. Además, previendo posibles fallos han de cifrarse los archivos para mayor seguridad en caso de que alguien no autorizado consiga hacerse con los archivos.

SEG 3. Pública: no es necesario tomar medidas de seguridad adicionales, ni siquiera el cifrado para la información pública.

Es vital para la empresa establecer mecanismos para el borrado seguro para que en caso de querer eliminar un archivo de la nube (porque ya no es necesario, presenta

algún error o cualquier otro motivo) que la compañía de la nube asegure mediante SLA que el archivo será irrecuperable.

2.3. Recomendaciones de seguridad adicionales. La Criptografía

Cuando trabajamos con servicio de almacenamiento en la nube el mayor riesgo al que estamos expuestos son los accesos no autorizados. A fin de dificultar un incidente hemos de tomar las siguientes medidas:

- Establecimiento de credenciales de acceso seguras.
- Activar la autenticación de doble factor.
- Tener el software actualizado a la última versión disponible.
- Emplear un potente antivirus (que además realice escaneos de seguridad) y tener activo el cortafuegos.
- No fiarse de correos electrónicos sospechosos evitando descargar sus archivos adjuntos y clicar en los link que incluyan.
- Priorizar el uso de datos móviles a una red WIFI pública, empleando, en caso de necesidad una red VPN para garantizar la privacidad de la conexión.

A la hora de trabajar en la nube encontramos un entorno en desarrollo y con muchas ventajas que nos podrían ser de gran utilidad:

V1. Se trata de un mercado con mucha competencia en el que hay múltiples empresas luchando por ofrecer el mejor servicio posible. De este modo, se añaden nuevas funcionalidades y mejoran la seguridad continuamente, todo ello con precios muy asequibles.

V2. Según se indica en Zinko Colombia (2019), aumenta la flexibilidad en el trabajo, ya que ofrece trabajar simultáneamente a varias personas en un mismo archivo, por lo que se produce un incremento en la productividad y supone una integración para aquellas personas que trabajan de forma remota.

V3. En caso de incendio, robo o ataque a los equipos de la empresa, la información que esté guardada en la nube se mantendrá a salvo. Tan solo serán necesarias las credenciales de acceso para acceder a ella desde un dispositivo con conexión a Internet compatible.

V4. Se puede acceder a los archivos desde múltiples dispositivos (ordenadores, tablets, móviles, etc.).

V5. El acceso es prácticamente inmediato y desde cualquier parte del mundo, ya que lo único que se requiere es de conexión a Internet en un dispositivo compatible.

V6. No es necesario destinar recursos a mantener actualizados los programas con los que trabajemos directamente en la nube, pues la propia plataforma se encarga de que los utilicemos en la última versión disponible.

Por otro lado, existen una serie de inconvenientes asociados al trabajo en la nube:

I1. Es necesario estar conectado a la red para poder trabajar. Además, la conexión a Internet ha de ser continua y de muy buena calidad, o nos será imposible extraer el máximo rendimiento del sistema.

I2. Posibles agujeros de seguridad en el sistema de la empresa. Por ello se antoja imprescindible elegir cautelosamente a la empresa que nos preste el servicio.

Trabajamos diariamente en nuestra empresa con distintos tipos de información. Mientras que varios tipos no son de especial relevancia existen otros que han de ser mantenidos confidenciales. La criptografía está a nuestro servicio pues es capaz de hacer que un archivo se vea ilegible a no ser que se cuente con la clave de descifrado. Este tipo de técnicas son de gran ayuda a la hora de almacenar y compartir archivos cuya privacidad es cuestión fundamental para la empresa, y es que nadie confiaría en una empresa con fama de tener fugas de información. Para realizar la criptografía correctamente y completarla con otras medidas de seguridad extra, hemos de seguir las siguientes medidas:

SEG1. Identificar la información susceptible de ser cifrada. No toda la información es confidencial, por lo que no existe la necesidad de cifrar cada archivo. Aquella información sensible que maneje la empresa deberá ser convenientemente cifrada y almacenada en dispositivos extraíbles, los servidores correspondientes o en la nube.

SEG2. Uso de la firma electrónica. Se trata de un método seguro y de obligado uso para diversas gestiones, principalmente relacionadas con la Administración.

SEG3. Certificados web. Sirven como garantía de seguridad. En nuestras web si vamos a realizar trámites o ventas online necesitaremos certificado electrónico.

SEG4. Cifrado. Siempre que vayamos a realizar backups (copias de seguridad) o a trabajar con empresas externas (como las que proveen del servicio de

almacenamiento de la nube), será necesario cifrar aquellos datos más confidenciales e importantes para la empresa.

SEG5. Seguridad en las apps. Cualquier aplicación que funcione introduciendo credenciales para acceder a una cuenta privada ha de cifrar los datos de los usuarios.

SEG6. Seguridad en conexiones VPN. Si fuera necesario realizar conexiones en las que se cuente con accesos externos autorizados será necesario emplear una red VPN para asegurar la privacidad de las comunicaciones.

SEG7. Tipos de cifrado. Por su seguridad superior hemos de emplear algoritmos de cifrado asimétrico de eficacia probada. Además, hemos de tener en cuenta que las nuevas técnicas criptográficas garantizan una mayor seguridad que las que emplean aquellos algoritmos que han quedado anticuados.

SEG8. Aplicaciones para criptografía. Han de definirse aquellas aplicaciones que se emplearán para el cifrado de datos, así como detallar los pasos para utilizarlas correctamente. Además, hemos de formar a los empleados en su uso.

SEG9. Seguridad WIFI. Debemos cambiar la contraseña del WIFI por defecto, así como utilizar el último protocolo disponible: WPA3 con algoritmo de cifrado AES.

2.4. Cultura de ciberseguridad en la empresa

La ciberseguridad dentro de una empresa sigue el modelo de una cadena: popularmente conocemos la frase de que “una cadena se rompe por su eslabón más débil”, y en el caso de la ciberseguridad sabemos que ese eslabón son los empleados.

Resulta muy sencillo y asequible proveerse de buenos equipos informáticos que incorporen robustos sistemas de ciberseguridad, pero a la hora de la verdad es el empleado quien ha de gestionarlos, por lo que si este no está concienciado con su importancia dentro de esta cadena o, simplemente carece de la formación específica, nuestros esfuerzos no habrán servido de nada.

Si bien es cierto que el empleado es el eslabón más débil de nuestra cadena, también es el más importante. Conseguir que el trabajador esté plenamente implicado con la ciberseguridad de la empresa y adapte sus labores diarias a cumplir unos estándares supondrá todo un reto, pero merecerá la pena el esfuerzo.

2.4.1. Establecer cultura de ciberseguridad en la empresa

Dentro de cualquier organización los empleados tienen sus rutinas y metodologías de trabajo, por lo que no ha de sorprendernos que al introducirles nuevas directrices, estos recelen de nosotros viendo nuestras indicaciones como un estorbo inservible a su labor. Aquí es donde cada empresa ha de desmarcarse llevando a cabo diferentes acciones:

ACCIÓN1. Formación a los empleados. En el mundo de la empresa real, los cursos de formación a empleados en materia de ciberseguridad suelen ser simples charlas en las que se mezclan a todos los trabajadores de las diferentes divisiones de una empresa a las que apenas se da importancia consiguiendo una nula implicación por parte de los mismos. La primera acción para desmarcarnos será la de proporcionar un aprendizaje personalizado a cada grupo de empleados dependiendo de su labor en la empresa. Esta formación ha de ser continua, con cursos periódicos de reciclaje, especialmente al personal técnico encargado del área de informática, a los cuales habrá que proporcionar recursos suficientes para dotar a la empresa de un sistema de ciberseguridad óptimo.

ACCIÓN2. Establecer políticas y protocolos de actuación en materia de ciberseguridad. Dentro de cada empresa deberá haber definidos una serie de documentos que se encarguen de detallar paso a paso cada acción a tomar ante cada situación que se pueda dar en la empresa de manera ordinaria (protocolo de formación ante una nueva contratación) o en caso de sufrir una incidencia (ataque de ciberseguridad). Se deberán de organizar en distintos niveles de lo más amplio a lo más concreto (políticas, normas, procedimientos, etc.).

ACCIÓN3. Supervisión. Es necesario que haya un encargado que será el máximo responsable de ciberseguridad dentro de la compañía. Este empleado deberá de contar con el pertinente apoyo de soportes informáticos para ejercer su labor. Tendrá que hacer uso de las normas escritas y explicadas a los empleados para garantizar que no se lleven a cabo acciones prohibidas dentro de la empresa empleando sus recursos corporativos.

ACCIÓN4. Concienciación. Para asegurar el éxito de las nuevas políticas será necesario lograr que todos y cada uno de los empleados se autoperciban como parte fundamental dentro de la ciberseguridad de la empresa. Para lograrlo han de llevarse a cabo diversas acciones que incluyen tanto el correcto tratamiento

de información (mesas limpias, posibles escenarios de fugas de datos, etc.) como el uso responsable de los recursos informáticos, redes y bases de datos (conexiones WIFI no seguras, uso de memorias de almacenamiento externo, uso seguro del correo electrónico, etc.).

2.4.2. La ciberseguridad en los distintos sectores empresariales

La ciberseguridad es un aspecto a tener en cuenta por todas las empresa y no únicamente con el fin de garantizar su actividad comercial, ya que incluye muchos otros aspectos como pueden ser la confianza y seguridad de las personas que establezcan algún tipo de relación con las mismas.

Dependiendo del sector económico en el que se encuadre cada empresa necesitará hacer hincapié en ciertos aspectos por ser en los que se muestra más vulnerable.

