Universidad Zaragoza
1542

Trabajo Fin de Grado

Estrategias de ciberseguridad: el caso de la pequeña y mediana empresa

Cybersecurity strategies: the case of small and medium-sized enterprises

Autora

Carmen Navarro Uriol

Directora

Inés Escario Jover

Facultad de Ciencias Sociales y del Trabajo

2020

ÍNDICE

ÍNDICE DE ILUSTRACIONES

Resumen

En el presente trabajo se señala la importancia que tiene la participación activa de los trabajadores en la ciberseguridad de una empresa. Teniendo en cuenta cómo se encuentra el tema de la ciberseguridad actualmente, se llega a la conclusión de que todas las empresas pueden ser objeto de ataques informáticos. Después de hacer una revisión bibliográfica de diferentes fuentes he observado que hay mucha información sobre el tema, pero muy especializada. Creo que es necesario que esa información pueda ser aplicada a la vida diaria de las pymes. Para ello, me he planteado como objetivo crear una guía pormenorizada que sirva de orientación a los empresarios de las pymes y a cada miembro de la empresa, para que conozcan qué es lo que tienen que hacer en cada momento para mejorar la seguridad de su empresa.

Palabras clave

- Ciberseguridad, PYMES, ataque informático, guía, empleados.

Abstract

This Final Degree Project points out the importance of the active participation of workers in cybersecurity in a company. Taking into account the current state of cybersecurity, it is concluded that every company can be the object of computer attacks. After doing a bibliographic review from different sources, I have observed that there is a lot of information about the subject, but very specialized. It is necessary that this information can be applied to the daily life of SMEs. To do that, I have considered the objective of creating a detailed guide that serves as an orientation for SME entrepreneurs and each member of the company, so that they know what they have to do all the time in order to improve the security of the company.

Key words

- Cybersecurity, SMEs, computer attack, guide, employees.

INTRODUCCIÓN

Actualmente nos encontramos en una globalización de tipo digital. Todos los ciudadanos emplean en su vida diaria las tecnologías de la información. Nos encontramos en la cuarta revolución industrial, los ordenadores forman parte de toda la sociedad y por lo tanto también dentro de las empresas. Las empresas si quieren mantener una posición competitiva tendrán que digitalizarse, y la ciberseguridad es un pilar fundamental.

Una empresa que esté a la última tendrá muchos de sus procesos informatizados, las maquinarias estarán computarizadas y tomarán datos de la nube, esto hace que deba aumentarse la ciberseguridad porque también podrán amenazar a las líneas de producción y sistema industrial de las empresas.

No existen fronteras digitales. Una problemática que preocupa es la delincuencia en el ciberespacio que afecta a todos los sectores de la sociedad. El sector económico de la pequeña y mediana empresa puede ser un blanco fácil si no se toman las medidas oportunas.

Para las pymes, internet, las redes y los sistemas de información, han supuesto un aumento de la posibilidad de negocio y nuevas oportunidades, pero también conllevan muchos riesgos y amenazas. Este riesgo va creciendo exponencialmente en el tiempo, ya que cada vez hay más usuarios y con más conocimientos técnicos.

Los delitos relacionados con la ciberdelincuencia pueden afectar a las pymes. Las amenazas son de dos tipos, contra la información y contra la infraestructura. Las pymes deben concienciarse de que si invierten en ciberseguridad sus beneficios estarán protegidos, ya que se ha constatado que la mayoría de los incidentes de ciberdelincuencia los sufren los ciudadanos y las empresas.

Las empresas necesitan en vez de soluciones puntuales, soluciones integradas, los servicios profesionales deben ser efectivos y los proveedores tecnológicos deben tener como punto importante la seguridad dando soluciones a través de todo el ciclo de su proceso de trabajo.

Al estudiar el Grado de Relaciones Laborales y Recursos Humanos he comprobado la importancia que tienen los empleados en el buen funcionamiento de la empresa. Es importante su selección de acuerdo con el puesto que van a desempeñar y también es importante el grado de compromiso que los empleados adquieren de cara a la empresa. Todos ellos deben tener claro las funciones que tienen que realizar y si el tipo de trabajo conlleva el tratamiento de datos personales utilizando medios informáticos, la empresa está obligada a proporcionarles la información necesaria para realizar el trabajo cumpliendo la legislación vigente. También en el tema de seguridad informática es importante que estén concienciados y motivados por la empresa, hay que evitar que a través de ellos surjan los incidentes de seguridad informáticos, la información es primordial.

Las grandes empresas que tienen un alto poder económico encargan a servicios externos todo el tema de seguridad informática, pero las pymes que tienen menos capacidad para invertir en este aspecto y tampoco conocen la importancia de este tema, porque sus directivos pueden ser autónomos que no tienen conocimientos sobre informática, se encuentran a veces desorientadas, es por lo que he pensado en crear una guía orientativa para ellos, diferenciando la parte en que se ven implicados todos los estamentos de la pyme.

Después de informarme sobre el tema leyendo numerosas publicaciones, veo que lo que se encuentra es todo información muy generalista que no trata temas concretos que les pueden interesar a las Pymes. También existe mucha información que es muy especializada, dirigida a técnicos e ingenieros informáticos y la guía que pretendo hacer es algo más concreto teniendo en cuenta las recomendaciones que dan los organismos oficiales del Estado.

El presente trabajo recoge cómo se encuentra el tema de la ciberseguridad actualmente en nuestro país, cómo se pueden reforzar las medidas de prevención, detección y respuesta y cómo las pymes deben prepararse para ello.

Primero, en el Marco Teórico voy a definir las palabras clave que van a aparecer en el trabajo y señalar los puntos concretos de las leyes vigentes que tratan el tema de la seguridad informática en las empresas.

En el Desarrollo voy a reflejar cómo se encuentra la situación en España y también en Europa y el mundo. También hay una referencia a los Organismo Oficiales que se han creado en España para tratar el tema de la Ciberseguridad.

Finalmente, y como objetivo principal he creado una guía práctica orientativa de los puntos clave de la seguridad en una pyme, para su aplicación por parte del empresario, del técnico informático de la empresa y del trabajador que utilice el sistema informático para el desempeño de su puesto de trabajo. Como he dicho, la colaboración de todo el personal es fundamental para llegar a buen fin.

MARCO TEÓRICO

La Unión Europea definió Pyme (Pequeña y Mediana Empresa) en una Recomendación de la Comisión de la Unión Europea de fecha 6 de mayo de 2003, que publicó en el Diario Oficial de la Unión Europea de 20 de mayo de 2003, como

- **Mediana empresa:** es una empresa que tiene menos de 250 trabajadores, con un volumen de negocio menor de 50 millones de euros o con un balance general anual menor de 43 millones de euros.
- **Pequeña empresa:** tiene menos de 50 trabajadores y su volumen de negocio anual o balance general es menor de 10 millones de euros.

Como ya he dicho en la introducción, la guía que he confeccionado va dirigida a estos dos tipos de empresas ya que han aumentado año tras año el volumen de negocio, lo que les obliga a aumentar sus medidas de seguridad y a conocer los procedimientos adecuados según la legislación vigente.

Antes de pasar a hablar de medidas de seguridad creo conveniente definir seguridad informática y ciberataque para pasar después a conocer los distintos tipos de amenazas informáticas a los que las empresas están expuestas.

- **Seguridad Informática** se define como *"la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad"* (Aguilera López, 2011)

- Se define **Malware** como *"el acrónimo de malicious software, traducido como programas maliciosos y se utiliza para describir los programas tipo virus, gusano, spyware y casi todo el software que está específicamente diseñado para dañar las computadoras, tablets y celulares o para robar la información que los usuarios tienen almacenada en este tipo de dispositivos"* (Andrada, 2017)

- También define **Spyware** como "*todo software instalado en un equipo que recolecta información sin el conocimiento del usuario y la envía al creador del programa para utilizarla con algún propósito perjudicial*" (Andrada, 2017)

- **Scareware** para la citada autora sería, "*el usuario es engañado, aprovechando su desconocimiento específico sobre temas de seguridad informática, para que descargue una aplicación que simula ser un antivirus que remueve un virus ficticio instalado previamente en el ordenador y que realiza tal acción sólo si se paga el costo de una licencia. Si la licencia no se paga, el programa "antivirus" instalado no se puede desinstalar y en algunos casos tampoco se puede utilizar de nuevo el ordenador".* (Andrada, 2017)

- **Amenaza** *"todo elemento o acción que pueda ocasionar daños. En el contexto informático, una amenaza podría estar dirigida a usuarios, a hardware o a datos"*. (Chaos García, y otros, 2017)

- **Vulnerabilidad** "*debilidad y por tanto es cualquier elemento o acción que no se haya protegido contra una posible amenaza*" (Chaos García, y otros, 2017)

- **Contramedida** "*cualquier elemento o acción para evitar una amenaza con el fin de proteger a usuarios, hardware o datos*". (Chaos García, y otros, 2017)

- **Phishing** "*suplantación de identidad, El pirata informático roba cualquier información del usuario como una palabra clave de una red social que utilice el usuario, un número secreto de su tarjeta de crédito o cualquier dato bancario que le identifique y le permita suplantarle*" (Chaos García, y otros, 2017)

Referente al tema de Protección de Datos, el diccionario del español jurídico define los términos que indico a continuación de la siguiente forma:

Protección de Datos, "*Conjunto de medidas para garantizar y proteger los datos de carácter personal (cualquier información concerniente a personas físicas identificadas o identificables) registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado, a los efectos de garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar."* (Diccionario del Español Jurídico, 2016)

Tratamiento de datos personales*, "conjunto de operaciones o procedimientos técnicos, automatizados o no, que permiten la recogida, registro, organización, conservación, adaptación o modificación, extracción, consulta, utilización, difusión o cualquier otra forma que facilite el acceso a los datos personales, cotejo o interconexión, así como su bloqueo, supresión o destrucción".* (Diccionario del Español Jurídico, 2016)

REFERENCIAS LEGISLATIVAS:

Sobre sistemas de comunicaciones

- **Constitución Española Artículo 18.3:**" *garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.".*
- **Artículo 2.2 de la Ley Orgánica 1/1982**: *"protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen establece que no se apreciará la existencia de intromisión ilegítima en el ámbito protegido cuando estuviere expresamente autorizada por Ley o cuando el titular del derecho hubiere otorgado al efecto su consentimiento expreso.".*

Sobre confidencialidad de datos informáticos:

Ratificación del Convenio sobre Ciberdelincuencia de Budapest de 2001, BOE de 17 de septiembre de 2010, capítulo II, artículos del 2 al 6, (Confidencialidad) y artículos 7 y 8 (Delitos informáticos)

Sobre protección de datos:
Ley Orgánica 3/2018 de protección de datos: destacamos los siguientes artículos.
Artículo 12.2 "*El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser*

fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio"

***Artículo 5**. "Deber de confidencialidad*
1. Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.
2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.
3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento".

***Artículo 82**. "Derecho a la seguridad digital*
Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos".

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

La necesidad de incorporar los nuevos delitos informáticos en nuestro Código Penal a través de la reforma de **Ley Orgánica 1/2015**, viene dada por la adopción de la Directiva Europea 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, y por la que se sustituye la Decisión Marco 2005/222/JAI del Consejo.
Los cambios sufridos tratan de dar una respuesta legal, desde la perspectiva del derecho penal, a la delincuencia informática**.**

En el caso en que la pyme hubiera diseñado algún producto, puede existir un delito tipificado en los artículos 270, 271 y 272 del Código Penal, si se produjera algún robo o traspaso de información conseguido a través del acceso ilegal al sistema informático de la empresa.

En este sentido, los delitos contra los sistemas de información introducidos y modificados por la **Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995 de 23 de noviembre, del Código Penal, son los que a continuación detallan**:

En el artículo 106 de la Ley Orgánica 1/2015 que modifica el artículo 197 del CP, se describe el delito que supone la intercepción de comunicaciones y revelaciones de secretos que también podría ocurrir en una pyme.

*"**106.1** El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses."*

*"**106.2** Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero."*

Se crea un nuevo artículo, el **197 bis**, que dice textualmente:
"*El que, mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses*". De esta forma, serán objeto de castigo no únicamente la interceptación de comunicaciones personales, recogidas ya en el CP, sino que, a la vez, todas las que se produzcan entre sistemas o equipos.

Además, también se añade el artículo **197 ter CP** considera que serán castigados todos aquellos que:
"*sin estar debidamente autorizados, produzcan, adquieran para su uso, importen o, de cualquier modo, faciliten a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:*
a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos
b) Una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información".

En los nuevos artículos **264 a 264 quáter del CP** se tratan delitos de daños y delitos de interferencia ilegal en sistemas de información o datos.

CIBERSEGURIDAD: SITUACION Y LEGISLACIÓN

SITUACIÓN DE LAS PYMES ESPAÑOLAS Y CIBERSEGURIDAD

Según el estudio que ha recogido el Observatorio del Sector Público de IECISA (OSPI) actualizado a 2019, realizado por The Cocktail analysis, las pymes españolas no se consideran a sí mismas como un blanco para el ataque informático (The Cocktail analysis, 2019, p.25).

Ilustración 1 Destinatarios ataques cibernéticos (INCIBE,2019). Recuperado de The Cocktail Analysis, 2019, p.29

En la Ilustración 1 se observa que la mayoría de los ataques van dirigidos a empresas de cualquier tamaño y particulares.[1]

Según un estudio realizado por (The Cocktail analysis, 2019) encargado por Google, en Europa se considera que el 60% de las pymes que han sufrido un ciberataque suelen cesar en su actividad seis meses después porque no pueden superar la pérdida económica que ronda los 35.000 euros.

La tecnología ha contribuido a que el negocio de las empresas haya crecido; es por lo tanto muy importante que la información que generan las empresas de cualquier tipo esté protegida, sobre todo en las pequeñas y medianas empresas, que son más vulnerables, por lo que es necesario que apliquen sistemas de seguridad.

Este tipo de empresas son las más afectadas por robos de información debido a que no poseen mecanismos de control, los cuales, si se aplicaran, reducirían la posibilidad de ser víctima de los desaprensivos.

Pueden ser que las pymes no desarrollen sistemas de seguridad, porque tienen pocos recursos económicos y los gastos en seguridad no los pueden asumir. También puede ser que estas empresas no tengan suficiente información ni conocimientos sobre este tema. A ellos les interesa aumentar ventas y negocio por lo que se tienen que dar cuenta, que invertir en resguardar y proteger la información de sus empresas, a la larga, también aumentará su beneficio.

