DESARROLLAR
CULTURA EN SEGURIDAD

Colección: protege tu empresa

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

ÍNDICE DE FIGURAS

1 Introducción

«Una cadena es tan fuerte como su eslabón más débil»

Esta frase tan popular significa que aunque las organizaciones inviertan mucho en dispositivos tecnológicos y en soluciones técnicas para proteger de manera adecuada los sistemas de información, si alguno de ellos falla, toda la seguridad se ve comprometida. El usuario es un eslabón más de la cadena,… y la experiencia ha ido demostrando que es uno de los eslabones más débiles, por donde esta cadena de seguridad se rompe.

Para cambiar esta situación, es necesario invertir también en la formación en seguridad a usuarios. Siendo conscientes de que:

«El usuario es el eslabón más IMPORTANTE de la cadena de la seguridad».

Tenemos que ser conscientes de que a la hora de hablar de seguridad de la información, la tecnología nunca es suficiente. Es importante, pero a la hora de la verdad los auténticos protagonistas de la seguridad en las organizaciones son los usuarios finales que son los que gestionan y utilizan los sistemas de información de nuestra organización.

2 ¿Cómo establecer una cultura de seguridad en la empresa?

Desarrollar e integrar una **cultura de seguridad** dentro de nuestra organización es uno de los objetivos más complejos de alcanzar. En primer lugar porque su aplicación requiere de unos plazos de tiempo amplios y de acciones continuadas en el tiempo; en segundo lugar, y mucho más importante, porque hablamos de personas. Conseguir que nuestros empleados interioricen en sus quehaceres cotidianos una manera de trabajar que garantice que las cosas se hacen bien en materia de seguridad de la información no es una tarea sencilla.

Habitualmente los empleados ven los protocolos de seguridad que implantamos en nuestras organizaciones como una complicación, un incordio o molestia. La percepción que tienen es que la seguridad es incómoda y dificulta sus actividades cotidianas imponiendo limitaciones. Es necesario revertir esa visión negativa y abordar las acciones necesarias para conseguir crear una auténtica cultura de la seguridad dentro de nuestra empresa.

La empresa para mantener un adecuado nivel de seguridad debe:

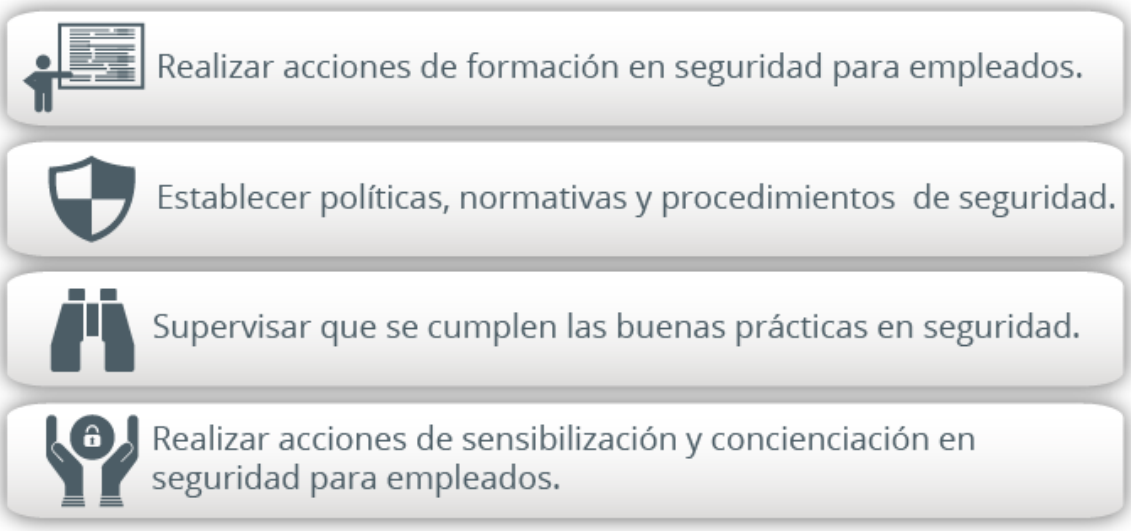

Ilustración 1: ¿Qué hacer para establecer una cultura de seguridad en la empresa?

2.1 Realizar acciones de formación en seguridad para empleados

Tradicionalmente la seguridad de la información en las organizaciones se ha entendido como un gasto que no aporta valor al negocio, pues es muy difícil ver el retorno de la inversión en medidas que no se perciben como productivas. La formación en materia de seguridad, hasta ahora ha tenido un protagonismo casi nulo en los planes de formación de las empresas. Y si se llega a abordar, ésta se realiza de manera puntual o a un grupo reducido de empleados.