Podemos identificar diferentes sectores y las amenazas más comunes a las que se enfrentan:

TIPO1. *Sector industrial*. Es especialmente severo el riesgo al que se enfrentan las empresas de este sector en lo referido al espionaje industrial y al robo de datos sobre la base de clientes.

TIPO2. *Sector de la construcción*. El principal peligro reside en el robo de documentación, incluyendo documentos legales y planos de obra.

TIPO3. *Sector de la salud*. Se trata de una parcela especialmente sensible, pues en muchos casos los diagnósticos y tratamientos médicos de los pacientes están sujetos a cláusulas de estricta confidencialidad. El mayor problema es, pues, el robo de datos de los pacientes, lo cual puede llegar a acarrear consecuencias muy graves para la compañía.

TIPO4. *Empresas de distribución o venta mayorista*. El principal riesgo está en los datos almacenados de base de los clientes, los cuales pueden conducir a fraudes complejos. Se puede llegar a poner en riesgo la seguridad de envío de mercancías por la vulnerabilidad de los sistemas de seguimiento de pedidos.

TIPO5. *Empresas de distribución o venta minorista*. En este caso cabe reseñar que para cuadrar las cuentas anuales el negocio con proveedores es vital, por lo que también se convierte en su mayor vulnerabilidad en caso de que se logre acceder a las bases de datos con información sobre los mismos o sobre los

contratos que mantienen entre las distintas compañías. No solo se incurriría en problemas legales por no haber custodiado datos confidenciales debidamente, sino que se podría perder un gran poder de negociación con otros proveedores pues estos podrían acceder de forma ilícita a las condiciones de los contratos de la empresa con otras compañías aprovisionadoras.

TIPO6. *Sector de ocio y tiempo libre*. Los mayores problemas asociados a estos tipos de negocios residen en la estricta relación de confidencialidad existente entre muchos consumidores de estos tipos de negocios y las compañías cuyos servicios contratan. De este modo es vital proteger la base de datos de clientes y los sistemas de pago, pues muchos de los desembolsos del sector se realizan de manera electrónica.

TIPO7. *Sector logístico*. Se trata, posiblemente, del sector que más está evolucionando en los últimos años gracias a inversiones millonarias por parte de gigantes como Amazon o Alibaba. El mayor problema es que al ser un sector tan intensivo en tecnología e inteligencia artificial, el robo de código podría suponer pérdidas de valor incalculable. Sin hacer de menos el valor de las bases de datos de clientes, su propia tecnología es donde han de centrarse los mayores esfuerzos por la ciberseguridad.

TIPO8. *Sector educativo*. Se trata de un sector con especial peligro, máxime si hablamos de alumnado menor de edad. Los datos personales de cada estudiante han de ser cautelosamente protegidos a la vez que se garantice la seguridad de las aplicaciones y la intranet del centro.

TIPO9. *Asociaciones y servicios profesionales*. Son especialmente vulnerables en todo lo referido a propiedad intelectual y los datos de clientes, afiliados o colaboradores que puedan almacenar en sus servidores.

Uno de los mayores retos de la ciberseguridad es concienciar de su importancia a todos, ya que en muchas empresas por desconocimiento de la realidad mantienen la creencia de que los datos que manejan carecen de valor para terceros.

La verdad es que la información es una herramienta muy valiosa que puede ser nuestra mejor aliada o nuestra peor enemiga. No es un secreto que las empresas más grandes del mundo como Facebook o Google obtienen grandes ganancias vendiendo información a otras empresas. Sin embargo, hay empresas que pueden acceder a todo tipo de información de forma ilícita aprovechando vulnerabilidades en nuestro sistema.

Según la Agencia de Ciberseguridad Estadounidense (National Cyber Security Centre –NSNC-, 2018), las principales precauciones que debe tomar una empresa en lo referido a la ciberseguridad son:

PREC 1. *La gestión de los riesgos.* Definir de forma clara y precisa los roles que desempeñarán los responsables de cada área y apartado sobre ciberseguridad, así como qué miembros de la organización tendrán responsabilidades al respecto.

PREC 2. *Software actualizado*. Mantener los equipos en buen estado con el software actualizado a la última versión disponible.

PREC 3. *Red protegida*. Es necesario que la red de la empresa esté firmemente protegida en todo momento, extendiendo la protección a amenazas internas y externas.

PREC 4. *La importancia del malware*. Resulta fundamental contar con un paquete completo, funcional y actualizado que mantenga un control diario sobre la seguridad. De esta forma se darán respuestas más rápidas, precisas y eficaces a los problemas que vayan surgiendo día a día.

PREC 5. *Privilegios de usuario*. Es necesario que un administrador dote a la empresa de un sistema de credenciales personales para los empleados (nombre de usuario y contraseña). Cada usuario del sistema tendrá unos privilegios de acceso acordes a su rol dentro de la compañía y del propio sistema informático de la misma.

PREC 6. *Control de dispositivos extraíbles*. Se recomienda que el propio administrador del sistema sea quien suministre cualquier tipo de dispositivo de almacenamiento externo que vaya a ser conectado al equipo. También son deseables escaneos periódicos de seguridad.

PREC 7. *Monitorización de redes y servicios*. Uso de herramientas encargadas de la monitorización y análisis de protocolo. Si la empresa fuera de un tamaño mayor sería necesario emplear otras herramientas comerciales como el análisis de tráfico o el uso de IP.

PREC 8. *Sensibilizar a los usuarios*. La ciberseguridad de una empresa depende de que todos los empleados pongan de su parte. Este puede ser uno de los mayores retos a la hora de implantar un protocolo, por lo que es importante hacerlos partícipes.

PREC 9. *¿Qué hacer con los dispositivos móviles de los empleados?* En el caso de los teléfonos de empresa es aconsejable para la compañía obligar a los empleados a tener instalados cierto software que los proteja de posibles amenazas, posibilitando también la localización y borrado remoto.

PREC 10. *El negocio debe seguir pese a los incidentes*. Cuando un negocio se enfrente a un ataque, ha de poner en marcha el protocolo de actuación y seguir operando lo más rápidamente posible.

2.5. Bondades y Riesgos del BYOD

Gracias a los avances tecnológicos se han producido mejoras bestiales en los dispositivos informáticos y sus redes de conexión. El cambio no solo los ha hecho más baratos, sino también mucho mejores, produciendo dispositivos extremadamente potentes, funcionales y ligeros.

Por estos motivos, los dispositivos con los que contamos en casa no tienen nada que envidiar a aquellos de un centro de trabajo, lo que ha dado lugar a un método conocido como BYOD (Bring Your Own Device o Lleva Tu Propio Dispositivo), en el que los profesionales trasladan a diario sus herramientas de trabajo de casa a la oficina y viceversa.

Figura 4. BYOD. Trabaja con tus dispositivos particulares

Fuente: Imágenes de Google

Este método de trabajo cuenta con la ventaja de reducir costes materiales a la empresa y la posibilidad de que el empleado se mantenga conectado (trabajando) desde otro lugar para poder realizar su jornada laboral habitual.

Sin embargo, surgen también desventajas que han de ser analizadas:

DESV1. Robo, pérdida o menoscabo del dispositivo, el cual es ligero, manejable y fácil de colocar en el mercado negro.

DESV2. Equipos vulnerables. En muchos casos no están convenientemente actualizados por lo que son vulnerables a ataques. A mayores han podido sufrir cambios de software (root o jailbreak) por lo que las vulnerabilidades aumentan. Además, abundan las Apps de fuentes no seguras.

DESV3. Red WIFI no segura. Las redes WIFI públicas añaden peligrosidad a esta práctica, puesto que cualquiera con ciertos conocimientos podría acceder a nuestros datos sin demasiada dificultad. El uso de VPN es obligatorio si no confiamos al 100% en la conexión.

DESV4. Ausencia de cifrado. Es raro que un equipo informático esté protegido por un cifrado robusto, pero aún más raro es que esta protección se amplíe a memorias extraíbles.

DESV5. Escasa o nula seguridad de acceso. Es imprescindible incluir comprobaciones robustas de seguridad, o incluso de doble factor para acceder a los dispositivos.

DESV6. Uso irresponsable/desleal del dispositivo. Hay que entender que nadie que no sea el dueño del mismo debería acceder al aparato por entrañar riesgo para la empresa. De este modo prestárselo a alguien sería un grave error. Del mismo modo, un ex-empleado de la empresa podría dañar a la misma con la filtración o venta de información confidencial.

Existen entonces recomendaciones adicionales de seguridad para aplicar en el caso de emplear el sistema BYOD:

RECOM1. Implantar una normativa clara, conocida y respetada que todos conozcan.

RECOM2. Establecer cifrado efectivo de los dispositivos, que estarán listados y disponibles para localización y borrado remotos.

RECOM3. Mantener el software actualizado y sin establecer cambios de permisos (root o jailbreak).

RECOM4. La única manera de conectarse a WIFI abierto será mediante VPN.

RECOM5. Se potenciarán y priorizarán las redes móviles de alta velocidad fuera del espacio de trabajo.

RECOM6. Instalar contraseñas y/o mecanismos de control biométricos en todos los dispositivos. Además será muy recomendable la configuración del bloqueo automático de los dispositivos tan un tiempo prudencial de inactividad.