[1] https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

El crecimiento de las pymes favorece la creación de empleo, ya que son ellas las que mantienen en cierto modo la economía local. Los propietarios de las pymes pueden pensar que no son blanco de los ciberdelincuentes porque su volumen de ganancias no es alto, pero en la realidad se observa que eso no es cierto ya que sufren muchísimos ataques.

Los directores de estas empresas deberían ser los responsables de tomar decisiones sobre el aspecto de la seguridad.

Las empresas si quieren mantener una posición competitiva tendrán que digitalizarse, y la ciberseguridad es un pilar fundamental. Todas las maquinarias estarán dirigidas por medios informáticos y tomarán datos de la nube, esto hace que deberá aumentarse la ciberseguridad porque también podrán amenazar a las líneas de producción y el sistema industrial de las empresas.

Hay una batalla entre las empresas de seguridad informática y los cibercriminales. Las empresas por lo tanto tienen que dar soluciones rápidas. Las empresas necesitan, en vez de soluciones puntuales, soluciones integradas. Los servicios profesionales deben ser efectivos y los proveedores tecnológicos deben tener como punto importante la seguridad, dando soluciones a través de todo el ciclo de su proceso de trabajo.

LA CIBERSEGURIDAD EN EUROPA Y EL MUNDO

Para poder comparar la seguridad conseguida entre los diferentes países se utiliza un indicador que es el ICG, este índice es el que se utiliza en las ilustraciones 2 y 3. La definición oficial de este indicador es: *"El Índice de Ciberseguridad Global (*Global Cibersecurity Index - GCI*) es una iniciativa de la Unión Internacional de Telecomunicaciones (*UIT*). Se trata de un índice compuesto para medir el compromiso de los Estados Miembros de la UIT, 194, con la ciberseguridad."* (Portal de Administración Electrónica del Gobierno de España, 2019).

En la ilustración 2, se ven los cinco aspectos que estudia:

- Aspecto legal: si el país tiene establecido un marco legal relativo a ciberseguridad y ciberdelito.
- Aspecto técnico: si tienen medidas técnicas para poder aplicar.
- Aspecto organizativo: Si poseen una organización con estructuras establecidas para poder llevar a cabo la ciberseguridad dentro del país.
- Aspecto de creación de capacidades: Si el país fomenta la investigación en este tema si proporcionan el conocimiento a sus habitantes mediante cursos, títulos profesionales y si la Administración pública emite certificados que demuestren la capacitación.
- Aspecto de cooperación: Si dentro del país tienen intercambio de información, asociaciones, para favorecer que el conocimiento sobre ciberseguridad llegue al mayor número de personas posible.

Y lo que vamos a medir es:

- Cómo ha variado la actuación del país respecto a fomentar la ciberseguridad dentro del país correspondiente y relacionándose con otros países.
- Cómo ha avanzado la cooperación entre países para que la protección en ciberseguridad se vaya extendiendo a todo el planeta.

- Los progresos desde el punto de vista regional respecto a la ciberseguridad.
- Las diferencias que existen entre países respecto a formar parte en iniciativas de ciberseguridad.

Los índices que aparecen en la ilustración 2 y 3 corresponderían a un baremo de tres niveles:

Nivel alto, correspondería a una puntuación entre 1 y 0,67.
Nivel medio, correspondería a una puntuación entre 0,66 y 0,34.
Nivel bajo, correspondería a una puntuación entre 0,33 y 0.

Como podemos observar en las ilustraciones 2 y 3 los países que se han incluido en esta tabla corresponden al nivel alto de la puntuación ICG. En aspecto técnico España tiene menos puntuación que Malasia, Noruega o Canadá.

Ranking	Paises	ICG	Legal	Técnico	Organizacional	Creación de capacidades	Participación en iniciativas
1	Reino Unido	0,931	0,200	0,191	0,200	0,189	0,151
2	EEUU	0,926	0,200	0,184	0,200	0,191	0,151
3	Francia	0,918	0,200	0,193	0,200	0,186	0,139
4	Lituania	0,908	0,200	0,168	0,200	0,185	0,155
5	Estonia	0,905	0,200	0,195	0,186	0,170	0,153
6	Singapur	0,898	0,200	0,186	0,192	0,195	0,125
7	España	0,896	0,200	0,180	0,200	0,168	0,148
8	Malasia	0,893	0,179	0,196	0,200	0,198	0,120
9	Noruega	0,892	0,191	0,196	0,177	0,185	0,143
10	Canada	0,892	0,195	0,189	0,200	0,172	0,137

Ilustración 2 Los 10 países que tienen más compromiso con la ciberseguridad. Recuperado de Portal Administración Electrónica. [2]

En la Ilustración 2, que corresponde al año 2018, podemos observar que España está en séptimo lugar del Ranking del Índice de Ciberseguridad Global, dentro de la clasificación mundial. Con un 0,896 de puntuación ICG.

[2] https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio-2019/Abril/Noticia-2019-04-24-Espana-7-puesto-Global-Cibersecurity-Index-2018.html

EUROPA			
Paises	Puntuación	Clasificación Europa	Clasificación Global
Reino Unido	0,931	1	1
Francia	0,918	2	3
Lituania	0,908	3	4
Estonia	0,905	4	5
España	0,896	5	7
Noruega	0,892	6	9
Luxemburgo	0,886	7	11
Paises Bajos	0,885	8	12
Georgia	0,857	9	18
Finlandia	0,856	10	19
Turquia	0,853	11	20
Dinamarca	0,852	12	21
Alemania	0,849	13	22
Croacia	0,84	14	24
Italia	0,837	15	25
Austria	0,826	16	28
Polonia	0,815	17	29
Belgica	0,814	18	30

Ilustración 3 Situación de España respecto a Europa y el mundo. Recuperado de Portal Administración Electrónica. [3]

En la Ilustración 3, donde se estudia la posición respecto a Europa, se observa que España está en quinto lugar. Es una buena posición teniendo en cuenta que países con PIB mayor que el de España, como Alemania, está por detrás en el tema de ciberseguridad.

[3] https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio-2019/Abril/Noticia-2019-04-24-Espana-7-puesto-Global-Cibersecurity-Index-2018.html

Ilustración 4 Incidentes que hizo frente Centro Criptologico Nacional- Computer Emergency Response Team. Recuperado de The Cocktail Analysis, 2019, p.32

En la **¡Error! No se encuentra el origen de la referencia.** se puede ver que el porcentaje i ntrusiones es muy alto con un 59%, y también que las políticas de seguridad son todavía muy bajas de un 3%.[4]

Un dato contrastado es que cada día aumentan más las conexiones en la web, por lo que los datos deberían estar cifrados.

Una acción de seguridad muy importante es que se aplique el segundo factor de autentificación, pero en la actualidad sólo llega al 28%, donde se usa bastante este sistema de seguridad es en la banca online.

Algo que todas las empresas españolas deben tener en cuenta es que existe una necesidad de intercambiar información sobre amenazas e incidentes informáticos para poder prever ciberataques. Así se podría mejorar la respuesta.

Respecto a la legislación sobre comunicación de incidentes, en España tenemos la Directiva 2002/58/CE que dice “los proveedores de servicios de comunicaciones electrónicas disponibles para el público están obligados a notificar las quiebras de seguridad que puedan afectar a datos personales a las autoridades competentes y en algunos casos también a los particulares afectados”.

En España la Agencia Española de protección de Datos es quien recibe las comunicaciones por parte de los proveedores.

A nivel más amplio, como las amenazas son globales, la colaboración también tiene que sobrepasar los estados. Los estados deben pasarse información sobre incidentes informáticos.

[4] https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

NECESIDAD DE CONTRATAR SEGUROS QUE CUBRAN LOS ATAQUES INFORMÁTICOS

Los ciber riesgos ya no son esporádicos, son un problema importante, por lo que hasta existen los ciberseguros que atenderán a las empresas ante un incidente de seguridad.

Este campo de los seguros está aumentando año tras año.

Muchas empresas piensan que por su tamaño no están en el punto de mira de los ciberdelincuentes, pero la realidad es que, aunque de las empresas pequeñas obtengan menos beneficios, también el esfuerzo que les supone atacarlas también es menor. Para compensar repiten los ataques sobre muchas pequeñas empresas.

Para la empresa afectada, el coste medio es de 35.000€, pero si la empresa no tiene protección adecuada le puede acarrear el cierre. Por eso actualmente se ofrecen ciberseguros que les dan seguridad jurídica y también económica.

Con la póliza de seguro, estarían cubiertos en el tema de recuperar datos, cambios de software, responsabilidad civil frente a terceros y si tienen pérdida de beneficios también les compensarían.

El precio de la prima según los servicios que ofrezcan puede variar entre 350 y 150.000 euros al año.

LEGISLACIÓN

- Ley 34/2002 de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico
- Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales
- Reglamento General de Datos de la Unión Europea.
- Con la directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de la Unión Europea de 6 de julio de 2016.

ORGANISMOS OFICIALES RELACIONADOS CON EL TEMA DE CIBERSEGURIDAD

- **EL CONSEJO NACIONAL DE CIBERSEGURIDAD (CNCS)**

  Constituido desde el 24 de febrero de 2014 por decisión del Consejo de Seguridad Nacional. Forman parte de él representantes de los ministerios españoles que tiene competencias en ciberseguridad. Su fin es llevar a cabo los cometidos que indica la Estrategia Nacional de seguridad desarrollando las líneas de acción.

- **EL SERVICIO DE INTELIGENCIA DE ESPAÑA (CNI)**
  Facilita al gobierno las decisiones estratégicas que tome sobre ciberseguridad. Obtiene información sobre ciberamenazas tanto dentro de España como fuera, ya que tiene intercambios de información sobre este tema con otros Servicios de inteligencia del extranjero.

- **LA OFICINA NACIONAL DE SEGURIDAD (CNS)**
  Colabora respecto a la información clasificada, para que haya protección de la misma.

- **CENTRO CRIPTOLÓGICO NACIONAL (CCN-CERT)**

  Su labor es importante ya que son los que cuando hay un incidente o alerta dan respuesta, trabajan en la Administración Pública y las empresas de alto valor estratégico.

  Han creado un sistema de alerta temprana. Reducen el impacto detectando la incidencia los más pronto posible.

GUÍA DE RECOMENDACIONES SOBRE CIBERSEGURIDAD PARA UNA PYME

Esta guía ha sido creada por mi después de leer la variada información que existe sobre el tema, y de comprobar que no había un texto donde hubiera una recopilación de puntos a tener en cuenta concretamente, para utilizarlos como base para su aplicación en una media o pequeña empresa. Está dividida en tres partes teniendo en cuenta el grado de responsabilidad dentro de la empresa y el trabajo real que realiza cada uno. He diferenciado entre orientaciones para el empresario, para el trabajador y para el personal técnico.

Las indicaciones del apartado para el "personal técnico", serían para el empleado con conocimientos especializados que se dedique a ello, si la pyme no ha contratado externamente este servicio, el director de la pyme deberá indicar cuál es el trabajador de la empresa que debe realizarlo, sino es el mismo.

ORIENTACIONES PARA EL EMPRESARIO:

- Gestión de recursos humanos

Dentro de la seguridad en una empresa, la parte clave es el empleado, ya que es el protagonista del error humano, al cual se deben la mayoría de los problemas de seguridad.

Cuando se selecciona una plantilla hay que tener en cuenta el tema de ciberseguridad, sería conveniente realizar pruebas para contratar a las personas con más conocimientos en estos temas.

- Cláusulas contractuales: En los contratos que debe firmar el empleado tiene que haber unas cláusulas que deberán firmar en referencia con la ciberseguridad. Aquí se señalará claramente las leyes de propiedad intelectual y de datos de carácter personal, y se establecerán responsabilidades.

-Acuerdos de confidencialidad: También deberemos llegar a un acuerdo de confidencialidad, respecto al acceso a la información. La deben firmar trabajadores y colaboradores. El contenido de estos acuerdos tratará sobre:

- Partes que intervienen
- Qué tipo de información es confidencial
- Compromisos de ambas partes
- Legislación aplicable y posibles sanciones

- Revisar las referencias de los candidatos: Para los puestos de manejo de información muy confidencial se debe hacer un estudio de su experiencia en otras empresas y ver las referencias que presentan antes de contratarlos. Hay que comprobar si los datos que aparecen en el curriculum del potencial empleado son ciertos, y si el puesto requiere el manejo de información muy sensible se les puede pedir un certificado de que no tienen antecedentes penales.

- Plan de formación y concienciación en ciberseguridad: La empresa debe tener un plan de formación y concienciación respecto a seguridad. Los cursos deben ser realizados de vez en cuando.

- Política de sanciones: Se deberá informar claramente al personal de la política de sanciones que se llevarán a cabo con los que no traten con seguridad la información de la empresa, explicando claramente cuando se pueden abrir expedientes que conlleven el despido.

- Finalización del contrato: Explicar a los trabajadores la obligación que tienen con la información sensible de la empresa cuando ya no trabajen para ella.

- Concesión autorizada de los permisos de acceso: El empresario tiene que tener claro qué permisos concede a cada puesto, para que solo pueda acceder a la información que nos interese.

Es conveniente, dar tarjetas de acceso físico a la empresa, asignarle unas cuentas de correo electrónico, y cuando se asigne un puesto trabajo, asignar también los equipos y dispositivos que le correspondan

- Revocación de permisos de acceso: No olvidarse de revocar los permisos de accesos de todo el personal dado de baja en la empresa. También se debe recoger la tarjeta de acceso y los dispositivos que les habían entregado, así como eliminar las cuentas de correos.

- Aprovechamiento de las sesiones formativas: Después de realizar sesiones formativas para los empleados, hacer algún tipo de prueba para comprobar si lo ha aprovechado.

➢ Almacenamiento en la red corporativa

El almacenamiento en la red es importantísimo para depositar tanto los trabajos individuales de los empleados como para la información de la empresa que deben utilizar todos. Hay que diferenciar este tipo de información y el responsable de sistemas informáticos, siguiendo las directrices del empresario, será quien limite los trabajadores que pueden acceder a según qué lugares de la red.