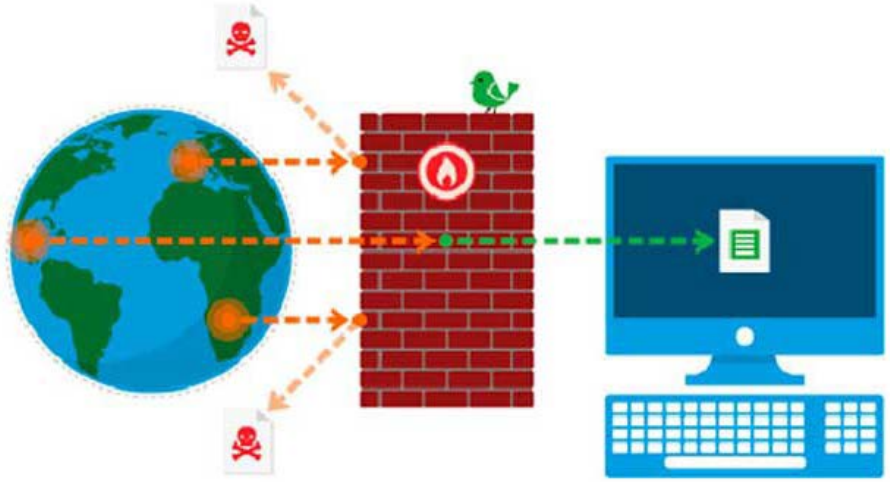
RECOM7. No se prestará en ningún caso el dispositivo informático a terceros.

2.6. Firewall

Un firewall es un filtro que controla las comunicaciones entre redes y autoriza o deniega el paso en función de cómo lo hayamos ajustado.

Con el paso de los años, el firewall ha ido evolucionando hacia una herramienta de mayor funcionalidad, mucho más completa que el firewall primitivo. Bajo las siglas de UTM (Unified Threat Management, por sus siglas originales en inglés, o Gestión Unificada de Amenazas, por su traducción al castellano) se agrupan una serie de herramientas necesarias para toda empresa u organización y muy recomendables para usuarios intermedios y avanzados en informática.

Figura 5. Firewall (Cortafuegos)



Fuente: Imágenes de Google

El UTM se define como un dispositivo multifunción de red que unifica en una única interfaz antivirus, firewall y sistema de detección/prevención de intrusos. Desde su creación, el UTM no ha dejado de crecer, y hoy en día añaden a las anteriores herramientas las de NAT, VPN, antispam, antiphishing, antispyware, filtro de contenidos y sistemas IDS/IPS.

Entre las mayores ventajas de este sistema podemos destacar flexibilidad, bajo costo, reducción de la complejidad e integración completa en un único programa.

Como desventajas debemos citar que estamos fiando toda la seguridad en un único sistema, por lo que de ser vulnerado estaríamos gravemente expuestos. Además, se generan problemas de rendimiento al activar todas las herramientas simultáneamente.

Existen numerosos firewall gratuitos, pero en el caso de una empresa es recomendable instalar uno de pago, ya que la protección que nos ofrece la versión gratuita del programa se antoja escasa para las necesidades actuales de las pymes.

A la hora de elegir cuál es el tipo de firewall UTM que mejor se adapta a las necesidades de nuestra empresa hemos de tener en cuenta los siguientes aspectos:

VENTAJA1. Interfaz clara, sencilla, fluida y de fácil manejo. Sería un gran punto a favor que ofreciera facilidades de manejo y actualizaciones de software.

VENTAJA2. El número de usuarios que se conectarán a la red.

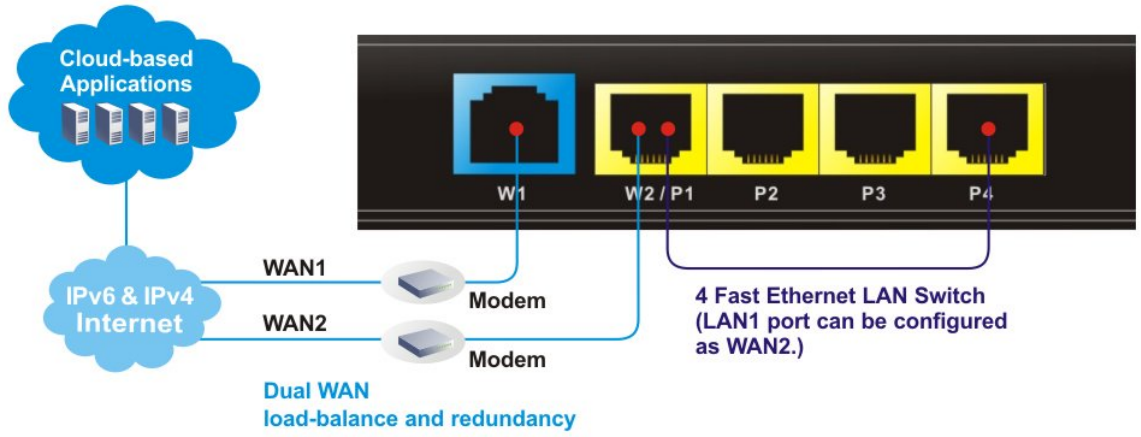
VENTAJA3. El número de sesiones simultáneas.

VENTAJA4. Según Tecnozero (2019), el número de puertos configurables, para lo que debemos tener en cuenta las necesidades de la empresa en cuanto al tamaño de red y el crecimiento esperado de dicha red en los próximos 3 años.

VENTAJA5. Posibilidad de emplear puertos USB para realizar backups periódicos y establecer conexiones 4G remotas.

VENTAJA6. Posibilidad de emplear puertos WAN como red de emergencia para actuar como salvavidas en caso de interrupción de los servicios de red habituales.

Figura 6. Puertos WAN



Fuente: Imágenes de Google

VENTAJA7. El Throughput, esto es, la tasa máxima de producción a la que la información puede ser procesada. Los más destacados son:

a. NGFW: Autorizan o deniegan los accesos a la información que pasa a través del dispositivo.

b. Túneles VPN: Permiten establecer conexiones privadas (seguras) entre la oficina y un trabajador que se ubique fuera de la misma, o entre distintas oficinas.

c. IPS: Permite una gestión mucho más efectiva de los paquetes de software.

d. Proxy: Se trata del programa que actúa como punto intermedio en una comunicación, siendo la primera barrera de protección de nuestra red.

VENTAJA8. Posibilidad de emplear conexiones WIFI dentro de la empresa. Hay que tener en cuenta la necesidad de realizar una cobertura completa, pues es fácil que aparezcan zonas de mala calidad de la conexión, lo que se incrementará con la distancia (si la oficina es grande) y con los obstáculos físicos (como paredes y muros).

VENTAJA9. Sistema para detectar y proteger contra APT y ataques dirigidos.

VENTAJA10. En conclusión, debemos de conocer las necesidades de nuestra empresa a la hora de decantarnos por una opción u otra, y estudiar con detenimiento las ofertas disponibles para escoger el firewall UTM que mejor se adapte a lo que buscamos.

2.7. El control de accesos

Uno de los mayores (o el mayor) activo de toda organización es la información que maneja. En ocasiones nos cegamos con protegerla con complejas técnicas de cifrado, caros equipos informáticos y complejos software de seguridad, pero olvidamos controlar algo tan básico como a las personas que tienen acceso a esa información. Aquí es donde cobra un especial protagonismo la importancia del control de acceso.

Lo primero que debemos de preguntarnos para comenzar a protegernos adecuadamente es quién maneja la información en mi organización.

Nos daremos cuenta enseguida de que nos enfrentamos a varias dificultades, entre las que destaca las producidas por el crecimiento del método BYOD, pues los

empleados manejan datos confidenciales de la empresa en sus propios dispositivos. La empresa no puede asegurarse del uso que hace el empleado de los mismos ni de si este elimina correctamente los archivos confidenciales de la empresa una vez cesa su relación laboral con la misma.

Para evitar las situaciones peligrosas a las que podría enfrentarse la empresa debemos de llevar a cabo una serie de medidas principales:

2.7.1. Política de usuarios y permisos

Se trata de definir a los usuarios en función de su rol dentro de la empresa asignando permisos de usuario acordes a las funciones de los empleados. De forma genérica se procederá a adjudicar el mínimo privilegio a los usuarios.

2.7.2. Creación, modificación y borrado de las cuentas de acceso

El sistema será controlado por un administrador, el cual añadirá a los nuevos empleados a los que suministrará las credenciales confidenciales de acceso, las cuales han de ser cambiadas cada cierto periodo de tiempo. El propio administrador se encargará de añadir los permisos de usuario a cada empleado de forma específica y modificar los mismos en caso de que varíen a lo largo del tiempo las funciones o el rol de este dentro de la compañía.

2.7.3. Cuentas de administrador

Las cuentas de usuario atesoran funciones muy limitadas dentro del sistema informático de la empresa, mientras que aquellas con permisos de administrador tienen la capacidad de hacer y deshacer a voluntad.