Hay que conseguir que los trabajadores utilicen correctamente los servidores de almacenamiento. Los empleados tienen que concienciarse que almacenando la información en un lugar centralizado:

- Se evitan duplicidades y varias versiones del mismo tema
- Se evitan pérdidas de documentos
- Se comparte información que puede servir a todos los empleados con vista a nuevos proyectos y emisión de documentos.

La política de seguridad tiene que contemplar:

- **Inventario de los servidores de almacenamiento**: Es deber del empresario dar la siguiente información a los empleados:
  - Número de servidores de almacenamiento existentes
  - Aclarar que qué datos deben almacenarse en ellos
  - Responsabilidades
  - Formar a los nuevos empleados sobre este tema.
  - Refrescar de vez en cuando esta información sobre los servidores.

- **Criterios de almacenamiento:** El empresario debe crear una normativa con información referente a este tema, donde se explique:

  - Tipo de información que se debe o no almacenar.
  - Quiénes son los trabajadores que tienen acceso a esa información
  - Quién tiene que actualizarla si se da el caso de que hay que modificarla.
  - Informar de cuál es el momento oportuno en que se debe borrar la información por obsoleta.

- **Clasificación de la información:** Respecto a la política de la empresa en cuanto a clasificación de la información en el momento de almacenarla, el trabajador debe conocerla perfectamente para que haga su trabajo correctamente.

- **Control de acceso:** Es importante que existan unas reglas de acceso para poder controlar a los trabajadores en el momento de acceder a los sistemas de almacenamiento.

- **Copias de seguridad:** El empresario tiene que pensar en un plan de copias de seguridad donde:
  - Se diga qué información se debe guardar con copia de seguridad
  - Cada cuánto tiempo se hacen las copias de seguridad
  - Se debe designar dónde se guardan las copias
  - Cuánto tiempo se deben conservar las copias de seguridad

- **Acceso limitado:** Hay que definir unos perfiles de acceso, teniendo claro que actividad realiza cada empleado entonces se le asignará un perfil para que sólo pueda acceder a la parte del directorio que le corresponda.

- **Almacenamiento clasificado:** Se deben crear carpetas para que los empleados guarden la documentación en la carpeta que corresponda. Cada empleado tendrá el permiso correspondiente.

- **Cifrado de la información:** La información importante que se almacene en la red deberá ser cifrada.

- **Auditoría de servidores:** Hay que revisar periódicamente el uso que se hace de los servidores, si están llenos o no, por si hay que crear alguno nuevo.

➢ Almacenamiento en los equipos de trabajo

La información que es generada por los trabajadores en su puesto de trabajo, también es necesario guardarla en los discos duros de los equipos. La empresa tiene que dar unas pautas de seguridad respecto a este tema.

- La empresa debe indicar a los empleados cuál es el tipo de información que se puede guardar en los equipos de trabajo personal. Hay información personal del trabajador como fotografías, música o documentos de índole personal, que no debe almacenarse.

- Cuando descarguen algún documento, el trabajador debe comprobar que no tenga derechos de autor, para no incumplir ninguna ley.

- La empresa debe detallar en qué zona del directorio del equipo debe guardar la información que genere por su trabado diario.

- Como los discos duros se pueden llenar, hay que establecer un periodo de tiempo para conservar la información dentro del disco duro, y pasado ese tiempo señalar si se borra la información o se transfiere a algún servidor concreto de la empresa.

- Después de haber transferido la información a algún servidor externo, se deberá mantener la información en el disco duro del empleado el tiempo que estime conveniente la empresa y posteriormente se procederá a su borrado para no duplicar información innecesariamente.

- El empleado debe conocer la técnica de cifrado de información y sobre todo en qué casos debe utilizarla.

- Toda la política de la empresa relativa al tema de almacenamiento de información en los equipos debe ser conocida por todos los trabajadores.

➢ Almacenamiento en la nube

La importancia de almacenar en la nube se deriva de que de esta forma se puede acceder a la información desde cualquier lugar:

- También se ahorran recursos
- Se pueden compartir directorios
- Permite que sobre un mismo documento puedan trabajar varias personas.

La pyme deberá tener una buena conexión a internet para implantar este sistema, además deberá establecer una política que trate sobre:

- Es el empresario quien debe decidir si se utiliza la nube pública. El empleado no puede usarla si no lo permite la empresa.
- La empresa debe crear un listado con los servicios de almacenamiento en nube que se permiten porque los considera seguros.
- La política que se utilice para decidir cuándo se borra información, también se aplicará al borrado de información en la nube.
- Se debe informar correctamente al empleado para que sepa en todo momento qué información puede almacenar en la nube y cuándo la tiene que cifrar.
- Si las copias de seguridad se hacen en la nube se tiene que valorar previamente las ventajas e inconvenientes de este sistema:

- **Ventajas:**
    - En la nube hay más espacio para las copias de seguridad
    - Los servicios de la propia nube como garantía realizan copias de seguridad
    - Utilizando la nube, la empresa se asegura de tener una copia fuera de la empresa por si hay algún incidente que destruyera equipos informáticos

- **Inconvenientes:**

  Si dependemos de terceros tenemos que asumir que también ellos pueden tener incidentes que nos pueden afectar

  Respecto a la contratación de un servicio de almacenamiento en nube, el empresario se tiene que asegurar de que la empresa de almacenamiento ofrece garantías en cuanto a copias de seguridad, confidencialidad y disponibilidad. Y también que cumplan la legalidad en cuanto al tratamiento de datos personales.

  Para ello es importante que el proveedor nos informe de su política de seguridad.

➢ Aplicaciones informáticas permitidas por la empresa

Todas las empresas deben utilizar un software legal. El utilizar software pirata conllevaría sanciones que, según la Ley, pueden ser económicas y penales.

También hay que tener en cuenta que es un riesgo para la seguridad, instalar en los equipos software ilegal, porque pueden generar una infección por malware.

En la política de la empresa tiene que tener en cuenta los siguientes puntos:

- Registro de licencias: La empresa tiene que llevar un registro detallado y actualizado de las licencias de los programas que utiliza. En ese registro tiene que reflejarse:
  - Nombre y versión del producto
  - Autor
  - Fecha de adquisición
  - Vigencia de la licencia
  - Número de usuarios permitidos por licencia
  - Número de licencias compradas por cada software
  - Facturas de la compra, por si hay que presentarlas en alguna inspección
  - Señalar dónde se encuentra guardado físicamente el producto.
- Respecto a designar la persona que debe instalar el software, así como su actualización y borrado, cabe reseñar que lo más adecuado sería que la empresa tuviera personal técnico que se dedicara a ello, si no lo tiene y se contrata algún servicio externo, es siempre la empresa la que debe dar autorización previa para que se realicen los trabajos de instalación, actualización y borrado.

  Siempre se debe usar una cuenta de administrador que sea diferente a la de un usuario habitual.

- La empresa no debe permitir que se instalen o actualicen programas a través de descargas de páginas web de las que no se tenga constancia de su seguridad. Es muy importante que el software esté actualizado.

- Para concienciar a la plantilla de que no utilicen software no autorizado se debe avisar que teniendo en cuenta la legislación de protección de la propiedad intelectual, la empresa impondrá sanciones a los trabajadores que incumplan esta normativa interna, además de que puede conllevar responsabilidad civil y penal.

- Sobre el repositorio de software se debe determinar exactamente dónde estará ubicado para que el personal pueda acceder, todo el personal que acceda debe quedar registrado por si ocurre algún incidente. En ese lugar es conveniente que estén también las claves de activación, licencias, números de serie

- La empresa debe avisar a los trabajadores de que en cualquier momento puede hacer una inspección de los equipos de trabajo personal, para ver que se cumple la normativa en cuanto a utilización de software oficial.

- Los trabajadores deben leer y comprender las condiciones de las licencias de uso del software instalado para que cumplan con la Ley de Propiedad Intelectual.

- Sobre el tema de realizar copias del software, la empresa debe hacer entender claramente a los empleados que no se pueden hacer copias del software sin consentimiento.

➢ Necesidad de clasificación de la información

La empresa debe proteger la información, ya que es uno de los activos más importante de ella.

Esta información puede estar en variados soportes:

- Formato digital
- Papel
- Película fotográfica

Dentro del formato digital la información puede estar guardada en ficheros:

- De texto
- De imagen
- Multimedia
- Bases de datos

Lo primordial antes de aplicar las medidas de seguridad es confeccionar un inventario y hacer una clasificación respecto a la importancia que tendría de cara a la empresa si hubiera una pérdida de información o accediera alguien no autorizado.

Para protección se tendrá que indicar que criterios de confidencialidad se aplican, para saber quién tiene acceso, quién es responsable de su seguridad y la periodicidad en la cual hay que hacer una copia de seguridad.

Por ejemplo:

- El contenido de las nóminas al ser confidencial, sólo pueden tener acceso a él algunos empleados concretos.
- A la página web es conveniente que sólo acceda quien decida el empresario, puede ser por ejemplo el departamento de marketing.
- Los documentos que se envíen fuera de la empresa por correo electrónico a una gestoría, por ejemplo, tendrían que estar cifrados.

Es fundamental decidir en el momento en el que clasifiquemos los archivos, la duración de su ciclo de vida, que dependerá de la vida útil del soporte y del contenido del mismo en referencia a su vigencia.

En el momento de que alguna información deja de ser útil, lo más conveniente es eliminarla.

Los puntos clave que debe tener la empresa respecto a este tema son:

- **Crear un inventario de la información**: Teniendo en cuenta tamaño del archivo, dónde está ubicado, quién es su responsable, servicio al que pertenecen.
- **Criterios de clasificación relacionados con las medidas de seguridad**:
    - **Según nivel de accesibilidad o confidencialidad**
        - Confidencial: Sólo puede acceder o el director de la empresa o personal concreto
        - Interna: Para acceso del personal de la empresa
        - Pública: Puede acceder todo el mundo.
    - **Por su utilidad o funcionalidad**
        - Información sobre personal y gestión interna
        - Información de compras y ventas
        - Información para clientes y proveedores
        - Información sobre pedidos y procesos de almacén
    - **Por el impacto que crearía su robo, pérdida o borrado**
        - Que se produzca daño de imagen
        - Consecuencias en la economía de la empresa
        - Consecuencias teniendo en cuenta la legalidad
        - Que se llegue a parar la actividad por el hecho de pérdida de información
- **Clasificación de la información**:
    - Se le atribuirá una etiqueta informativa a cada archivo de información según esté encuadrado en la clasificación.
    - Hay que elaborar un listado con tratamientos referentes a seguridad informática que tiene la empresa, como
        - Sistema de copias de seguridad
        - Sistema de control de accesos
        - Herramientas para realizar cifrado.
- **Cuando ya se tenga clasificada la información, hay que asignar los tratamientos que estarían indicados para cada tipo de información.**

  Los tratamientos podrían ser estos:
    - Sistema que limite el acceso a ciertas personas o grupos
    - Proceder al cifrado de información
    - Generar copias de seguridad
    - Controlar y designar a los trabajadores que puedan acceder a la información o modificarla.

- **Realización de auditorías**. Es muy necesario efectuar con periodicidad auditorías de seguridad, para realizar una certificación que demuestre el que se han realizados los tratamientos que la empresa ha asignado.

➢ Formar y enseñar a los empleados

En la actualidad casi todas las pymes utilizan las nuevas tecnologías, es por lo tanto necesaria la concienciación de los empleados sobre el riesgo que lleva la utilización de estas tecnologías.

Las buenas prácticas son indispensables en cuanto a la utilización de todos los dispositivos y servicios informáticos, como redes sociales, correo electrónico, la nube etc. El empresario por lo tanto tiene el deber de facilitarles la formación sobre ciberseguridad adecuada al puesto que desempeñen. De esta forma los incidentes informáticos se pueden prevenir.

El empresario debe tener en cuenta los siguientes puntos:

- Tiene que haber una correcta difusión de la política de seguridad, todas las normas referentes a seguridad tienen que ser accesibles a todos los trabajadores en cualquier momento.
- Es necesario concretar el plan formativo que se va a llevar en la empresa que debería contener los siguientes apartados:
    - Es interesante que se aborde el tema de controles de seguridad básicos y procedimientos a seguir.
    - Es recomendable que se conozcan las leyes, normas y reglamentos.
    - Se tratará también de la seguridad aplicada al puesto de trabajo, para que tengan conocimiento claro de las aplicaciones permitidas, como utilizar correctamente los recursos. Será interesante que tengan una visión general de la Ley de Protección de datos personales y de propiedad intelectual.
    - Las explicaciones del plan de formación deben favorecer que los empleados se den cuenta de los peligros actuales en cuanto a ciberseguridad.
    - Hay que informar de las sanciones que serán impuesta si no se cumplen las normas.

- En la formación que se imparte se debe diferenciar la que va dirigida a nuevos empleados, de la que recibirá el personal que trabaje en puestos más especializados en temas informáticos y por lo tanto su contenido será más técnico.

- La formación y los cursos de concienciación deben ser periódicos, así los contenidos estarán actualizados en cuanto a ciberseguridad y se podrá insistir en los puntos más débiles y reforzar los mensajes más importantes.

- Además de concienciar a los empleados de la empresa, también hay que pedir a nuestros clientes o empresas externas que colaboran con la nuestra, que también tengan políticas de seguridad acordes con la nuestra.

- Es interesante realizar evaluaciones a los empleados para comprobar el nivel de concienciación y formación que han conseguido.

➢ Cumplimiento de leyes relacionadas con ciberseguridad

Toda empresa que realice su trabajo a través de internet utilizando la tecnología actual, tiendas online, redes sociales, debe conocer y cumplir la legalidad vigente en cuanto al uso de las citadas tecnologías.

Dentro de la ciberseguridad y para proteger a los usuarios hay una regulación concreta sobre temas de privacidad, firma electrónica, comercio electrónico referido a los consumidores y propiedad intelectual. Existe una revisión constante de las leyes relacionada en todo momento con los cambios del mundo globalizado y la tecnología actual.

Algunas leyes que toda empresa debe conocer son:

- Ley de Propiedad Intelectual (LPI), tanto en formato digital como tradicional, regula derechos sobre la producción artística, literaria, científica.

- Reglamento europeo de protección de datos (RGPD) su fin es la protección de la privacidad de personas sobre todo en comunicaciones electrónicas referente a sus datos.

- Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE), trata sobre la reglamentación jurídica de la actividad referida al comercio electrónico, la información, los contratos realizados en línea e intermediación.

- Leyes de Propiedad Industrial para proteger la marca o nombre comercial de la empresa, los diseños industriales, y también las patentes.

- Reglamento europeo de identificación electrónica y servicios de confianza en el mercado interior, que sirve para el público tenga confianza en la utilización de transacciones electrónicas.

Detalles a tener en cuenta:

- La empresa debe tener claro qué procedimientos utiliza en su trabajo diario para saber si cumple con la legislación vigente, sobre todo lo referido a la información.

- Hay que garantizar sobre todo los derechos de propiedad intelectual de personas ajenas a la empresa para ello
    - Hay que concretar para que lo conozcan todos los miembros de la empresa, la forma correcta de comprar software legal, cómo usarlo, copiarlo o eliminarlo dentro de la legalidad.
    - Si tenemos contratos mercantiles que nos permitan utilizar documentos o información que generen derechos de propiedad intelectual, debemos tener un registro de ellos.
    - Informar al personal de la empresa, el tipo de sanciones que se impondrían si utilizara software no autorizado.

- Respecto a las creaciones de la propia empresa hay que exigir a los empleados mediante contrato por escrito el que cumplan los derechos de propiedad intelectual de la empresa.

- Si la empresa realiza transacciones comerciales con algún país de la Unión Europea, o utiliza datos personales de alguna persona con residencia en la UE, se tiene que cumplir respecto a la seguridad unas normas, según el RGPD. La empresa debe en todo momento poder demostrar que se cumple la legislación sobre privacidad si se lo requieran.

- Dentro de la empresa se tiene que **definir claramente qué puesto se encarga del tema de protección de datos personal:**
    - Habrá un responsable del tratamiento de datos, que determinará los fines del citado tratamiento
    - También existirá un encargado del tratamiento que realizará el tratamiento de los datos. Deberá firmar un contrato.
    - Para las empresas grandes o con gran cantidad de datos a tratar, es obligado contar con un Delegado de Protección de datos, que puede ser un empleado de la empresa o no pertenecer a la misma. Puede asesorar, informar y coordinar sobre el tema.

- **Para que puedan ejercitar sus derechos es de obligado cumplimiento informar a los interesados:**
    - Tiene que informarse mediante una forma accesible, visible y sencilla.
    - El interesado tiene dar consentimiento expreso.
    - Los interesados deben poder ejercitar de forma no complicada sus derechos
    - Si ha existido algún problema de ciberseguridad en el que ha habido datos afectados, hay que avisar a las autoridades y a los interesados mediante notificación.
- Si la empresa trata datos de categoría especial, hay que hacer una evaluación de impacto.

- Si la empresa tiene más de 250 empleados o se tratan datos de alto riesgo, la empresa debe tener un registro de actividades referidas al tratamiento.

- Como hay obligación de notificar en un plazo de 72 horas a las autoridades los incidentes respecto a seguridad que estén relacionados con la privacidad de las personas, la empresa debe tener claro el procedimiento que utilizará para cuando ocurra.

- **El empresario tiene que organizar su personal para que:**
    - Se cumpla el Reglamento de Protección de Datos
    - Poder garantizar a los interesados el ejercicio de sus derechos.
    - Todo el personal de la empresa que trabaje en tratamiento de datos personales reciba la adecuada formación.

- **La aplicación de medidas de seguridad es fundamental. Respecto a los datos es conveniente:**
    - Hay que clasificarlos, sabiendo dónde están ubicados.
    - Saber en todo momento que trabajador accede a ellos (gestión de identidad), implantando controles con privilegios de acceso y custodia de ficheros.
    - Establecer cuándo se deben borrar estos datos
    - Proceder al cifrado de datos si es necesario, para proteger la confidencialidad.
    - Si procede, se pueden usar modos de anonimización.

  - Tener instalados programas antimalware y herramientas antifraude, todo ello actualizado.
  - Llevar un control del software que la empresa utiliza, siempre tiene que ser comprado legítimamente.
  - La empresa debe tener equipos con cortafuegos para proteger sus comunicaciones.
  - Con periodicidad, la empresa debe hacer copias de seguridad.

- **Si la empresa utiliza comunicaciones comerciales debe cumplir la LSSI**

- **Si se trabaja con comercio electrónico la empresa debe tener expuesto en su página web para que cualquier posible cliente lo pueda ver:**
  - Su denominación social, NIF, datos de inscripción en registro, correo electrónico
  - Si hay venta de productos, diferenciar claramente los precios del producto del precio del gasto de envío.
  - Si por la naturaleza de nuestro trabajo estamos adheridos a un código de conducta dar la correspondiente información, así como, indicar la titulación académica y la colegiación.

- **Si en la empresa se hacen servicios online también debe informar sobre:**
  - Trámites del contrato
  - Disponibilidad del contrato y su registro electrónico
  - Formas para poder corregir datos erróneos que hubiera en la contratación
  - Lenguas oficiales en la que se podrá redactar el contrato.
  - Condiciones generales.

- **Si la web de la empresa utiliza cookies hay que informar al cliente de cuál es su utilidad y si son propias de la empresa o de terceros:** El cliente tendrá que dar su consentimiento previo antes de poder acceder a todo el contenido de la página web.

- **Respecto a los diseños industriales, marcas, nombres comerciales, patentes, logotipos de terceros ajenos a la empresa, se debe garantizar que no se usan fraudulentamente:**
  - Si nuestra empresa tiene una marca o nombre comercial, tenemos que solicitar nuestros derechos en la Oficina Española de Patentes y Marcas

- Si la empresa tiene un dominio web hay que abonar los correspondientes derechos.

➢ Plan de referencia de la empresa para aplicar en seguridad

Actualmente, hay que tener en cuenta en una empresa que es necesario proteger la información de la empresa si se quiere salvaguardar el negocio. Es importante que cada empresa tenga un Plan de referencia. El fin es minimizar los riesgos hasta un nivel aceptable.

Primero habrá que analizar cómo se encuentra la empresa en la actualidad. Concretar los intereses de la empresa y también habrá que contar con la participación de los empleados ya que ellos tienen unas obligaciones y deberán cumplir un código de buenas prácticas. Cuando este plan de seguridad funcione bien podremos obtener un certificado.

Objetivos que cumplir:

Planificación a nivel legal, de organización y técnico, teniendo en cuenta los intereses de la empresa.

- **Previamente:**

- Se formará un equipo para hacer un análisis de ciberseguridad de la empresa en la actualidad.
- Dentro de la empresa el Plan de referencia se puede aplicar, para toda ella en conjunto o solamente para algún departamento o proceso concreto, esto pues habría que delimitarlo.
- Señalar al responsable de seguridad y a otros tipos de responsables relacionados con la información.
- Hacer una valoración previa.
- El modo de hacer el análisis para ver el grado de cumplimiento puede ser con reuniones, inspecciones y revisiones.
- Designar los objetivos que se propone cumplir la empresa sobre ciberseguridad.

- Se realizará un análisis técnico. Se estudiará los antivirus y cortafuegos de que dispone el sistema de seguridad la empresa. También se comprobará la seguridad de la página web y si existe control de acceso.

- Se tendrán que analizar los riesgos a los que se expone nuestra empresa.
    - Concretar qué activos de la empresa pueden estar en riesgo.
    - Estudiar las posibles amenazas.
    - Calcular las consecuencias que ocurrirían si una de las amenazas se cumpliera.
    - Comprobar las medidas de seguridad.
    - Estudiar los riesgos de tipo residual que también puede afectar a la empresa.

- Cuando ya tengamos concretados los riesgos, deberemos establecer qué nivel puede aceptar la empresa para corregir todo lo que se pueda.
    - Se puede contratar un seguro, para que el riesgo lo asuma un tercero.
    - Anular el riesgo del todo.
    - Asumir un porcentaje de riesgo si está justificado.

- El Plan de referencia debe tener en cuenta la planificación futura de la empresa, el crecimiento previsto, si se va a externalizar alguna parte de la producción o si va a haber alguna reorganización.

- Dentro de los proyectos pensados para llevar a cabo este plan deben tener prioridad los que con poco esfuerzo se consiga un mejor resultado respecto de la seguridad.

- Cuando ya esté preparado el boceto del Plan, lo deberá revisar y aprobar la dirección de la empresa. Cuando esté aprobado por dirección se deberá informar a los trabajadores.

- En la ejecución del Plan de referencia hay que hacer primero una presentación del mismo a los empleados que estén implicados. Dotar de presupuesto y recursos a cada proyecto e indicar quién es el responsable. Señalar la periodicidad concreta en que se harán las

revisiones de los proyectos parciales y del Plan en su totalidad, tendiendo en cuenta que todo cambio importante que surja en la empresa puede conllevar una revisión del Plan.

- Cuando se haya llevado a cabo con éxito el Plan de referencia, la empresa podrá obtener un certificado de calidad según la ISO 27001 de Sistemas de gestión de la seguridad de la información. También puede resultar interesante que la empresa firmara la adhesión con algún sello de confianza.

➢ Conveniencia de que los proveedores también tengan medidas de seguridad

En la actualidad la mayoría de las empresas contratan servicios con empresas externas. No sirve de nada que la empresa tenga un maravilloso sistema de seguridad si sus proveedores externos que trabajan con su información no lo tienen. Se les debe exigir por lo tanto que tengan la misma seguridad.

Los proveedores a los que debemos exigir este nivel adecuado de seguridad son:

- Los que nos dan servicios tecnológicos: Almacenamiento en la nube, páginas web, servicio de pagos con tarjetas, soporte informático.
- Los que nos dan servicios no tecnológicos pero que pueden acceder a datos de nuestra empresa como los relacionados con publicidad, marketing, entidades financieras.
- Los que nos suministran productos tecnológicos, nos venden hardware, aplicaciones informáticas o dispositivos (móviles, equipos informáticos)

El objetivo es que nuestra información esté protegida, para ello los proveedores que tengan acceso a nuestra información deberán firmar unos acuerdos y unos contratos referentes a esta protección. Esta protección debe exigirse durante el servicio y cuando ya haya finalizado.

También debemos comprobar que los servicios y productos que hemos contratado son acordes con la política de la empresa respecto a seguridad.

➢ Redes sociales

1. Uso de redes sociales

Para publicitar las actividades que realiza nuestra empresa podemos utilizar las redes sociales ya que permite relacionarnos de manera más cercana con nuestra clientela. Estas redes sociales disponen de unas estadísticas donde nos informan del género de las personas que nos ven, su edad, desde donde nos ven y las preferencias que tienen, que las tendremos que tener en cuenta en el momento de realizar una campaña de publicidad. Asimismo, sirven para conseguir nuevos clientes y conocer su opinión.

Un mal uso de las redes por parte de la empresa les puede suponer una gran inseguridad ya que puede perjudicar a su imagen.

2. El peligro que conllevan las redes

Errores que cometen los trabajadores:

La mayoría de los errores tienen su origen en los trabajadores como por ejemplo poner opiniones en nombre de la empresa o responder comentarios de las publicaciones de manera "agresiva".

Otro de los errores más comunes es difundir información privada de la empresa tanto desde la cuenta de la empresa como desde la del personal de los trabajadores. La información difundida de este tipo puede ser utilizada por delincuentes para dañar a la compañía.

Configuración de la privacidad:

Para cualquier página en la que se requiera usar una contraseña tenemos que utilizar una que sea fuerte para que no ponga en peligro el usuario de nuestra empresa ya que podrían robarla para publicar en nuestro nombre.

Dejar que cualquiera de nuestros trabajadores publique en nuestra página web puede ser peligroso porque la imagen que queremos dar puede ser que vaya variando. Hay que tener bien claro en qué tono y de qué manera nos vamos a comunicar con los clientes, responderemos a sus comentarios y a las quejas. Solo a ciertas personas se les permitirá publicar en la página.

Engaños en las redes sociales:

La delincuencia también se lleva a cabo en las redes sociales mediante distintos procedimientos, el propósito final es conseguir dinero.

- **Usuarios falsos fingiendo ser un cliente o proveedor:**

Mediante este procedimiento pueden cambiar los datos de envío de los productos, los de cobro.

- **Malware:**

Enviar programas peligrosos fingiendo que son usuarios normales de la red social es otro de los métodos que tienen para atacar los ordenadores y móviles de los clientes.

Al ganarse la confianza de los clientes o proveedores les pueden indicar que entren a ciertas páginas, en las cuales descargaran algún programa sin darse cuenta. Otro método es enviárselo como un archivo adjunto en un mensaje privado o al correo electrónico.
En cualquiera de los casos, el fin es corromper su equipo.

- **Phishing:**

En este caso, actúan como una empresa conocida por todo el mundo e intentan enviar a las personas a una página web donde trataran de conseguir sus datos personales y bancarios.

3. Cómo podemos prevenir esto

Todos estos ataques afectan a la imagen que tienen nuestros clientes sobre nosotros, asimismo, puede atacar nuestros equipos y que nos roben datos.

Utilizar la lógica:

Tenemos que anticiparnos a los problemas que nosotros mismos podemos causar al publicar cierta información. Hay que pensar cómo podrían utilizar toda esa información en nuestra contra, aunque no sea nuestra cuenta privada la tenemos utilizar adecuadamente.

Es recomendable que no publiquemos cosas de este tipo:

- Mensajes negativos, inadecuados
- Entrar en disputas, ofender, hostigar
- Compartir información o noticias que no estén contrastadas
- Publicar datos privados o secretos

Privacidad:

Configurar este apartado nos ayudará a evitar engaños, pero no nos debe perjudicar en nuestro trato con los clientes ni impedir que nos comuniquemos de una manera agradable.

Enlaces:

Como hemos dicho antes, pueden intentar atacar nuestros ordenadores adjuntando programas peligrosos en mensajes de la red social o invitándote a entrar en páginas externas.

No debemos fiarnos de todo lo que nos manden, por ello, antes de abrirlo debemos revisar la extensión final del archivo, si tenemos dudas, no lo abriremos. En los enlaces de las páginas web tendremos que seguir el mismo procedimiento, comprobar si conocemos el enlace y si no nos fiamos, la mejor opción es no acceder al sitio para así evitar ataques.