Por lo tanto, estas cuentas tienen una importancia vital, motivo por el que deberán de:

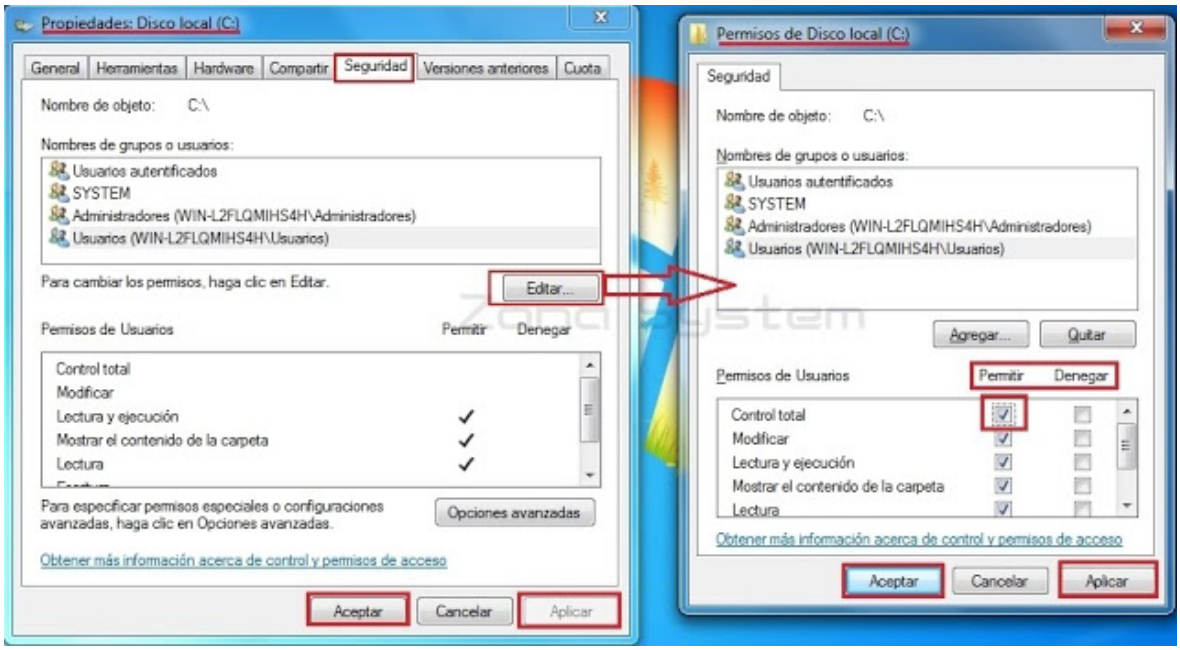
SEG1. Ser protegidas de forma robusta, empleando contraseñas seguras y la autenticación de doble factor. Además, hemos de cambiarlas cada cierto tiempo.

SEG2. Acceder a ellas únicamente cuando sea necesario.

SEG3. Mantenerlas bajo vigilancia constante sometiéndolas, además, a auditorías cada cierto tiempo.

SEG4. Llevar a cabo una anotación continua de las acciones que realicen mediante un registro de logs.

Figura 7. Cuenta de administrador. Permisos de usuario



Fuente: Imágenes de Google

2.7.4. Mecanismos de autenticación

Se deberán de valorar los diferentes mecanismos de autenticación y aplicar los más convenientes en función de la empresa.

2.7.5. Registro de actividad

Es importante que los cambios de cierta importancia que se realicen queden registrados en una base de datos detallando fecha, hora y usuario que los realizó.

2.8. Permisos de usuarios

Los permisos con los que cuentan los usuarios deberán de ser inspeccionados periódicamente, pudiendo ser revocados algunos de ellos si se comprueba que no son necesarios para la actividad normal del usuario en la plataforma.

Todas estas medidas de protección han de aplicarse a través de una política de ciberseguridad adecuada y cuidadosamente seleccionada.

2.9. ¿Cómo afecta a la reputación de tu web el Black SEO?

El SEO (Search Engine Optimization) “es una disciplina que consiste en aplicar una serie de técnicas tanto dentro (On-Page) como fuera (Off-Page) de una determinada

página web, con el objetivo de optimizar su visibilidad en los resultados orgánicos de los diferentes motores de búsqueda.

En conclusión, es un conjunto de acciones enfocadas a mejorar la posición del sitio en los resultados de búsqueda para las consultas específicas de los diferentes usuarios, con el fin de aumentar el tráfico web y la posibilidad de monetización." (Facchin, 2018, 5.º párrafo).

Cuando realizamos búsquedas a través de los principales buscadores de Internet (Google, Yahoo, DuckDuckGo…) nos encontramos de manera general cientos de miles de resultados, y por difícil que sea de creer solemos encontrar la página que más se ajusta a nuestras necesidades en las primeras posiciones. Entonces, ¿cómo funcionan los buscadores?

El criterio más importante es la autoridad. Según nos han revelado varios análisis SEO sobre Google, el buscador más popular a nivel mundial, la autoridad es el componente que condiciona el 75 % de los resultados en dicho buscador.

Para calcular la autoridad de una página web los buscadores se ayudan de complejos algoritmos que conocen lo que estamos buscando y dan con las páginas que mejor se ajustan a ello. A pesar de que suele indicarse que la autoridad de un determinado sitio web viene determinada por la cantidad de enlaces que direcciones hacia el mismo contenido en páginas externas, la realidad es que eso no siempre es así. Por ejemplo, si queremos buscar información sobre biotecnología es factible que en lugar de aparecer Wikipedia como primera opción (a pesar de ser quien más enlaces externos tenga a su página sobre el tema) nos aparezcan los resultados de "Centro de Biotecnología" en primer lugar. Este fenómeno se produce porque Google interpreta que existe otra opción más especializada en el tema de lo que lo está Wikipedia. A pesar de la gran autoridad de Wikipedia en Internet, la página de "Centro de Biotecnología" tiene más autoridad sobre biotecnología.

El otro criterio a tener en cuenta no es otro que la relevancia. En este caso se trata de la relación existente entre los términos que la persona escribe en el buscador y los resultados que obtiene.

El método empleado consiste en un análisis mediante algoritmos de las web. Por desgracia, es el método en el que existe un menor avance, pues mientras que analizar texto resulta sencillo, las imágenes y vídeos son muy difíciles de analizar para los algoritmos de los buscadores.

Este fenómeno hace que las web introduzcan un “texto ancla” (anchor text) en los enlaces que envían a la página en la que trabajamos. Se trata de una estrategia muy inteligente para ganar visibilidad en la web, ya que los buscadores acuden a este texto para indexar los resultados de búsqueda.

Por último debemos de hablar de la jerarquía de la información como método ingenioso de estructurar el contenido de una web.

Es probable que como compañía queramos que la gente nos conozca por un producto o servicio estrella que ofrecemos. Por lo tanto en la URL de nuestra web deberemos de incluirlo de algún modo. Por poner un ejemplo, si vendemos material de oficina y tenemos los archivadores como producto estrella, nuestra URL se articulará al final como /archivadores en lugar de /4368453. De este modo logramos que se nos reconozca inmediatamente por el producto o servicio que más queremos enfatizar en nuestro negocio. De este modo resultará sencillo para nuestros clientes potenciales identificar nuestra actividad o fortaleza que resaltamos y los buscadores averiguarán la actividad a la que nos dedicamos.

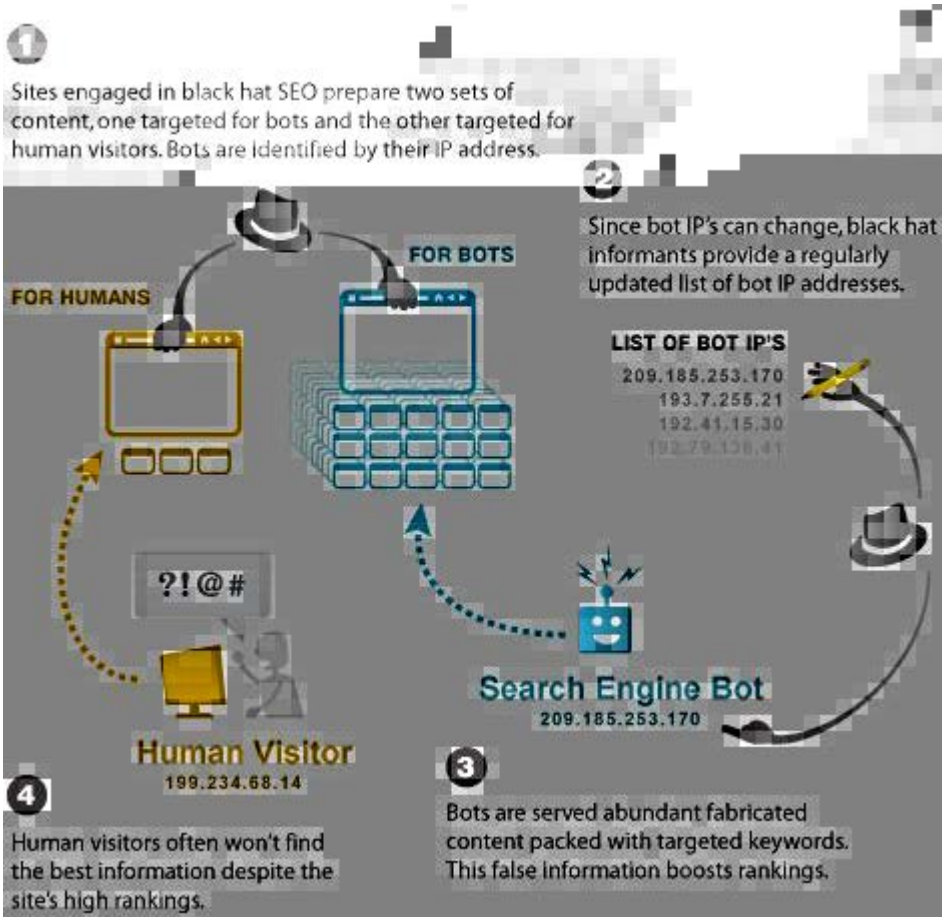
Una vez expuesto el concepto de SEO y el funcionamiento de los buscadores web damos paso a profundizar en los usos, tanto positivos como negativos del SEO.

Por un lado el White SEO (explicado anteriormente) emplea una ingeniería de contenido inteligente que permita que una página gane notoriedad y posicionamiento.