ORIENTACIONES PARA EL PERSONAL TÉCNICO

➢ Guarda de información en soportes externos

Estos dispositivos externos en los que podemos guardar información y transmitirla a otros rápidamente son indispensables hoy en día. Al ser tan cómodo llevarlos encima es muy fácil que los perdamos o nos lo roben.

Si permitimos que nuestros trabajadores utilicen este tipo de dispositivos para almacenar información de la empresa deben ser seguros y guardarse correctamente.

Normas de uso de estos dispositivos:

Tendremos que redactar una norma para controlar la utilización de estos dispositivos en la que reflejemos:

- Los distintos dispositivos que hay
- En qué casos se permite utilizarlos
- Cómo hay que configurarlos para que sean seguros

Avisar a los empleados:

Como se ha dicho anteriormente el peligro de estos dispositivos es que son fácilmente hurtados y por tanto hay que enseñar a los trabajadores a que los protejan y los empleen correctamente siempre conservándolos adecuadamente.

Otros métodos para guardar información:

Se pueden usar otro tipo de dispositivos para guardar información como, por ejemplo:

- Utilizar las plataformas de guardado en la nube que estén permitidas por la empresa
- Configurar el VPN para acceder al equipo de la empresa y poder trabajar desde casa

Listado de dispositivos:

Hay que llevar un listado en el que se indique que dispositivos hay y cuales tienen cada trabajador.

Procedimientos para proteger la información:

Estas técnicas sirven para asegurar que el soporte se usa adecuadamente para cuidar de la información que contiene.

Seguridad en el dispositivo de almacenamiento:

Cambiar cada cierto tiempo la contraseña del soporte externo.

Seguridad de los equipos a los que se conectan:

- Impedir que los dispositivos que no estén autorizados no puedan conectarse al ordenador.
- Desactivar los puertos USB y activarlos solo para el trabajador que tenga permiso para usarlos.
- Desactivar que se ejecute instantáneamente en cuanto se conecta el dispositivo.

Seguridad de los documentos que contiene:

- Cifrar los archivos que contenga
- Supervisar quien entra mediante permisos de acceso con claves

➢ Borrado de información de los dispositivos

En el momento en el que ya no necesitamos la información tendremos que eliminarla de forma segura. Esto es fundamental para seguir las directrices de la Ley de Protección de Datos.

Otro momento en el que nos querremos deshacer de la información es cuando queremos volver a utilizar un dispositivo externo de almacenamiento que tiene archivos en su interior o vamos a tirar uno que se ha quedado anticuado.

Si los datos que utilizamos están en papel los destruiremos mediante el uso de una destructora de papel ya que es la manera más segura para confirmar que se ha eliminado toda la información.

Listado de todos los soportes de almacenamiento que disponemos:

Mediante este inventario organizaremos todos los dispositivos que tenemos como pendrives, CD, discos duros externos, qué persona tiene cada soporte, qué tipo de información hay en ellos y cómo de peligroso sería perder esos datos que contienen para la empresa.

Borrar los datos:

En dispositivos que no sean electrónicos como pueden ser los documentos en papel, cintas magnéticas, CD usaremos la trituradora para destruirlos.

En los dispositivos electrónicos si queremos volver a usarlos tenemos que grabar encima de ellos la nueva información y por lo tanto la información que contenía anteriormente quedará eliminada. Este método se puede utilizar en todos los soportes que permitan que se borre e incluya información nueva todas las veces que se desee (mientras no esté deteriorado) como son los pendrives, discos duros.

Si queremos eliminar algún soporte electrónico porque su funcionamiento ya no sea el adecuado o porque se haya queda anticuado, habrá que usar la destrucción física para impedir que se pueda volver a utilizar.

Hay que tener en cuenta que los equipos como tabletas y móviles también guardan información en su interior y cuando queramos tirarlas para conseguir unas nuevas tendremos que borrar la información que contienen

Registro de los documentos borrados:

El programa con el que borremos todos los documentos y archivos del dispositivo tiene que proporcionarnos un documento final en el que indique cuando, el que se ha eliminado y de qué manera.

Empresas de destrucción de documentos:

Hay empresas que se dedican a eliminar documentos, estos acuden a la empresa a recoger los documentos a destruir y los eliminan. Al final se emite un documento en el que queda reflejado todo este proceso.

➢ Modo de utilización del antivirus

La gran cantidad de virus que se crean actualmente supone un gran peligro para nuestros equipos.

Los medios por los que es más fácil que nos infecten el equipo son:

- Descargar archivos de páginas web que no son seguros o directamente de correos electrónicos que no llegan y desconocemos su procedencia
- Usar soportes de almacenamiento de otras personas como por ejemplo pen drives.

Decidir qué soluciones son aconsejables:

De acuerdo con el número de trabajadores que tengamos y el grado de seguridad que necesitemos para cuidar la información que tenemos guardada necesitaremos un modelo de actuaciones u otro.

Ante varias actuaciones elegiremos la más apropiada.

Configurar el antivirus:

Para que el antivirus sea eficaz lo debemos configurar correctamente utilizando todas las funciones disponibles.

- Activar los análisis para que se realicen cada varios días de forma automática
- Que se analice el correo electrónico y las descargas automáticamente
- Dejar que se analicen ciertas páginas para detectar si son peligrosas
- Denegar la entrada a algunas páginas peligrosas

Actualizar el antivirus:

Para que todos estos programas funcionen debemos mantenerlos actualizados ya que cada día van apareciendo distintos virus. Lo más conveniente es programarlas para que se actualicen solas y así no estar pendientes cada día.

Qué hacer cuando detectamos un virus en nuestro equipo:

- Tendremos que comprobar como de grave ha sido el ataque
- A que archivos ha podido afectar
- Como podremos arreglar esos archivos
- Eliminar los archivos
- Volver a instalar los programas que han sido atacados
- Desconectar el ordenador que ha sido afectado para revisarlo posteriormente
- Anotar este ataque para futuros estudios

Instruir a los trabajadores sobre cómo actuar para evitar los ataques:

Con establecer unas normas no es suficiente debemos enseñar a los trabajadores unas técnicas para prevenir los ataques.

Cualquier archivo o programa que queramos descargar se debe presuponer que es peligroso y no confiar, aunque parezca que lo estamos obteniendo de una fuente fiable.

<u>Además, estará prohibido:</u>

- Abrir cualquier archivo descargado que no se ha revisado antes.
- Cambiar la configuración de los antivirus
- Programa el correo electrónico para que abra todos los archivos que le llegan de manera adjunta.

Sólo se deberá usar los programas que la empresa decida que están permitidos

➢ Auditoría de sistemas informáticos

Como actualmente los ataques de ciberseguridad están aumentando, la empresa, después de haber establecido cuál es el nivel de seguridad al que quiere llegar, deberá realizar auditorías para comprobar hasta dónde ha llegado.

- Tiene que determinar qué quiere auditar concretamente. Pueden ser ficheros, páginas web, programas, bases de datos, equipos informáticos. Revisando:
    - Los sistemas antimalware
    - Los permisos de acceso
    - El cumplimiento de las leyes
    - Los sistemas que prevengan el fraude
    - La posible fuga de datos
    - Las actualizaciones de programas

- La auditoría se debe hacer con el fin de mejorar

  Hay varios tipos de auditoría como vemos y se debe elegir la que más convenga en cada caso, registrando los resultados de la misma.

    - Se deben hacer auditorías legales para ver si la empresa cumple los requisitos a los que nos obligan las leyes.

    - También hay que hacer auditorías forenses cuando se ha producido algún incidente, para poder después analizarlo, ver quien ha sido el responsable del hecho e interponer una denuncia si corresponde.

- Para revisar a fondo el tema de la seguridad de información de nuestra empresa, por lo menos cada dos años, se debe hacer una auditoría independiente.

- Después de tener el resultado de la auditoría, se lleva a cabo un análisis para buscar errores e implantar un sistema de corrección de la vulnerabilidad.

➢ Seguridad en el comercio electrónico

En la actualidad hay un auge en la utilización del comercio electrónico entre los consumidores por ello las empresas lo están utilizando en su mayoría porque supone llegar a un público más amplio, conlleva un crecimiento del negocio de la empresa y no hace falta hacer una gran inversión.

Pero para que este comercio sea fiable para el potencial cliente, la empresa debe tener en cuenta unas cuestiones concretas sobre seguridad:

- La empresa en su página web debe mostrar claramente el aviso legal, las condiciones de sus contratos y la política de cookies.
- Si se trabaja con empresas como eBay, Amazon, etc. Se tiene que conocer claramente sus condiciones respecto a la legalidad.

- Es necesario que los clientes puedan realizar compras online mediante pago seguro con tarjeta.
- Es necesario que la empresa tenga copias de seguridad para que ante un ataque cibernético puedan restaurar la web con rapidez.

La política de seguridad debe tener estos puntos clave:

- Debe haber un seguimiento además de la política de seguridad de nuestra web, de la política de seguridad de las webs de los proveedores.

- La tienda online debe tener un certificado web.

- Mostrar sellos de confianza que avalen la seguridad del comercio por internet de la empresa. Los proporcionan entidades públicas, empresas u organizaciones privadas. Interesa sobre todo que estas entidades realicen auditorías de seguridad.

- **Las empresas respecto a sus tiendas online deben cumplir las leyes:**
    - LSSI-CE Ley de Servicios de la Sociedad de Información y Correo Electrónico
    - RGPD Reglamento europeo de protección de datos

- **Hay que prevenir las adquisiciones engañosas, para ello hay que:**
    - Crear unas listas donde aparezcan los clientes fiables (listas blancas) y otras los clientes que han dado problemas (listas negras)
    - Cuando la empresa contrate los pagos online con otras empresas que hacen de intermediario entre el banco de la tienda virtual y el cliente. Ellas deben ofrecer formas de pago con tarjeta seguras, además realizar un seguimiento de operaciones que nos den formas de trabajo seguras para evitar el fraude.

- Como lo habitual es pagar con tarjeta de crédito, se deben seguir las normas de seguridad de datos para la industria de tarjeta de pagos PCI DSS. Si se siguen esos procesos hay garantías de que la compra será segura y no existirán fraudes. Es importantísimo que no sea obligado para nuestra empresa, el guardar datos de tarjetas ni números de cuenta de los potenciales clientes.

- Debe haber un control de contraseñas y accesos para las personas que dentro de la empresa se dediquen a manejar la tienda online. Si se puede es muy útil la doble autentificación. También es conveniente que el ordenador sea seguro y tenga conexión cifrada.

- La empresa puede detectar una compra fuera de la legalidad si se fija en los siguientes detalles:
    - El comprador ha intentado varias compras erróneas antes de finalizar el pedido.

    - Hay que comprobar que existe realmente la dirección de email

- Debe crear sospechas, el que se elija por parte del cliente el envío urgente, cuando ello encarezca mucho el producto.

- Sospechar que es un receptor intermediario si utiliza la misma dirección de destino para nombres distintos de clientes.

- **Cuando aceptemos nuevos clientes:**
  - Comprobar el que sus datos nos estén en lista negra
  - Si la compra es de exagerado importe
  - Comprobar que la dirección del pedido coincide con los datos de localización geográfica de la tarjeta, también se puede ver donde está situada la IP del ordenador desde donde hacen el pedido.
  - Se debe llamar al cliente si algún dato que nos ha dado nos parece extraño.

- **Cuando el cliente ya esté registrado también hay que comprobar:**
  - Que sigue en la lista blanca de clientes
  - Si ha habido algún problema de pago en pedidos anteriores.
  - Si ha elegido la forma de pago de otras veces.
  - Si los datos bancarios son los de otras compras anteriores.
  - Si la dirección de destino es la misma de siempre.

- **Cuando tenemos la sospecha de que estamos ante una compra no legal debemos:**
  - No mandar la mercancía
  - Llamar a la entidad bancaria para hacer la comprobación de la cuenta, exigiremos respuesta por escrito.
  - Ponernos en contacto con el cliente y pedirle que por correo electrónico nos mande de nuevo sus datos personales.
  - No utilizar el dinero que viene de una compra que puede ser no legal ya que en el futuro la empresa emisora de la tarjeta nos puede reclamar el dinero.
  - Poner una denuncia ante la policía.

➢ Formas de controlar el acceso informático

Un tema importante para proteger nuestra empresa es controlar el acceso a su información para ello hay que tener en cuenta:

- Hay que establecer unos grupos diferenciados, que tendrán acceso a cierto tipo de información.
  - Teniendo en cuenta el área o departamento
  - Según la tipología de la información
  - Teniendo en cuenta a qué operaciones a realizar sobre la información tiene permiso el trabajador.
- Se darán permisos a cada trabajador según el grupo al que pertenezcan, según hemos señalado en el punto anterior. Estos permisos están relacionados, sobre la lectura, modificación, borrado, copia de información dentro de los archivos.

- La empresa tiene que tener establecido un procedimiento para crear, cambiar y borrar cuentas de acceso.
- Cuando se entregue al trabajador las credenciales se le informará de cuándo caducan las contraseñas, cuándo se deben cambiar y cómo se hace un bloqueo.
- También se crearán unas cuentas de administrador, que tienen el poder de realizar cualquier acto sobre todos los sistemas administrados por ellas.
    - Las claves de la cuenta de administrador deber ser muy fuertes, cambiadas con frecuencia y realizar sobre ellas auditorías.
    - Los privilegios de estas cuentas no deben ser heredados.
    - Debe haber un control de acceso con doble autentificación
    - Hay que anotar en un registro todas las acciones que se hagan como administrador.

- Para autentificar a la persona que lo usa utilizaremos mecanismos internos mediante:
    - Vía web
    - Servicios de directorio
    - Serán del tipo
        - Biométricos (huella dactilar)
        - Contraseñas
        - Con alguna tarjeta personal

- Se revisarán los permisos de los usuarios periódicamente

- Cuanto termine el contrato de trabajo con algún empleado tenemos que anularle los permisos de acceso y las cuentas de correo. También tendrá que devolvernos las tarjetas de acceso de la empresa y los dispositivos de almacenamiento.

➢ Información sobre copias de seguridad

Como la información que posee la empresa es importantísima, hay que proteger los dispositivos donde se encuentra guardada, ya que cualquier incidente puede poner en un grave problema a nuestra empresa.

- Lo principal es que haya un correcto inventario de los lugares donde tenemos la información con un registro de software para poder hacer periódicamente las copias de seguridad.

- El empresario y los técnicos de la empresa debe decidir cuál sería la información necesaria que haría falta para poder volver a poner en marcha el negocio si hay un problema grave.