Por otro lado, el Black SEO emplea artes nocivas con el mismo fin. Las malas prácticas llevadas a cabo en el Black SEO son:

1. Añadir comentarios falsos o spam en diferentes websites con enlaces a la web que pretende ser atacada para engañar a los buscadores y que la consideren más relevante.
2. Cloaking, en español encubrimiento, que consiste en enseñar una página al buscador con aquellas palabras clave que nos pueden dar notoriedad, y una diferente al usuario, la cual sería nuestra verdadera web.

Figura 8. Explicación del concepto de Cloaking



Fuente: (Dircomfidencial Medios, 2016)

3. Ocultar texto (que contenga palabras claves para el buscador) dentro de nuestra web utilizando, por ejemplo, el mismo color para el texto que para el fondo de la página, por lo que no sería posible de percibir para el usuario.

Evidentemente, no está todo escrito en lo referente a métodos de engaño a los SEO, por lo que van surgiendo otros nuevos con el paso del tiempo.

Pese a que la tentación de emplear las técnicas de Black SEO para aumentar la monetización de nuestra web puede ser muy grande, conviene que lo pensemos dos veces antes de emplear la mala praxis, pues en caso de que un SEO se percate de nuestras prácticas, seremos penalizados, pudiendo llegar a ser eliminados de sus resultados de búsqueda.

Por lo tanto nos surge una duda: ¿Qué sucedería si terceras personas o empresas de la competencia emplearan Black SEO para potenciar nuestra web, ser detectados y penalizados por los buscadores?

Existen multitud de webs gratuitas en Internet en las que podemos buscar backlinks (links que redireccionan a nuestra web), siendo la forma más sencilla escribir en la caja de búsquedas “link:www.nuestrawebejemplo.com" con nuestra dirección web.

Las herramientas gratuitas más famosas son: Google para Webmasters, Open Site Explorer, Majestic, Woorank, OpenLinkProler, CognitiveSEO, Site Explorer, Ahrefs, LinkResearchTool. En caso de encontrar sites donde se hallen links con apariencia fraudulenta que apunten a nuestra página hemos de desacreditarlos contactando con los buscadores.

Otro método de Black SEO consiste en duplicar el contenido de nuestra web y copiarlo en otra página de mayor relevancia, lo que hará que los algoritmos del buscador nos identifiquen como copia y perdamos reputación, lo que desembocará en una merma de nuestra notoriedad y presencia. De igual manera tendríamos que contactar con los buscadores para solucionar el problema.

En resumen, los SEO pueden ser nuestros mejores aliados para ganar mercado y presencia en la red si sabemos cómo sacar partido de ellos. Sin embargo, si empleamos malas artes para lograr nuestros objetivos o si alguien nos trata de dañar mediante el uso de Black SEO, es conveniente estar preparados, desconfiar si apreciamos cambios en el entorno y actuar con brío y rapidez para solventar el problema cuanto antes y no dañar reputación, notoriedad ni presencia de nuestro negocio.

2.10. Fugas de información y otros riesgos

Distinguimos tres causas posibles de la fuga de información: accidental, intencionada o por medio de un ataque externo.

De una fuga intencional no nos podemos defender, pero podemos implementar medidas de seguridad para conocer qué personas tenían acceso a esa información y acotar al delincuente.

Si la fuga es accidental sigue suponiendo un serio problema para la empresa, por lo que la mejor forma de evitarlo es formar a los empleados en medidas preventivas para evitar accidentes.

Si por el contrario la fuga se produce por medio de un ataque externo a la organización perpetrado por ciberdelincuentes lo que podemos hacer es dificultar al máximo su labor y tratar de que si roban datos no los puedan leer.

Además, existen otros riesgos como:

Fugas de información relacionadas con imprudencias en el uso de la nube o del correo electrónico.

Ataques de ingeniería social, como puede ser un soporte técnico fraudulento o el uso de la página web de la organización para instalar software malicioso que infecte a aquellos que interactúen con la misma.

Por ello, lo principal es que la organización implemente una lisa de buenas prácticas y requisitos legales para guarnecer su seguridad.

El propósito primordial es resguardar la información y los sistemas que gestionan la organización aplicando una serie de políticas de seguridad y buenas prácticas:

BP 1. Utilizar medidas de seguridad para garantizar un acceso seguro a los equipos y a la nube.

BP 2. Clasificar y tratar la información de distinta manera en función a su importancia.

BP 3. Fijar permisos de usuario para que quienes accedan al sistema solo puedan hacerlo a los apartados que tengan asignados.

BP 4. Mantener el software actualizado a la última versión disponible.

BP 5. Hacer uso de un potente antimalware y crear un protocolo para evitar ataques mediante el correo electrónico.

BP 6. Conseguir implicar de forma activa y eficaz a todo el equipo que conforme la organización.

BP 7. Instaurar una política de actuación que cada empleado conozca a la perfección y se sienta implicado en el reto de la ciberseguridad.

BP 8. En caso de que se registre un incidente habrá que notificarlo ante la autoridad competente y los afectados en un máximo de 72 horas (si la información sustraída pusiera en peligro la privacidad) en cumplimiento del RGPD, que será tratado con más detenimiento posteriormente.

2.11. Los sellos de confianza online

El negocio de las empresas que operan online se sustenta sobre la confianza que la empresa genera en los clientes. Estos valoran los bienes y/o servicios que la empresa ofrece y tienen un alto grado de certeza de que sus datos están a salvo de terceros y de que podrán disfrutar del bien o servicio en cuestión.

Para nosotros resulta fundamental construir una buena relación de confianza con el cliente, por lo que nos podemos servir de sellos de confianza para incrementar la seguridad de clientes potenciales.

Una acción muy sencilla que puede hacernos lucir de forma más segura a ojos de aquellos que visiten nuestra web son los sellos de confianza.

Los sellos de confianza pueden conseguir de múltiples maneras:

FORMA1. Por buenas prácticas

FORMA2. Por una auditoría externa

FORMA3. Por medio de un certificado

FORMA4. Mediante las buenas opiniones de nuestros clientes

Para obtener cada uno de los sellos se evalúan una serie de aspectos que explicaremos a continuación:

ASPECTO 1. Protección de datos personales. Se ha de asegurar que el sitio web cumple la normativa (española o internacional equivalente) en lo referido al tratamiento de datos personales.

ASPECTO 2. Seguridad de la información. La entidad solicitante del sello deberá probar que emplea métodos de seguridad en el tratamiento de la información más allá de los previamente mencionados respecto al tratamiento seguro de datos de carácter personal.

ASPECTO 3. Confidencialidad de las comunicaciones. Verificar que los datos confidenciales que el cliente comparte con la entidad solicitante, como aquellos involucrados en los procesos de compra, se envían de forma segura. Por norma general se recomienda el uso de certificados electrónicos.

ASPECTO 4. Protección de colectivos específicos.

ASPECTO 5. Identificación. Tiene como objetivo especificar aquellos contenidos cuyo destinatario sea exclusivamente público adulto.

ASPECTO 6. Transacciones. La entidad solicitante debe de disponer de métodos seguros para impedir que menores sin la autorización de sus padres lleven a cabo compras en su web.

ASPECTO 7. Acceso. Se deberá de restringir el acceso a menores a determinados contenidos y compras.

ASPECTO 8. Publicidad. La entidad solicitante ha de verificar que la publicidad sea respetuosa con menores.

ASPECTO 9. Resolución extrajudicial de conflictos. El usuario tiene la capacidad de exigir a la marca proveedora del sello de confianza que ejerza de mediador en un conflicto, cuando este no se haya solucionado entre las otras partes.

ASPECTO 10. Transparencia. La web que solicita el sello ha de presentar de forma clara toda la información referida a la propia empresa, su actividad y formas de operar ante posibles eventualidades del servicio.

ASPECTO 11. Revisión continua. Es imprescindible que de forma anual, la propia empresa que concede el sello, audite (ella misma o mediante una tercera parte independiente) a la parte solicitante del sello, a fin de verificar que sigue cumpliendo los requisitos necesarios.

Respecto a los sellos en sí, existen diferentes tipos en los distintos apartados (INCIBE, 2019):

Comercio electrónico

1. AENOR eComercio
2. Confianza Online
3. eValor
4. iCERT
5. Trusted Shops

Cloud

1. CSA Star

2. McAfee Cloud 

Web

1. Comodo COMODO
2. Digicert 
3. Entrust 
4. GeoTrust 
5. GlobalSign 
6. GoDaddy 
7. HTTP CS 
8. Network Solutions 
9. Norton Secured 
10. SSL.com 
11. Thawte 
12. Trustwave 
13. Viesec 

Otros

1. AEI Sello de Seguridad para Organizaciones 

2. EuroPriSe 
3. Juego Seguro 
4. Leet Security 
5. TRUSTe 

2.12. RGPD

El Reglamento General de Protección de Datos (RGPD) es una ley de obligado cumplimiento para toda organización que se encuentre en la UE, haga negocio con personas u organizaciones que se encuentren en la UE o se dedique al tratamiento de datos de personas u organizaciones de la UE.

El RGPD establece una serie de medidas de obligado cumplimiento para las páginas web que llegan para legislar porque la aparición de nuevos conceptos y tecnologías obligaba a una actualización de la ley a estos nuevos tiempos.

2.12.1. ¿Cómo aplicarlo correctamente?

FORMA1. Identificar el tipo de datos con los que estamos tratando, pues datos especialmente sensibles pueden requerir de medidas especiales de seguridad.

FORMA2. Mantener informadas a las personas en todo momento de cómo se procederá al tratamiento de sus datos personales.

FORMA3. Asegurarnos de que solicitamos su consentimiento para el tratamiento de sus datos de forma clara, precisa e inequívoca.

FORMA4. Facilitar la solicitud para la eliminación de datos personales.