- Hay que decidir quién son los responsables de hacer estas copias

- Sólo accederán a las copias de seguridad el personal autorizado.

- Es obligado por ley hacer copia de la información crítica de la empresa y de la que nos exijan las relaciones con terceros, según los contratos que la empresa haya suscrito.

- Hay que establecer con que periodicidad se hacen las copias. Hay que tener en cuenta.

  - Cada cuanto tiempo varían los datos que genera nuestra empresa
  - Valorar el coste que supone almacenar datos.
  - Cumplir con el Reglamento de Protección de datos respecto a las copias de seguridad.

- La empresa debe decidir el modelo de copia más apropiada según, el tipo de información, la durabilidad del soporte donde se hacen las copias y si también es necesario guardar varias copias de las anteriores a la realizada en último lugar.

- Hay que designar un lugar para guardar las copias.
  - Es necesario que haya una copia fuera de las dependencias de la empresa.
  - No guardar en casa copias de archivos que contengan datos personales.
  - Si hay datos muy valiosos puede ser conveniente contratar algún servicio externo a la empresa.

- Pueden hacerse copias en la nube, pero tomando precauciones:
  - Previamente a hacer la copia se debe cifrar la información.
  - Se deben firmar con el proveedor de la nube, acuerdos que garanticen la confidencialidad, disponibilidad y control de acceso.
  - Respecto a la instalación en la empresa, se debe pensar en el ancho de banda que se necesita para utilizar la nube.

- Para que el proceso de copia, así como el de restauración de la información sea rápido, hay que redactar unos procedimientos que sean claros.

- Hay que comprobar cada cierto tiempo que las copias no se han estropeado, restaurándolas de vez en cuando.

- Se debe decidir el tipo de soporte que se va a utilizar para guardar las copias (USB, la nube, DVD, discos duros externos, etc.)

- Los soportes de copia deben estar bien etiquetados para que sea rápido el poder encontrarlos.

- Hay que destruir de forma segura los soportes de copia que ya no sean necesarios.

- Para proteger los datos en caso de que alguien que no esté autorizado pueda acceder es necesario cifrar la información. También la almacenada en la nube.

➢ Protección de la página web de la empresa

El uso de una página es imprescindible para casi todas las empresas. Ya que su servicio puede llegar a cualquier parte del mundo, permite una relación más cercana con el cliente, permite a la empresa no gastar tantos recursos, le podemos enviar publicidad a nuestros compradores, se puede ofrecer el servicio de venta online.

Mediante un ordenador conectado a internet con un software determinado podremos crear nuestra página web. El contenido lo podremos gestionar mediante un gestor de contenidos como WordPress. También podemos crear nuestra página con herramientas online como Wix o

acordando el uso de un servicio de alojamiento a un proveedor y además de contratar que nos diseñen la página.

Puntos clave

Disponer de un certificado web:

Si nuestros clientes pueden entrar con su cuenta a nuestra página o dejar comentarios debemos cifrar los canales por los cuales se transmite esa información para ello tendremos que conseguir un certificado web.

Protección de datos del cliente:

Si nuestra página web obtiene datos de nuestro cliente, el Reglamento General de Protección de Datos nos obliga a cumplir ciertas pautas:

- Sólo debemos obtener la información que necesitemos
- Implantar procedimientos de seguridad para los datos por ej. Copias de seguridad, control de los clientes que han accedido)
- En el momento en el que se pida el consentimiento al cliente, hacerlo con lenguaje sencillo
- Tener una política de cookies
- Garantizar los derechos de acceder, rectificar, cancelar y oponerse

Creación de la página por un tercero:

Si la página la va a crear una tercera persona, tenemos que añadir requisitos de seguridad, por ejemplo, que se cifren las credenciales, copias de seguridad, que se realice todo de manera segura.

Cumplimiento de la ley:

Existe otra ley que debemos cumplir si nuestra página tiene fines lucrativos, es la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico.

Por ello tendremos que indicar las condiciones de uso o de contratar el servicio y lo que tenga que ver con los avisos comerciales.

Servidor propio:

Si el servidor para la página web va a ser el nuestro, tenemos que revisar ciertas cosas:

- Tenemos medidas de seguridad como cortafuegos e instrumentos para detectar accesos indebidos
- Tener disposiciones sobre medidas contra el malware
- Los administradores entran de manera segura a realizar sus actividades

Servidor externo:

Si nuestra web está en un servidor externo debemos revisar nuestro contrato con ellos:

- Comprobar que tenga apartados de confidencialidad
- Indicar quién es el responsable de tratar los datos
- Que disponga de copias de seguridad, auditorias

Web dirigida por una tercera persona:

Al estar la página web administrada por una tercera persona tendrá que estar disponible un registro en el que quede reflejada toda la actividad de los administradores para que podamos acceder ella por si sucede algún incidente en cuanto a la seguridad.

Configuración del Sistema de Administración Central:

Seamos nosotros o una tercera persona quien administre la página debemos tener en cuenta una serie de normas de seguridad.

- Usar CAPTCHA para así evitarnos spam
- Comprobar si ocurren cambios en los contenidos
- Vigilar la gente que entre al panel de control

Entradas panel control:

Hay que comprobar que las contraseñas con las que se entre al panel de control se generen de acuerdo con las pautas de seguridad.

- Si los nombres y contraseñas no se van a usar debemos deshabilitarlos.
- En cuanto a la cuenta del administrador, hay que ponerle una contraseña fuerte y que esta se cambie continuamente.
- Usar métodos para comunicarse de manera segura.

Restringir el acceso:

Hay que configurar el servidor de la página web, independientemente de si está en nuestra empresa o en la del nuestro proveedor, para que tenga un límite de accesos.

Usuarios creados automáticamente:

Verificaremos que se han eliminados los usuarios que aparecen originalmente en los servidores web.

Archivar todos los registros de los usuarios:

En el caso de que ocurra algún percance en el que intervenga nuestra página web o debamos entregar los registros en el caso de un juicio, debemos almacenar todos los registros que hay en nuestra página.

Si gestionamos el servidor directamente nosotros, seremos quienes guardaremos los registros durante el tiempo conveniente, en cambio, si la gestión se lleva externamente, deberá quedar bien indicado en el contrato y detallando cuáles son los registros que hay que almacenar y durante cuánto tiempo.

Tienda online en nuestra página web:

Puede que nuestra página disponga de una tienda online, en ese caso debemos crear y cumplir una normativa específica para ellos, en la que así evitemos los engaños y ayudemos a los clientes.

Sello que certifique es una tienda de confianza:

Mediante este distintivo podremos asegurar a los clientes que nuestra tienda online es segura.

Copia de seguridad:

Hay que efectuar copias de seguridad regularmente sin importar si la página web está en un servidor externo como propio.

Auditorías:

Es recomendable encargar que se elaboren auditorías externas para comprobar la seguridad de la página.

Mantener el software al día:

Actualizar el software tiene que ser una de las actividades que tenemos realizar regularmente, sin importar si la página se gestiona por nosotros o por nuestro proveedor. Además, es recomendable que tengamos las notificaciones de los programas que utilicemos activadas, para enterarnos de las nuevas actualizaciones.

Antivirus:

Hay que instalar un antivirus en los ordenadores de la empresa, que ofrezca protección tanto al correo electrónico como a las páginas web. Asimismo, debemos estar al tanto de las actualizaciones que vayan apareciendo para tenerlo actualizado siempre.

- Formas de respuesta ante los incidentes

Como en la empresa puede suceder un incidente respecto a la seguridad, la empresa debe tener un plan para actuar y cuando llegue el momento estar preparados. Se ha debido de establecer con anterioridad qué es lo que se tiene que hacer, qué trabajadores participarán y cómo se informará al resto de la empresa.

- Se debe nombrar a un grupo encargado del tema, puede formar parte del grupo tanto el director de la empresa como el técnico informático.

- Es bueno hacer simulacros para que todos los trabajadores estén preparados y sepan la forma correcta de actuar.

- Es primordial que esté establecido la fecha en que el plan deja de tener validez.

- Definir claramente lo que es un incidente, clasificándolo según su importancia, para saber el orden en la actuación con él.

- Los empleados deben saber claramente a qué trabajadores o departamentos de la empresa deben avisar cuando se produce un incidente.

- Con el asesoramiento del técnico informático se deberá tener determinada la forma de actuar para solucionar un incidente. Es importante la rapidez, y si no se puede reparar totalmente conseguir que los daños sean los menos posibles.

- Es importante llevar un registro donde queden reflejados todos los incidentes que ha habido, debe haber el mayor detalle posible de los mismos. Poner cuándo se han

producido, de qué tipo son, a qué parte del sistema de la empresa han afectado, qué o quién lo ha producido, cómo se encuentra en el momento actual el tema, cómo y cuándo se solucionó y quién consiguió repararlo.

- Como la ley obliga a avisar a las personas perjudicadas y a la policía, si ha habido un problema con datos personales, la empresa debe cumplirlo.

➢ Conveniencia de utilización de técnicas criptográficas

En la empresa trabajamos con mucha información privada como por ejemplo los correos electrónicos, bases de datos, copias de seguridad, datos que se encuentren en móviles, aparatos de almacenamiento externo y claves para efectuar comprar por internet.

La importancia de todos estos datos para nuestra compañía hace que debamos guardarlos evitando que otras personas puedan acceder a ellos.

Qué datos se deben cifrar:

Para tomar esta decisión tenemos que organizar toda la información que tenemos, algunos ejemplos de información que podríamos tener:

Información que contenga datos personales, datos de los clientes al registrarse, documentos guardados en dispositivos externos o en la nube.

Firma electrónica:

La firma electrónica es el procedimiento por el cual se comprueba y autentica la información de un sujeto ante las Administraciones Públicas u otros procesos cotidianos como la emisión de facturas. Existen varios tipos de certificados: de representante, de persona jurídica…

Certificado para nuestra página online:

Mediante un certificado aseguraremos que los datos de nuestra web son seguros

Necesidad de cifrar los datos cuando se acuerdan servicios con terceros:

Si vamos a acordar un servicio en el que los datos que se usen sean privados, debemos comprobar que el envío de esos datos es seguro, para ello los cifraremos antes de enviar o los trasmitiremos por canales fiables.

Cifrado de información en APP:

Al pactar la creación de una aplicación web o para móviles que permita a los usuarios registrarse y acceder con una cuenta, las claves de los usuarios deben permanecer cifradas.

Acceder mediante VPN:

En el momento que deseemos que nuestros trabajadores realicen su jornada laboral desde casa tendremos que habilitar el acceso mediante VPN que este cifrado para asegurar el carácter privado de los datos.

- Necesidad de actualización de software

Cualquier tipo de programa precisa actualizaciones para mantener sus niveles de seguridad, incluso los sistemas operativos y antivirus. Constantemente, los creadores de estos programas envían nuevas versiones y actualizaciones de los programas que corrigen ciertas partes que no funcionaban correcta o directamente incluyen nuevas opciones que no estaban anteriormente.

Software actualizable:

Revisaremos todo el software que tenemos en nuestro equipo y comprobaremos que todos estos programas están al día, revisando si han aparecido nuevas actualizaciones. Si localizamos alguna versión nueva procederemos a instalarla.

Así pues, nos anticiparemos a posibles errores que tendríamos en estos programas durante mucho tiempo sin darnos cuenta.

Cuando actualizar:

Que comience una actualización mientras estamos realizando nuestro trabajo es muy molesto. La gran mayoría de los programas que utilizamos comienzan a actualizarse automáticamente sin avisar previamente, pero existen algunos en los que podemos activar las alertas para que nos avisen cuando se ha publicado una nueva versión del programa y poner en funcionamiento la descarga en el momento en el que nosotros deseemos.

Del mismo modo, podremos ver que nuevas funciones trae esa actualización y que requisitos previos exige antes de instalarse.

Comprobar:

Las actualizaciones que queramos añadir a nuestro equipo las deberemos descargar de un lugar seguro y que sea oficial, aunque nunca viene mal comprobarlas en otro equipo para ver si funcionan correctamente.

Volver a la anterior versión:

Hay que tener en cuenta que puede que la actualización que nos acabamos de descargar se ajuste a las necesidades que tenemos o que por ejemplo no funcione correctamente y queramos volver a la versión anterior. Es muy conveniente que antes de cambiar a la nueva versión hagamos una copia de seguridad.

Instrumentos para comprobar nuevas actualizaciones:

Hay distintas aplicaciones para comprobar si el programa está actualizado a la última versión o no y si vemos que ha aparecido una nueva podemos proceder a actualizarla en todos los equipos a la vez, esto es muy beneficioso si en nuestra empresa queremos que todos los ordenadores tengan la misma versión del programa.

Programar sistema de avisos:

Es muy recomendable activar este sistema para que nos avise cuando aparezca una nueva versión del programa. Nos podemos suscribir a páginas que nos envían un correo cuando aparezca la nueva versión o seguir en redes sociales a cuentas que compartan contenido de este tipo.

Inventario de la versión de los programas:

Al llevar una lista de la versión de los programas que tenemos en cada equipo y que actualización hemos instalado, podremos ver rápidamente que programas tenemos instalados en cada ordenador.

ORIENTACIONES PARA EL EMPLEADO

- Cada empleado debe proteger su puesto de trabajo

Los puntos clave de esta política son:

Reglamento de protección:

Es imprescindible que la empresa goce de una normativa específica en la que se señalen los procedimientos para la protección del puesto de trabajo, pero teniendo en cuenta que estas medidas tendrán que ser examinadas para comprobar su funcionamiento.

Si aparecieran cambios que les influyan como por ejemplo que se cambien los sistemas, estas deberían ser modificadas.

- Se debe informar a los trabajadores de otras normas que existan para los equipos utilizados como por ejemplo el correo electrónico, sistemas de almacenamiento.

Eliminar los documentos:

Los documentos obsoletos se deberán destruir de forma segura de acuerdo con la Política de borrado seguro y gestión de soportes. Algunos de los medios que se pueden utilizar son:

- Usando destructoras de papel a las cuales tendrán acceso los trabajadores.
- Acordando utilizar un servicio externo de destrucción segura, informando a todos los trabajadores de él y de su obligación de utilizarlo.
- Avisando a los empleados del riesgo que supone utilizar papeleras para los documentos que contengan datos personales, información económica.

Bloquear los equipos informáticos:

Los informáticos se encargarán de programar los equipos informáticos para que en el momento en el que no se detecte actividad del usuario en unos pocos minutos se cierre automáticamente la sesión. Asimismo, se puede plantear que se programe el apagado de todos los equipos cuando se acabe la jornada laboral.

Mantener al día el sistema operativo:

Los trabajadores responsables de los equipos deberán revisarlos regularmente para garantizar que están actualizados a la última versión o programando las actualizaciones informáticas.

Última versión del antivirus y comprobar su funcionamiento:

El antivirus se instalará y actualizará los antivirus en todos los equipos de la empresa y se revisarán periódicamente para garantizar su protección.

Desactivar los puertos USB:

Es conveniente que se deshabiliten los puertos USB de todos los ordenadores y sólo se habilitarán en el caso de que un trabajador de forma justificada solicite utilizarlo.

Impresoras:

Se comprobará que las impresoras conectadas a internet:

- Se accederá a su configuración a través de una contraseña
- Si están conectadas por wifi se debe configurar su seguridad
- Si disponen de discos duros hay que revisar su almacenamiento
- Deshabilitar los conectores USB si se dispone de ellos

Medios para almacenar:

El uso adecuado y seguro de los medios de almacenamiento depende de que el empleado conozca y aplique las normas de la empresa sobre el almacenamiento en el ordenador, en la red, en la nube y en los dispositivos externos como un USB.

No está permitido cambiar la configuración del ordenador:

Alterar la configuración del ordenador o instalar aplicaciones que a su juicio son necesarias implica un gran peligro ya que podría resultar en la infección del equipo informático y, por tanto, en una pérdida de archivos. Si el trabajador pide cierta configuración en su equipo o la instalación de determinados programas los deberá pedir a los trabajadores encargados del servicio informático.

Mesas sin documentos:

Con este nombre se refiere a la imposición de guardar los documentos usados durante el trabajo en el momento en el que el trabajador se ausente de su puesto. La información que contiene datos sensibles no se debe dejar a la vista de cualquier persona ya que, podría hacer un uso inadecuado de ella. Para cumplir con este precepto se debe:

- Permanecer con nuestro puesto de trabajo ordenado
- Recoger todos los documentos y dispositivos extraíbles que ya no vayan a ser usados durante ese tiempo o al finalizar la jornada laboral.
- No escribir en notas adhesivas usuarios ni contraseñas

Destruir documentos:

Los trabajadores deben usar las destructoras de papel para eliminar todos los documentos con información sensible

No dejar documentación con datos personales en las impresoras:

Con esto conseguiremos que esa información no llegue a personas que no queremos.

- Cogeremos rápidamente los documentos que mandemos a la impresora
- Recoger los documentos cuando ya estén escaneados

No dar información personal a cualquiera:

La información para la empresa es muy valiosa, por ello, es muy probable que alguien trate de conseguir parte de esa información mediante engaños a un trabajador. Alguna de la información puede ser por ejemplo las contraseñas, información de las cuentas bancarias de los clientes…

Para conseguir estos datos, se hacen pasar por alguna empresa o persona popular para que el trabajador confíe en él y le proporcione la información que le piden, utilizando el correo electrónico, WhatsApp, redes sociales.

No publicar la información:

Los trabajadores deben comprometerse a que la información a la cual tenga acceso debe permanecer sin ser pública. Esta obligación tiene que mantenerse durante todo el contrato e incluso cuando el trabajador ya no pertenece a la plantilla de la empresa.

Contraseñas:

- Las contraseñas son privadas y no se deben publicar ni entregar a otras personas.
- No debemos dejarlas apuntadas en cualquier lado al alcance de todo el mundo.
- Hay que intentar que tengan más de 8 caracteres y que incluyan caracteres especiales
- Cambiarlas periódicamente

Bloquear y apagar el ordenador:

Podemos impedir que accedan personas a nuestro equipo si lo bloqueamos cuando dejemos nuestro puesto de trabajo por unos momentos y sobre todo al apagarlo cuando terminemos nuestra jornada de trabajo.

Usar internet con responsabilidad:

Conocer la normativa que regule el uso adecuado del Internet, los programas permitidos y los consejos de seguridad permitirá que no se ponga en peligro el equipo.

- Para ello podemos comprobar que las URL no son extrañas
- Confirmar que la dirección a la que vayamos comience por https://

Utilización móviles y portátiles de la empresa:

Mediante firma el trabajador deberá aceptar la normativa que regule el uso de estos dispositivos.

Cifrado de la información privada:

El trabajador aceptará la normativa correspondiente respecto a esto.

Deber de informar sobre los problemas de seguridad:

Como, por ejemplo:

- Notificaciones del antivirus por virus/malware
- Mensajes sospechosos solicitando información
- Correos electrónicos con virus

- Extravío de dispositivos electrónicos
- Borrado de información accidentalmente
- Funcionamiento extraño de los sistemas
- Desconfianza en que alguien haya accedido a áreas o documentos protegidos
- En definitiva, cualquier actividad extraña que notemos

➢ Utilización segura del correo electrónico

La empresa deberá elaborar una normativa que regule este aspecto, la cual deberá aceptarla el trabajador en el momento que comience a trabajar con nosotros. Está vetado usar el correo electrónico para usos personales y el uso incorrecto podrá ser sancionado. Además, la empresa podrá vigilar el uso que hace el trabajador del correo electrónico si en la regulación que se le hace firmar al trabajador se indica.

Protección contra spam y malware:

Es conveniente que se disponga de aplicaciones que eviten spam y malware, así evitaremos que los correos peligrosos lleguen a nuestra bandeja de entrada para prevenir que los abramos.

Firma digital:

Mediante la firma digital aseguraremos la protección de la información sensible y garantizaremos que somos los remitentes del correo.

Ocultar direcciones de email:

Si vamos a difundir la dirección de correo de la empresa por internet, es recomendable protegerla para que no acabe en listas de correos a las que se envía spam.

Para ello podemos:

- Publicar nuestra dirección en una imagen en vez de publicarla como un texto el cual se puede copiar fácilmente.
- En vez de poner @ escribir la dirección de esta manera “empresarrobanombrepuntocom”

Utilización adecuada del correo:

El trabajador debe entender toda la normativa respecto al correo electrónico, la cual, debe aceptar.

Claves apropiadas:

- Hay que utilizar una contraseña que no sea sencilla
- Usar doble autenticación para las cuentas más importantes
- No se debe seleccionar “recordar contraseña”

Correos electrónicos recibidos que no son seguros:

Se debe enseñar a los trabajadores a reconocer los correos peligrosos

- Por ejemplo, cuando los mensajes de las empresas que recibamos habitualmente cambien su formato en los logotipos, firmas…
- El correo nos indica que debemos realizar algo distinto a lo normal.
- Nos pidan las claves para entrar a una aplicación

Conocer al remitente:

No se debe abrir un correo si no conocemos quién es el que lo manda. Habrá que estar alerta ya que puede ser un cliente nuevo o un correo peligroso.

Si conocemos a la persona/ empresa que lo envía, pero el cuerpo del mensaje es distinto debemos contactar con el mediante otros medios para conocer si es él.

Si el correo contiene un archivo adjunto debemos tener mucho cuidado antes de abrirlo ya que ese archivo puede provocar que nuestro ordenador se infecte.

Algunas cosas que debemos comprobar antes de descargarlo

- Los archivos que contiene tienen un nombre que empuja a abrirlo
- El icono no corresponde con el tipo de archivo que dice ser
- La extensión que se ve es conocida pero realmente tiene una serie de espacios que ocultan la verdadera extensión.
- Solicita que habilitemos algunas opciones

Antes de interactuar con un enlace:

Para cerciorarse de que es seguro debemos realizar una serie de comprobaciones

- Poner el ratón encima del enlace para poder ver la dirección entera
- Fijarnos atentamente en el enlace para ver letras sobrantes que podemos pasar por alto.
- Usar ceros en vez de “o”.

No contestar a los correos spam:

Cuando lleguen este tipo de correos no debemos contestar ya que si no se demostrará que nuestra cuenta está activa y nos volverán a mandar correos de este estilo. Hay que añadirlo a la lista de correos spam y borrarlos.

Usar copia oculta cuando enviemos correos:

Al enviar un correo a varios destinatarios utilizaremos la copia oculta para que así, los demás destinatarios, no vean a quien se le ha enviado ese mismo correo. De este modo evitaremos que consigan otras direcciones de correo a las que puedan enviar correos engañosos o spam.

Las direcciones de correo son datos privados y por lo tanto no debemos revelarlas sin su permiso.

No usar el wifi de lugares públicos:

Es recomendable no acceder ni usar el correo electrónico cuando estamos conectado a alguna de estas redes es mejor usar una red móvil como 4G.

- Forma de utilización de dispositivos móviles proporcionados por la empresa

Actualmente continuar con el trabajo fuera de la oficina es de lo más normal, todo esto lo podemos conseguir mediante el uso de móviles, tabletas, portátiles que sean de propiedad de la empresa o del empleado.

Todas estas tecnologías autorizan al trabajador a entrar al correo, los programas que utilicen en la empresa.

Hay un riesgo de que los trabajadores pierdan estos dispositivos y con ellos pierden también toda la información de la empresa. Hay que prevenir antes de que suceda esto por ejemplo poner contraseñas difíciles, tener siempre el móvil actualizado.

Conceder los equipos electrónicos:

Hay que crear un método para conceder los móviles, tabletas… a los trabajadores para que quede registrado quién solicita un dispositivo y a quién se lo concede.

Inscribir los dispositivos:

Es aconsejable llevar un documento en el que se indique quién tiene cada dispositivo, para que va a utilizarlo y los programas y dispositivos externos que va a tener que utilizar.

Cuidado de los equipos:

Los únicos que se deben dedicar a la conservación de los dispositivos en perfecto estado tienen que ser el departamento que se encargue de todos los equipos informáticos de la empresa. No está permitido que el trabajador que reciba el equipo realice cambios, instale programas o cambie la configuración sin permiso.

BIOS protegida:

Los dispositivos propiedad de la empresa deberán preservar la entrada a la BIOS mediante una contraseña para que los trabajadores no puedan acceder.

Programas para la localización:

En el momento de proporcionar el equipo al trabajador se le informará de si contiene algún programa de localización. En caso de que lo contenga, se le hará firmar un documento en el que acepta que este software este instalado en su dispositivo.

Guardar la información:

Si existe información de la empresa que no es necesaria que se guarde, no se debe almacenar en el equipo. Puede ser que podamos visualizar la información desde varios equipos, en ese caso, los documentos deben estar sincronizados para evitar que haya varios archivos iguales y nos equivoquemos con las versiones.

Cómo proceder con la información privada:

La información privada que se guarde en el dispositivo debe cifrarse y en el momento que se deposite de vuelta a la empresa debemos borrar toda esta información.

Conexión segura:

Si se conecta el dispositivo a redes distintas a la de la empresa se deben seguir ciertas normas para que este procedimiento se realice de manera segura.

Alertas por virus:

Si creemos que nuestro equipo ha sido atacado por un virus debemos informar rápidamente a las personas encargadas de estos asuntos.

Traslados y cuidado:

El calor puede afectar negativamente a las piezas internas del dispositivo por tanto debemos evitar exponerlo a ello. El trabajador tiene que evitar que terceras personas puedan llegar a la información que contiene el equipo, por ello no debe dejarlo sin vigilancia en los transportes públicos ni dejarlo a la vista de cualquiera en el coche.

Si el lugar donde se presta el trabajo no nos garantiza que donde dejemos el dispositivo es seguro, debemos dejarlo en un armario seguro y si se produce un robo debemos informar a los responsables.

Obligaciones del trabajador:

El trabajador tiene el cometido de cuidar el equipo que se le ha entregado y de toda la información que este contiene.

- Forma de utilización de dispositivos móviles propiedad del empleado

No utilizar equipos manipulados:

Se aconseja no usar equipos que hayan sido "rooteados" ya que se pueden instalar aplicaciones no oficiales.

Alertar a los trabajadores sobre robos:

Ordenadores portátiles, móviles y otros dispositivos es muy fácil que sean robados, por tanto, debemos informar a los empleados sobre ello para que estén alerta. La pérdida de algún equipo supone un peligro ya que tiene un montón de datos.

Proporcionar conocimientos a los trabajadores:

Les daremos información para que sepan usar los dispositivos correctamente y de manera segura. Algunas de las cosas que deben saber son:

- Configurar los apartados de seguridad de los equipos.
- Conocer cómo se actualiza el sistema operativo o las aplicaciones que correspondan.
- Los programas que requieran que se acepten unos permisos antes de su instalación no es recomendable instalarlos.
- Programar el equipo para que se bloquee automáticamente después de un periodo sin usarlo y que ese bloqueo sea con contraseña.

No usar redes wifi-públicas:

Es mucho más recomendable usar los datos de su móvil 3G/4G ya que las redes wifi-públicas no son seguras.

Aplicaciones prohibidas:

Elaboraremos un listado en el que quedarán reflejados los programas que no se pueden instalar en los equipos porque exigen permisos para acceder a datos que son privados de la empresa, como por ejemplo los datos de contactos.

Inspeccionar quien accede a la red:

Es recomendable que se demuestre quién entra a la red de la empresa. Si acceden mediante red VPN será mucho más seguro ya que queda cifrado.

Registro de accesos:

Conservaremos la lista de las personas registradas y con los equipos que han accedido para conocer quiénes son estos usuarios que pueden llegar hasta los datos y programas de la empresa.

Normas para guardar los datos de manera segura:

- Añadir en los equipos un sistema de cifrado de la información
- Imposibilitar que se almacene automáticamente los datos de los usuarios.

Pérdida de equipos:

Es muy fácil perder estos dispositivos por ello estableceremos una serie de normas/ consejos

- Se podrá localizar el equipo por medio de GPS o wifi.
- Activar el bloqueo de pantalla
- Existe una opción para borrar los datos que contiene el que equipo a distancia de manera que si lo coge otra persona no pueda usarlos.

➢ Teletrabajo

La utilización de los nuevos dispositivos móviles entraña muchos riesgos como:

- Que el dispositivo sea robado, a parte del coste del aparato, también se pierde la información que puede ser confidencial.

- La infección por malware también puede ocurrir en estos equipos pequeños, no hay que descuidar su protección.