FORMA5. Determinar las dificultades a las que nos podremos enfrentar para prepararnos frente a ellas.

FORMA6. En el caso de que decidamos subcontratar el tratamiento de datos a otra empresa, prestar especial atención al contrato, asegurándonos de que garantice un tratamiento seguro.

FORMA7. Examinar cada parte del proceso, dictaminar el grado de satisfacción respecto al su aplicación y evalúa en éxito o fracaso del mismo.

FORMA8. Se deberán llevar a cabo una serie de medidas:

FORMA9. Mantener los ficheros (tanto físicos como virtuales) que contengan datos personales correctamente almacenados.

FORMA10. Evitar transportar soportes físicos que contengan datos personales.

FORMA11. Garantizar un tratamiento de datos de carácter personal seguro, permitiendo su acceso únicamente a los trabajadores autorizados.

FORMA12. Eliminar datos personales cuando sea solicitado.

FORMA13. En caso de incidencias que menoscaben la privacidad, comunicar a los afectados y a la autoridad competente en un plazo máximo de 72 horas.

FORMA14. Priorizar una correcta disposición de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).

2.12.2. ¿Cuáles son los objetivos del RGPD?

Los objetivos principales que se pretenden alcanzar son los siguientes:

- Evitar vacíos legales debido a cambios sustanciales en el entorno debido a las nuevas tecnologías.
- Defensa a ultranza del derecho al honor y a la intimidad.
- Establecer un marco en el que las personas recuperan parte del control sobre sus datos personales y su tratamiento en las empresas.

2.13. LOPDGDD

El RGPD se trata normativa europea, de obligado cumplimiento en la UE. Sirve para definir la base dentro de la cual se enmarcarán los distintos reglamentos que a nivel individual creen los legisladores de cada país miembro.

La LOPDGDD (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales), también conocida como LOPD (Ley Orgánica de Protección de Datos), se trata de normativa española en base al RGPD.

La LOPD establece que aquellas empresas que por su trabajo se vean obligadas a recopilar información de sus clientes de carácter personal deban de realizar un determinado tratamiento a los ficheros:

ACCIÓN1. Primará el secreto respecto a la información contenida en los mismos.

ACCIÓN2. Cuando los datos sean almacenados de manera física se deberá de hacer en condiciones de máxima seguridad, bajo llave.

ACCIÓN3. Permitir el acceso a la información únicamente al personal autorizado.

ACCIÓN4. Derecho del cliente a solicitar el borrado y destrucción de sus datos personales.

ACCIÓN5. En caso de algún ataque o algún otro tipo de incidencias ha de ser comunicado a la autoridad competente y a los afectados de forma rápida.

Se pretende reforzar la protección de los datos especialmente sensibles, como es la información del historial médico de las personas, su raza o etnia. Además, se busca proteger a los menores y el tratamiento de sus datos personales de forma más severa.

Por último, destacar que se facilita el acceso a los datos de personas fallecidas, así como se presupone un uso con interés legítimo de los datos por parte de empresarios, haciendo especial hincapié en el derecho del individuo de exigir a una empresa que elimine sus datos personales de sus bases de datos. Se amplía este derecho al derecho a la intimidad y al derecho a no estar monitorizado por sistemas de geolocalización en el ámbito laboral.

3. Entrevistas a empresarios

El cuestionario siguiente se ha creado con el objetivo de aportar trabajo de campo a este documento, mostrando la situación en cuanto a ciberseguridad de empresas reales (cuatro de Valladolid y provincia, y una de Madrid), para aportar una visión más práctica de los aspectos de seguridad detallados a lo largo del proyecto.

Para crear las preguntas en un primer momento se creó un borrador de cuestionario, que en una reunión con mi tutor académico consideramos que debía de ser modificado haciéndolo menos intrusivo, por lo que nos dispusimos a rehacerlo, mostrando a continuación el cuestionario definitivo. Las entrevistas, todas ellas presenciales, se realizaron entre el 11 y el 27 de mayo de 2019, y las preguntas que se realizaron en las mismas se detallan a continuación:

ÍTEM 1. ¿Qué medidas de ciberseguridad tienen implementadas en su empresa?

ÍTEM 2. ¿Dispone su empresa de responsable de ciberseguridad?

ÍTEM 3. ¿Han recibido los empleados formación específica en temas de ciberseguridad? En caso afirmativo, ¿la reciben con cierta periodicidad? ¿Cada cuánto tiempo?

ÍTEM 4. ¿Ha sufrido su empresa algún ataque de ciberseguridad? En caso afirmativo, ¿me podría indicar muy brevemente en qué consistió?

ÍTEM 5. ¿Tienen la posibilidad sus empleados de trabajar empleando sus propios ordenadores portátiles y teléfonos móviles? ¿Emplean alguna medida de seguridad extra impuesta por la empresa?

ÍTEM 6. ¿Existe la posibilidad para los empleados de realizar teletrabajo? ¿Emplean alguna medida de seguridad extra impuesta por la empresa?

ÍTEM 7. ¿Utiliza su empresa el servicio de computación (gestión) en la nube? ¿Me podría indicar si emplean nube privada, pública o híbrida?

ÍTEM 8. ¿Ha cambiado sustancialmente vuestra forma de trabajar la implantación del RGPD? ¿Qué cambios ha supuesto en caso de trabajar con otros países europeos?

ÍTEM 9. ¿Realizáis copias de seguridad? ¿En qué formato? ¿Cómo y dónde las almacenáis?

ÍTEM 10. Respecto al tratamiento de datos, ¿sois vosotros quienes lo gestionáis o se encuentra subcontratado este servicio?

Indicar que estas entrevistas no pretenden en ningún momento, por el número reducido de ellas, tener un valor estadístico extrapolable a ningún espacio muestral. Es decir, los datos obtenidos no sirven como representativos de Valladolid, y menos aún de posibles territorios más extensos.

La notación R1, R2… que utilizaremos a continuación, se refiere a las respuestas de cada empresa en los 10 ítems antes indicados.

EMPRESA 1: Empresa anónima dedicada a la venta online de ropa. Cuenta con 2 trabajadores.

R1. Utilizamos una cuenta de Google Drive, así como una cuenta Premium de Google Business. Además, nuestra página web emplea el protocolo https.

R2. No, porque las medidas de seguridad que nos protegen vienen proporcionadas por la empresa de hosting Shopify.

R3. No. Al ser una empresa de reciente creación, el único empleado es un alumno en prácticas que no ha recibido entrenamiento en ciberseguridad por parte de la empresa.

R4. No.

R5. Sí. No.

R6. Sí. No.

R7. Sí, Pública.

R8. Cuando la empresa fue creada, el RGPD ya estaba en vigor.

R9. Sí. Disco duro y Google Drive, almacenadas en la vivienda del propietario.

R10. Subcontratado. Shopify lo lleva pero podemos acceder a esos datos para mailing u otros motivos.

EMPRESA 2: Empresa anónima dedicada a la industria alimentaria. Cuenta con unos 20 trabajadores.

R1. Aquellas medidas de seguridad que ofrece WordPress. Además contamos con pago seguro a través de Paypal o la plataforma de pagos online del Banco Santander. Nuestra web cuenta con el protocolo https. En los ordenadores desde los que se trabajamos hay antivirus instalados.

R2. No.

R3. No.

R4. No.

R5. Sí. No.

R6. Las conexiones remotas las realizamos mediante el programa Teamviewer. No.

R7. No.

R8. No. Ninguno.

R9. Sí, semanalmente. Disco duro externo. Guardados bajo llave en la oficina.

R10. Subcontratado.

EMPRESA 3. Empresa anónima dedicada a industria alimentaria. Cuenta con unos 120 trabajadores.

R1. Firewall, antivirus, control de acceso limitado por usuario, copias de seguridad, formación al personal de las medidas de prevención.

R2. Sí.

R3. Periódicamente se va poniendo en conocimiento de todos los usuarios de equipos informáticos, de buenas prácticas a seguir. Y en caso de que haya algún ataque específico conocido, se avisa de ese riesgo de forma particular.

R4. En un par de ocasiones por ataque de ransomware vía correo electrónico. Se pudo detectar de forma rápida por el aviso de los usuarios al detectar actividades sospechosas en ficheros y aplicaciones. Los ficheros que se vieron afectados pudieron ser totalmente recuperados gracias a la copia de seguridad en uno de los casos y a la vacuna proporcionada por el fabricante del antivirus en el otro caso.

R5. En algunos casos concretos sí pueden trabajar desde sus equipos, pero sólo como pasarela para conectarse remotamente a los equipos de la empresa.

R6. Sí, los empleados que por razones de su puesto, tienen que trabajar desde fuera de las oficinas, tienen instalado en sus equipos la conexión vía VPN para poder trabajar como si estuvieran en la oficina.

R7. No lo usamos.

R8. No nos ha afectado especialmente. A nivel de seguridad ninguno.

R9. Sí, con distintas periodicidades y almacenando el contenido en distintos formatos y en distintos dispositivos para tener varias alternativas a la hora de tener que realizar una recuperación de ficheros.

R10. Subcontratado.

EMPRESA 4: Empresa anónima dedicada a servicios financieros. Cuenta con unos 300 trabajadores.

R1. Más que medidas son procedimientos.

R2. Sí.

R3. No. Se recibe información relativa a Protección de Datos, pero no de ciberseguridad.

R4. Hasta ahora no lo ha sufrido.

R5. Sí pueden trabajar con sus ordenadores privados, pero el procedimiento indica lo contrario. Por lo tanto, si seguimos el procedimiento, NO emplean sus ordenadores privados. Respecto a la medida de seguridad, todos los equipos están protegidos con BitLocker y poseen su propio antivirus

R6. Sí.

R7. Sí. Nube privada

R8. No ha cambiado la forma de trabajar, pero sí la premisa del RGPD está siempre encima de la mesa. Respecto a trabajar con otros países europeos, el RGPD siempre es transversal a toda conversación; es decir: todas las operaciones y conversaciones se hacen dentro del marco controlado y gestionado por el RGPD

R9. Sí. Las tenemos en dispositivos físicos (no en cintas). Se almacenan en dos entornos, uno de ellos está fuera de la unidad central de proceso

R10. Somos nosotros.

EMPRESA 5: Empresa anónima dedicada a la gestión y creación de páginas web. Un único trabajador.

R1. Una medida fundamental para nuestro modelo de negocio son los servidores protegidos con ban de tiempo al introducir mal la contraseña en varias ocasiones. Empleamos además, https. Siempre aplico la prudencia y la formación continua en ciberseguridad como mis grandes medidas defensivas.

R2. Subcontratado.

R3. No hay empleados.

R4. He sufrido ataques para tumbar el servidor negación de servicio.

R5. Sí, prudencia, además de un WIFI doméstico con contraseña robusta

R6. Sí, conectarse a la red privada del móvil.

R7. Sí. Privada.

R8. He tenido que actualizar las cláusulas en la web. No trabajo con otros países europeos.

R9. Dos veces al día. Nube.

R10. La propia empresa.

Analizando las respuestas de las empresas que han aceptado la invitación para responder a este breve cuestionario, podemos ver que son empresas con un nivel medio-alto de ciberseguridad.

Como se menciona a lo largo de todo el trabajo, los ataques a las empresas son bastante habituales, como queda reflejado en el cuestionario, donde varias empresas confiesan haber sufrido varios.

En el caso concreto de la empresa 2, el hecho de no requerir almacenar datos es un punto a su favor. Además, la plataforma de pagos que emplea es Paypal, que dispone de uno de los sistemas de pago más robustos del mundo, o la plataforma de una conocida entidad bancaria, por lo que evitan entrar en contacto siquiera con los datos bancarios, siendo menos atractivos para posibles atacantes.

Otra de las conclusiones obtenidas es que las empresas que te permiten subcontratarles alguna parte no esencial de tu negocio son una opción muy rentable, ya que varias de las empresas acuden a este tipo de compañías para ahorrar tiempo.

Me gustaría hacer una mención especial al apartado de la computación en la nube, ya que pese a la gran cantidad de nubes públicas y asequibles que existen, varias empresas emplean su propia nube privada. Existen dos lecturas al respecto: la confianza que genera ser uno mismo quien gestione su propia nube puede ser importante para la empresa y para el cliente (siempre que la empresa se esfuerce en hacer visible ese aspecto) o existe cierta reticencia a que compañías como Google, por ejemplo, almacene datos sensibles por si pudieran hacer un uso ilícito de los mismos.

4. Conclusiones

De la realización completa de este trabajo, así como de toda la literatura empleada para la realización del mismo y de las cinco entrevistas realizadas, llegamos a las conclusiones siguientes:

1. La ciberseguridad, durante tanto tiempo ignorada por el usuario medio de Internet y por las empresas, se ha convertido en una prioridad, siendo un negocio que mueve más de 100 mil millones de euros al año.
2. Desde el primer gran virus de propagación masiva, conocido como *ILoveYou* y que infectó de forma masiva a ordenadores de todo el mundo, se han creado infinidad de recursos maliciosos con el único objetivo de monetizar esos ataques. Mientras que en un primer momento el objetivo de muchos hackers era demostrar al mundo y a sí mismos el poder que ostentaban desde detrás de la pantalla de un ordenador, hoy en día su principal objetivo es la capacidad de ganar dinero.
3. Las empresas que se dedican a la ciberseguridad han experimentado un enorme crecimiento en los últimos años, debido a que tanto el usuario medio de un ordenador o un dispositivo informático hasta las empresas de todo el mundo demandan sus servicios, atemorizados de que sus datos privados o los de sus clientes o proveedores puedan caer en malas manos.
4. En el caso particular de las empresas españolas, por lo general, no se presta demasiada importancia a ciertas medidas de seguridad cuya importancia es superior a lo que se suele imaginar, aunque a medida que van aumentando los ataques cibernéticos, esa percepción de riesgo aumenta. De este modo, los expertos en ciberseguridad son un perfil muy demandado en la actualidad.

   Respecto a las entrevistas con las cinco empresas:

5. El protocolo https está muy extendido, así como la procedencia y medidas generales que incorporan los gestores o plataformas web.
6. No siempre existe un responsable de ciberseguridad en las empresas, seguramente por resultar imposible asumir el coste a empresas pequeñas. No obstante, en las empresas grandes, sí existe tal figura.
7. La formación específica en ciberseguridad a los es una característica exclusiva de las empresas de mayor tamaño. No obstante, en algunas empresas pequeñas la persona que gestiona los equipos informáticos tiene un gran conocimiento sobre el tema.

8. Varias empresas reconocen haber sufrido ataques de ciberseguridad. Por suerte, eran muy precavidas y lograron minimizar sustancialmente los daños que podían haber llegado a sufrir.

9. El BYOD es un método de trabajo extendido que genera cierta preocupación en las empresas en el apartado de la ciberseguridad, por lo que se suelen tomar algunas medidas de protección extra. Sin embargo, considero importante destacar, que en alguna empresa se prohíbe esta práctica por considerarla demasiado arriesgada para la seguridad de la compañía.

10. El teletrabajo es una práctica habitual, ya sea empleando VPN, algún programa de conexión remota con cifrado, los datos móviles o ninguna medida extra de ciberseguridad. Los datos móviles o una VPN robusta son, a priori, las medidas más seguras.

11. La nube es un servicio habitual en las empresas. Mientras que algunas se decantan por la nube privada, otras lo hacen con servicios de nube pública muy extendidos como Drive de Google.

12. El RGPD no ha supuesto un gran cambio en la forma de trabajar de estas empresas.

13. Todas las empresas entrevistadas realizan copias de seguridad con frecuencia, siendo el disco duro externo el formato más empleado. No obstante, difieren a lo largo del almacenamiento de los discos duros.

14. Por lo general, el tratamiento de datos es una actividad que la empresa subcontrata a otras empresas especializadas.

15. La empresa promedio es vulnerable ante un empleado con escasa formación en ciberseguridad, o que tenga malas intenciones para con la propia empresa.

16. Varios empresarios y directivos de varias empresas han aceptado nuestra petición de realizarles una entrevista anónima, donde he podido constatar que se trataba de empresas que tienen implementado un nivel de protección superior al de la media nacional, aunque eso no debiera de hacerlas sentirse seguras, porque la ciberseguridad requiere de atención y actualización constantes.

5. Bibliografía

10minutemail. (2019). *Bienvenido a 10 Minute Mail*. Recuperado el 15 de mayo de 2019, de https://10minutemail.net/

Alemán, M. (2017). *Correo electrónico temporal: Qué es, para qué sirve y cómo crearlo.* Recuperado el 25 de mayo de 2019, de https://bit.ly/2WhCuDS

Asociación para el Progreso de la Dirección (APD). (2018). *Ciberseguridad para empresas según tu sector empresarial.* Recuperado el 25 de mayo de 2019, de https://bit.ly/2IdQXI7

Blanco, A. [La Tienda de las Licencias]. (2019). *Cómo crear cuentas de correo temporales.* Recuperado el 22 de mayo de 2019, de https://bit.ly/2Hv9eBq

Condenet Ibérica [Revista GQ]. (25 de octubre de 2019). *Esto es lo que las empresas tecnológicas gastan al día en ciberseguridad*. Recuperado el 9 de junio de 2019, de https://bit.ly/2Llk4NQ

Dataseg consultores y auditores. (2019). *Ya está aquí la nueva LOPD, la LOPDGDD.* Recuperado el 25 de mayo de 2019, de https://bit.ly/2Hv93G3

Diaz, A. [ELISA INTERACTIVE]. (2017). *¿Qué son los Logs y por qué deben interesarte?* Recuperado el 10 de junio de 2019, de https://bit.ly/2Ib49in

Dircomfidencial Medios. (2016). *Black Hat SEO.* Recuperado el 22 de junio de 2019, de https://bit.ly/2x9jJUT

Domantas, G. [Hostinger]. (29 de mayo de 2019). *¿Qué es SSL/TLS y HTTPS?* Recuperado el 6 de junio de 2019, de https://bit.ly/2R5Gmmj

Donohue, B. [Kaspersky Daily]. (11 de junio de 2013). *¿Qué es una APT?* Recuperado el 8 de junio de 2019, de https://bit.ly/2GoEUIc

EAE Business School. (2019). *Diez claves sobre ciberseguridad en pymes.* Recuperado el 25 de mayo de 2019, de https://bit.ly/2Fcs0xH

Facchin, J. (2018). *¿Qué es el posicionamiento SEO y qué factores tener en cuenta para optimizarlo?* Recuperado el 10 de junio de 2019, de https://bit.ly/2wSGxpY

González, R. (1 de octubre de 2018). *Más de la mitad de las pymes sufren ciberataques.* Recuperado el 20 de junio de 2019 de https://bit.ly/2NfqG3b

InboundCycle. (23 de abril de 2014). *¿Cómo funcionan los buscadores?* [Blog]. Recuperado el 25 de mayo de 2019, de https://bit.ly/2YWWCJj

Instituto Nacional de Ciberseguridad (INCIBE). (16 de octubre de 2018). *El correo electrónico como canal para el fraude digital* [Blog]. Recuperado el 25 de mayo de 2019, de https://bit.ly/2W9rucy