- Los sitios web fraudulentos. Con los móviles es más difícil librarse de la publicidad engañosa. Hay que aumentar la precaución.

- Utilizar redes wifi inseguras. Al estar en sitios públicos donde se pueden utilizar redes sin claves, podemos ponernos en riesgo ya que los ciberdelincuentes también pueden acceder a esas redes para robarnos información.

- La instalación de aplicaciones innecesarias las cuales necesitan permisos del dispositivo para funcionar, pueden ser peligrosas porque pueden comprometer la información de la empresa.

- Que el dispositivo no tenga control de acceso fuerte, es un peligro en el caso de que se pierda el dispositivo o lo roben, cualquier podría acceder.

- Tener el sistema operativo o la aplicación desactualizada es un riesgo para la seguridad de la información.

- Eliminar los controles de seguridad que vienen de fábrica en los aparatos.

- No hay que elegir la opción de que el dispositivo recuerde la contraseña automáticamente.

- Es peligroso utilizar servicios en la nube.

LAS MEDIDAS DE PROTECCIÓN QUE DEBEMOS USAR SON:

- **Utilizar protección antimalware y sitios web peligrosos:**

  Por correo electrónico, por las aplicaciones o por pendrives pueden llegar códigos maliciosos. Hay que tener por lo tanto herramientas que nos sirvan para detectar y eliminar software malicioso.

  Hay que tener la última versión del antivirus y que esté actualizado.

- **Protección contra accesos no autorizados:**
  - En los portátiles tiene que haber contraseña de firmware
  - Hay que crear diferentes cuentas de usuarios con privilegios de acceso para que puedan desarrollar su trabajo, cada cuenta tiene que tener una contraseña fuerte para que no fácil entrar.
  - Es conveniente que exista un bloqueo de pantalla que se active en el menor tiempo posible y que haga falta una contraseña robusta para entrar de nuevo. Lo ideal sería utilizar la huella dactilar.

- **Protección de la información:**
  - Así como los móviles actuales con sistema Android e IOS tienen cifrado de información por defecto en los sistemas operativos de los ordenadores hay que activarlo.
  - A la información confidencial se debe acceder a través de internet para no descargarla en el dispositivo.

- **Utilizar aplicaciones legítimas:**
- Todas las descargas de aplicaciones deben ser desde tienda oficial en los móviles y desde web oficial en los ordenadores.
- La empresa debe tener licencia válida de todos los programas que utilizan sus trabajadores. Los programas deben ser de la última versión.
- No utilizar nunca en los dispositivos móviles la función “recordar contraseña”.
- Si se utilizan muchas es mejor contar con un gestor de contraseñas como ayuda.
- Utilizar siempre redes wifi-seguras.
- Descartar el uso de redes wifi gratuitas en edificios públicos, restaurantes, aeropuertos, hoteles, ya que al no conocer su seguridad no sabemos si alguien puede interceptar la información que enviemos.
- La conexión móvil 4G es más fiable para realizar tareas con riesgo como acceso a la banca on line.

SI SE HACE TELETRABAJO EN CASA

Es conveniente tener en casa un nivel de ciberseguridad aceptable, utilizar aplicaciones con licencia y tener contraseña y sistema de bloqueo del equipo, así como cifrado de la información.

En el dispositivo que se utilice en casa para trabajar no se permitirá que otros miembros de la familia descargue juegos, etc.

Periódicamente se harán copias de seguridad.

Si se utiliza red wifi doméstica, tiene que tener una clave robusta, se debe utilizar cifrado y desactivar la función WPS.

- Hay veces que los empleados utilizan dispositivos de su propiedad para hacer trabajos en casa, esto beneficia a la empresa porque no ha gastado en comprar equipos y al trabajador ya que le permite conciliar la vida laboral.

También conlleva unos riesgos como:

- Puede producir distracciones entre los empleados, ya que al ser su ordenador tienen facilidad para acceder a páginas web no relacionadas con el trabajo, a su correo electrónico o a las redes sociales.
- Aumentan las posibilidades de robo de información, ya que pueden aumentar también los accesos no autorizados.
- Puede ocurrir que se preste el dispositivo a algún familiar o amigo, y por lo tanto la seguridad de la empresa queda en riesgo.
- Cuando termine el contrato de trabajo, el empleado puede seguir utilizando la información de la empresa, lo que es un riesgo.

Medidas de seguridad:

- No hacer cambios en el software del dispositivo
- Tener bajo custodia el dispositivo (incluso ante familiares y amigos)
- El empresario tendrá una normativa referente a la utilización de estos dispositivos. Además, tendrá que tener un registro de cuántos dispositivos tienen información de la empresa, qué aplicaciones utilizan y sobre todo tenerlos localizados por GPS.
- Si el dispositivo de propiedad del empleado ha sido robado hay que dar los siguientes pasos:
    - Avisar a la empresa para que tome medidas respecto de la información de la empresa.
    - Si ha sido sustraído hay que interponer una denuncia ante la Policía
    - Bloquear de manera remota el dispositivo.
    - Con el GPS localizar el dispositivo (Por lo cual los empleados deben tenerlo activado obligatoriamente)
    - Si no se puede recuperar se debe hacer un borrado remoto de la información. Por lo que esta opción debe estar activada.

CONCLUSIONES

Muchas de las pymes ofrecen actualmente servicios web y aplicaciones móviles con las que aumentan día a día sus negocios y sus ganancias. El resto de las empresas va a evolucionar también hacia este tipo de mercado digital. Todo ello aumentará el riesgo de que sean atacadas, por lo que es importante que conozcan a fondo todos los sistemas de seguridad aplicables. Los ciberataques también van cambiando por lo que las empresas deben estar al día y no dejar de lado el tema de la seguridad si quieren seguir creciendo.

Año tras año la implicación de las empresas en cuanto a establecer medidas de seguridad va aumentando, esto es lo necesario, es mejor que se anticipen y lo hagan antes de ser atacadas, es un ahorro de dinero para ellas. Como se ha visto las empresas son un blanco fácil para los atacantes, en España como en el resto de países del mundo han aumentado los ciberataques. Las empresas tienen que tomar conciencia del peligro y pasar a la acción aumentando los recursos que destinan a su autoprotección.

La guía que he confeccionado será muy útil ya que tiene unos puntos clave a seguir, diferenciados según la responsabilidad dentro de la empresa. Indicando lo que se debe hacer o no, en cada caso. Actualmente existe mucha información dispersa en muchas publicaciones de todo tipo, yo he intentado recopilar lo más interesante de algunas de ellas, pensando sobre todo en que les sirva a las pymes para poder aplicarla prácticamente.

Son muy importantes las indicaciones dirigidas al empleado, ya que suele ser por donde llegan la mayoría de los ciberataques. Tienen instrucciones sobre documentación, equipos informáticos, utilización del correo electrónico, de dispositivos móviles y sobre teletrabajo.

Debido a la situación de alarma generada por el Covid19, se ha comenzado a teletrabajar en muchas empresas actualmente, pero en la mayoría de los casos con poca seguridad. Con la utilización de esta guía se reducirían los riesgos del teletrabajo. El empresario también tiene su apartado, que le servirá como base, pero siempre deberá estar al día en cuanto a novedades que puedan surgir.

Sería interesante que se captara talento en la universidad, también espero que técnicos especializados hagan publicaciones más asequibles a cualquier persona, aunque no tenga estudios de informática, para que cualquier empresario pueda proteger su empresa sin invertir una gran cantidad de dinero.

Pienso que sería interesante el impartir cursillos gratuitos por parte de alguna entidad pública, para que los empleados adquirieran un nivel mínimo en cuanto a seguridad informática.

El enemigo también avanzará por lo que la lucha será dura, ya que siempre hay amigos de lo ajeno, por lo que seguirán existiendo amenazas.

Las limitaciones que he encontrado es que la mayoría de información disponible está dirigida a ingenieros y programadores informáticos, y mi trabajo se crea desde el punto de vista del Grado de Relaciones Laborales y Recursos Humanos.

Sería interesante que en un futuro se aplicara esta guía a una pyme real y que con una auditoría posterior valoraran su utilidad respecto a la consecución de una mejora en la seguridad.

BIBLIOGRAFÍA

Administración Electrónica Gobierno de España. (24 de Abril de 2019). *Administración Electrónica Gobierno de España*. Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio-2019/Abril/Noticia-2019-04-24-Espana-7-puesto-Global-Cibersecurity-Index-2018.html

Agencia Española de Protección de Datos. (2018). *Agencia Española de Protección de Datos.* Obtenido de https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf

Aguilera López, P. (2011). *Redes seguras (Seguridad Informática).* Madrid: Editex.

Álvarez Marañón, G., & Pablo Pérez García, P. (2004). *Seguridad Informática para empresas y particulares.* Madrid: McGraw Hill.

Andrada, A. M. (2017). *Nuevas Tecnologías de la Información y la Comunicación.* Argentina: MAIPUE.

Aparicio Salom, J. (2009). *Estudio sobre la Ley Orgánica de protección de datos de carácter personal.* Pamplona: Aranzadi.

Beynon-Davies, P. (2015). *Sistemas de información: introducción a la informática en las organizaciones.* Barcelona: Reverté.

Carpentier, J.-F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas.* Barcelona: ENI.

Centro criptológico nacional. (2019). *ccn-cert*. Obtenido de https://www.ccn-cert.cni.es/

Chaos García, D., Gómez, P., Sebastián, R., Molina Letón, E., Rodrigo San Juan, C., & Rubio González, M. (2017). *Introducción a la informática básica.* UNED.

Datos Macro. (2019). *Datos Macro/ Expansión*. Obtenido de https://datosmacro.expansion.com/pib

Digitales.es. (Mayo de 2019). *Ciberseguridad: 8 consejos para proteger tu vida digital.* Obtenido de Digitales.es: https://www.digitales.es/wp-content/uploads/2019/05/cierseguridad.pdf

Dirección General de Industria y de la Pequeña y Mediana Empresa. (2014). *Portal Pyme*. Obtenido de http://www.ipyme.org/es-ES/UnionEuropea/UnionEuropea/PoliticaEuropea/Marco/Paginas/NuevaDefinicionPYME.aspx

Instituto Nacional de Ciberseguridad. (29 de junio de 2015). *Como gestionar una fuga de información. Una guía de aproximación al empresario.* Obtenido de INCIBE: https://www.incibe.es/protege-tu-empresa/guias/guia-fuga-informacion

Instituto Nacional de Ciberseguridad. (17 de octubre de 2017). *Cloud computing: una guía de aproximación para el empresario.* Obtenido de INCIBE: https://www.incibe.es/protege-tu-empresa/guias/cloud-computing-guia-aproximacion-el-empresario

Instituto Nacional de Ciberseguridad. (18 de mayo de 2018). *Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario.* Obtenido de INCIBE:

https://www.incibe.es/protege-tu-empresa/guias/ganar-competitividad-cumpliendo-el-rgpd-guia-aproximacion-el-empresario

Instituto Nacional de Ciberseguridad. (2019). *Desarrollar Cultura en Seguridad.* Obtenido de INCIBE: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_desarrollar-cultura-en-seguridad.pdf

Instituto Nacional de Ciberseguridad. (26 de noviembre de 2019). *Navegación segura y privada para ti y tu empresa. Parte I.* Obtenido de INCIBE: https://www.incibe.es/protege-tu-empresa/blog/navegacion-segura-y-privada-ti-y-tu-empresa-parte-i

Instituto Nacional de Ciberseguridad. (3 de diciembre de 2019). *Protección del puesto de trabajo. Escenarios de riesgo.* Obtenido de INCIBE: https://www.incibe.es/protege-tu-empresa/blog/proteccion-del-puesto-trabajo-escenarios-riesgo

Instituto Nacional de Ciberseguridad. (14 de enero de 2020). *Cómo evitar incidentes relacionados con los archivos adjuntos al correo.* Obtenido de INCIBE: https://www.incibe.es/protege-tu-empresa/blog/evitar-incidentes-relacionados-los-archivos-adjuntos-al-correo

Instituto Nacional de Ciberseguridad. (27 de febrero de 2020). *Consideraciones de seguridad para tu comercio electrónico.* Obtenido de INCIBE: https://www.incibe.es/protege-tu-empresa/blog/consideraciones-seguridad-tu-comercio-electronico

Instituto Nacional de Ciberseguridad. (16 de enero de 2020). *Las 7 fases de un ciberataque. ¿Las conoces?* Obtenido de INCIBE: https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces

Instituto Nacional de Ciberseguridad. (21 de enero de 2020). *Luchando contra la ingeniería social: el firewall humano.* Obtenido de INCIBE: https://www.incibe.es/protege-tu-empresa/blog/luchando-ingenieria-social-el-firewall-humano

Instituto Nacional de Ciberseguridad. (14 de mayo de 2020). *Seguridad en redes wifi: una guía de aproximación para el empresario.* Obtenido de INCIBE: https://www.incibe.es/protege-tu-empresa/guias/seguridad-redes-wifi-guia-aproximacion-el-empresario

Jiménez Castillo, W. (2017). *Seguridad informática o de la información en pymes.* Bogotá: Universidad Piloto de Colombia.

Jimeno Muñoz, J. (2019). *Derecho de daños tecnológicos, ciberseguridad e insurtech.* Madrid: Dykinson.

Ley Orgánica 1/2015 por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. (30 de marzo de 2015). Boletín Oficial del Estado. Madrid, España.

Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales. (5 de diciembre de 2018). Boletín Oficial del Estado. Madrid, España.

Observatorio del Sector Público. (2019). *Observatorio del Sector Público*. Obtenido de OSPI: https://www.ospi.es/es/index.html

Ratificación de Convenio sobre Ciberdelincuencia hecho en Budapest. (17 de septiembre de 2010). Boletín Oficial del Estado. Madrid, España.

Real Academia Española. (2016). *Diccionario del Español Jurídico.* Madrid: Espasa.

Roa Buendía, J. (2013). *Seguridad informática.* Madrid: McGraw Hill.

Romero Castro, M., Figueroa Moràn, G., Vera Navarrete, D., Álava Cruzatty, J., Parrales Anzúles, G., Álava Mero, C., . . . Castillo Merino, M. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Alcoy: Área de Innovación y Desarrollo, S.L.

The Cocktail Analysis. (2019). *Panorama Actual de la Ciberseguridad en España.* Madrid.