Instituto Nacional de Ciberseguridad (INCIBE). (20 de diciembre de 2018). *Sigue estas recomendaciones para almacenar tu información en la nube* [Blog]. Recuperado el 25 de mayo de 2019, el 21 de mayo de 2019, de https://bit.ly/2LUk30B

Instituto Nacional de Ciberseguridad (INCIBE). (2016). *Desarrollar Cultura en Seguridad.* Recuperado el 25 de mayo de 2019, de https://bit.ly/2JImapH

Instituto Nacional de Ciberseguridad (INCIBE). (2018). *RGPD para pymes.* Recuperado el 25 de mayo de 2019, de https://bit.ly/2IbzvCw

Instituto Nacional de Ciberseguridad (INCIBE). (27 de noviembre de 2018). *Protege la información mediante técnicas criptográficas.* Recuperado el 25 de mayo de 2019, de https://bit.ly/2wkRjHa

Instituto Nacional de Ciberseguridad (INCIBE). (29 de noviembre de 2018). *Día Internacional de la Seguridad de la Información. El control de accesos.* Recuperado el 25 de mayo de 2019, de https://bit.ly/2TZQldW

Instituto Nacional de Ciberseguridad (INCIBE). (6 de marzo de 2018). *¿Cómo afecta a la reputación de tu web el Black SEO?* Recuperado el 25 de mayo de 2019, de https://bit.ly/2pz4wco

Instituto Nacional de Ciberseguridad (INCIBE). (6 de octubre de 2018). *Bondades y riesgos del BYOD.* Recuperado el 25 de mayo de 2019, de https://bit.ly/2GyxH8J

Instituto Nacional de Ciberseguridad (INCIBE). (8 de enero de 2019). *Sigue estas recomendaciones para almacenar tu información en la nube – Segunda parte.* Recuperado el 25 de mayo de 2019, de https://bit.ly/2RCuLxS

Joan Carles [no se indica apellido]. (25 de octubre de 2015). *¿Qué es y para qué sirve un email temporal?* [Blog]. Recuperado el 25 de mayo de 2019 de https://bit.ly/2EoyhUR

National Cyber Security Centre (NCSC). (2018). *10 steps to cyber security. Guidance on how organisations can protect themselves in cyberspace, including the 10 steps to cyber security.* Recuperado el 5 de junio de 2019, de https://bit.ly/2K8Ci48

NowMyMail. (2019). *Crea tu correo temporal y dile adiós al spam.* Recuperado el 15 de mayo de 2019, de https://www.nowmymail.com/

Pérez, J. y Gardey, A. (2013). *Definición de WAN*. Recuperado el 16 de junio de 2019, de https://definicion.de/wan/

Raul, A. C., Brown, C. T. y Blythe, F. (2019). *Spain's New Data Protection Act Now in Force.* Recuperado el 25 de mayo de 2019, de https://bit.ly/30wOtN6

Rodríguez, G. (2012). *¿Qué significa hacer Jailbreak y Root en un móvil?* Recuperado el 10 de junio de 2019, de https://bit.ly/2WnNnA0

Sage. (2018). *RGPD: ¿qué significan las siglas GDD dentro de la nueva LOPDGDD?* Recuperado el 25 de mayo de 2019, de https://bit.ly/2Hv9jVx

Tecnozero. (2019). *Firewall para empresas ¿Cuál elegir?* Recuperado el 25 de mayo de 2019, de https://bit.ly/2JHd6S1

Zinko Colombia. (2019). *Ventajas y desventajas de trabajar en la nube informática.* Recuperado el 25 de mayo de 2019, de https://bit.ly/2waHIT5

6. ANEXO: Glosario de términos

AES (Advanced Encryption Standard): También conocido como Rijndael (pronunciado "Rain Doll" en inglés), es el algoritmo de cifrado adoptado como estándar por el gobierno de los Estados Unidos.

APT (Advanced Persistent Threat o Amenaza Persistente Avanzada): Ataque por parte de un grupo de crackers a un empleado en concreto de una empresa que puede tener acceso a cierta información valiosa. Una vez logrado el crackeo, se sirven del empleado para llegar a mandos superiores en busca de información más valiosa.

Backup: Copia de seguridad.

Ban de tiempo en servidores: Penalización que se aplica dentro de una plataforma a quien haya incumplido sus normas. Se les impide el acceso a dicha plataforma por un periodo definido o indefinido de tiempo, atendiendo a la gravedad de la infracción, gravedad definida por los moderadores del servicio.

BYOD (Bring Your Own Device) o Lleva Tu Propio Dispositivo: Método de trabajo que consiste en prescindir de los equipos informáticos proporcionados por la empresa, haciendo que sea el propio trabajador quien emplee los suyos propios trasladándolos diariamente desde su vivienda a su oficina y viceversa.

Centro Criptológico Nacional (CCN): Organismo español público que forma parte del Centro Nacional de Inteligencia (CNI) y que se encarga de funciones derivadas de la ciberseguridad. También realiza certificaciones y cursos de formación.

Cifrado: Es el hecho de modificar un mensaje para que no sea posible leerlo si no se dispone de la clave correcta.

Conexión 4G: Conexión remota de alta velocidad a Internet. El nombre hace referencia a la cuarta generación móvil. Actualmente se está implementando la tecnología 5G. La principal diferencia entre el 4G y el 5G es que este último habilita conexiones a Internet mucho más veloces, al mismo tiempo que permite conectar muchos más dispositivos simultáneamente sin sacrificar la calidad ni la seguridad de la conexión.

Fake: Se trata de la difusión masiva de noticias falsas o bulos a través de correo electrónico, WhatsApp o Telegram principalmente. Suelen venir acompañadas de enlaces potencialmente peligrosos.

Firewall (Cortafuegos): Es un filtro que controla las comunicaciones entre redes y autoriza o deniega el paso en función de cómo lo hayamos ajustado.

Hosting o alojamiento web: Plataforma que permite la elaboración y sostiene el servicio de una página web, para que cualquiera pueda acceder e interactuar con ella.

Instituto Nacional de Ciberseguridad (INCIBE): Sociedad dependiente del Ministerio de Economía y Empresa para el Avance Digital y consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y demás sectores estratégicos.

Mailing: Técnica de marketing que consiste en enviar de forma masiva mediante un programa de gestión de correo, correos electrónicos comerciales a todas las direcciones almacenadas en una base de datos.

Malware: Correos electrónicos que adjuntan algún tipo de archivo malicioso que se introduce en el ordenador y lo infecta. ES fácil enviarlos masivamente y que algún trabajador de la empresa caiga en la trampa.

Nube: Dicho de manera sencilla, la nube es el suministro de servicios informáticos (servidores, almacenamiento, bases de datos, software…) a través de Internet. Estros servicios no están instalados en nuestros propios dispositivos, sino en servidores a los que se accede vía internet desde cualquier punto.

Phishing: Consiste en la suplantación de identidad a través del correo electrónico para obtener datos (generalmente bancarios) de la víctima.

Protocolo de seguridad TLS (Transport Layer Security o Seguridad en la Capa de Transporte): Normas de seguridad digital para cifrar la comunicación entre un servidor web y un navegador web.

Puerto WAN (Wide Area Network o Red de Área Amplia): Red de ordenadores que se extiende a lo largo de un gran territorio.

Registro de logs: Trazas de datos que nuestro ordenador almacena. Estos datos revelan nuestra actividad dentro de un equipo informático, así como aspectos relacionados con la seguridad y las conexiones.

Reglamento General de Protección de Datos (RGPD): Es una ley de cumplimiento obligado para toda organización que se encuentre en la UE, haga negocio con personas u organizaciones que se encuentren en la UE o se dedique al tratamiento de datos de personas u organizaciones de la UE.

Root o Jailbreak: Se trata de una reprogramación de los ajustes de un teléfono móvil o tablet. De este modo, el dispositivo queda a merced de las modificaciones que le hagamos. En dispositivos Android el proceso de denomina root (raíz) por lo que se dice que el usuario tiene permisos de usuario raíz o superusuario. En el caso de Apple, este mismo proceso se conoce como jailbreak.

Scam: Consiste en hacer creer a la víctima que ha sido ganadora de algún premio, concurso o herencia con el fin de cobrarle una tasa para desbloquear el pago. También se puede emplear para sustraer información confidencial.

Search Engine Optimization (SEO) u Optimización de Motor de búsqueda: Es una disciplina que consiste en aplicar una serie de técnicas tanto dentro (On-Page) como fuera (Off-Page) de una determinada página web, con el objetivo de optimizar su visibilidad en los resultados orgánicos de los diferentes motores de búsqueda.

Service Level Agreement (SLA): Es un contrato entre la empresa que presta el servicio de almacenamiento y su cliente. Se trata de un pacto que fija el tipo de servicio contratado y la calidad del mismo, así como las compensaciones a percibir en caso de que no cumplir el contrato.

Spam: Se basa en el envío masivo de correo electrónico con fines publicitarios o fraudulentos, generalmente por parte de usuarios no conocidos.

Virtual Private Network (VPN) o Red Privada Virtual: Red privada que se crea dentro de otra red para garantizar la privacidad e inaccesibilidad de la conexión a Internet. A las empresas las sirve para, entre otras cosa, establecer conexiones privadas (seguras) entre la oficina y un trabajador que se ubique fuera de la misma, o entre distintas oficinas.

WPA3: Reciente protocolo de conexión segura a redes wifi a través de routers. Progresivamente irá sustituyendo al anterior, WPA2, el cual ha demostrado poseer diferentes vulnerabilidades.