De hecho, si preguntamos por iniciativas relacionadas con la **formación en seguridad**, veremos que únicamente se tratan acciones relacionadas con la seguridad en el puesto de trabajo y la prevención de riesgos laborales, dejando fuera los ámbitos de la seguridad de la información.

Con la aparición en 1999 de la LOPD (Ley Orgánica de Protección de Datos Personales) se produjo un pequeño cambio en este sentido, y las organizaciones más afectadas por el cumplimiento de esta normativa, empezaron a llevar a cabo sesiones de formación relacionadas con los requerimientos de protección de la privacidad de los usuarios.

De hecho, el Reglamento General de Protección de Datos (RGPD) [1], contempla como una obligación de nuestra empresa formar a los empleados de la organización en materia de seguridad de los **datos de carácter personal**, garantizando así que son gestionados de una manera adecuada y conforme a la ley.

Es fundamental que seamos conscientes de la importancia de formar a nuestros empleados en materia de seguridad de la información para nuestros intereses como organización, y no sólo en materia de protección de datos personales, sino también desde el punto de vista de toda la información que trata la organización: datos de facturación, tarifas, márgenes, sistemas de producción, clientes, proveedores, acuerdos, etc.

Sin embargo, no todo el personal de una organización necesita el mismo tipo ni grado de formación en materia de seguridad. La formación que necesita el personal técnico que gestiona los servidores no debe ser la misma que reciba el usuario final que sólo dispone de acceso a una pequeña parte de la información corporativa.

2.1.1 Personal técnico

El personal técnico del Departamento de Informática es quien precisa más formación en materia de seguridad y con un **mayor grado de especialización**. Debemos poner a disposición de los administradores de sistemas los recursos y mecanismos adecuados para formarse o autoformarse en aspectos relacionados con la seguridad de los sistemas y aplicaciones que dan soporte a los procesos de negocio de nuestra organización.

Dentro de estos aspectos podemos señalar algunos tan críticos como:

Ilustración 2: Formación para personal técnico

Además, la vertiginosa evolución de la tecnología exige que nuestro personal técnico deba estar en un **continuo proceso de formación**, sobre todo si nuestra organización tiene una alta dependencia de la tecnología. No sólo eso, sino que en muchos casos este personal se convierte, a falta de un proveedor de servicios especializado, en asesor de los usuarios finales de la organización en el uso de la tecnología y sus necesidades de seguridad, incluyendo por ejemplo el uso de herramientas para gestionar información en la nube.

Todo lo que hemos comentado es también aplicable si nuestra empresa ha externalizado la administración de la infraestructura TIC a través de un proveedor especializado. Debemos tener en cuenta que la empresa que lleve a cabo este servicio tendrá que ser competente en materia de seguridad de la información: no sólo debe gestionar la infraestructura TIC de la empresa de una manera eficiente; también debe hacerlo de una manera segura.

2.1.2 Usuarios finales

No debemos pensar que el personal informático debe ser el destinatario exclusivo de la formación en materia de seguridad de la información. Actualmente en las empresas la gran mayoría de sus empleados trabajan con ordenadores o con dispositivos que les permiten conectarse a los sistemas corporativos.

Por tanto, la seguridad hoy en día no se debe limitar sólo a los **aspectos técnicos**, sino que debe incorporar otros ámbitos como el **organizativo** y el **legal**, rebasando así las competencias del Departamento de Informática o sistemas. Es necesario tener en cuenta que existen departamentos como el de Recursos Humanos o el Comercial, que deben conocer aspectos vitales en la gestión de la seguridad de los datos, como el RGPD [1], con los que trabajan como parte de sus funciones cotidianas. No hacerlo puede provocar que la empresa incurra en **situaciones de riesgo**, tanto a nivel de protección de datos como a nivel de infracciones legislativas. En este caso, es necesario que algunas personas de la organización reciban formación específica e incluso contar con el asesoramiento de algún experto en legislación aplicada a la protección de datos en un entorno corporativo.

De hecho, si nuestra empresa tiene como clientes a personas físicas resulta fundamental la formación en el ámbito de **protección de datos de carácter personal**, puesto que el nivel de riesgo asociado puede ser muy alto. El tratamiento de los datos de nuestros clientes debe realizarse partiendo de unas determinadas condiciones, tanto a nivel técnico como legal, que son establecidas por el RGPD [1]. Por ejemplo, nuestro personal de atención al cliente debe estar perfectamente formado para saber cómo atender una petición de ejercicio de los derechos de acceso, rectificación, cancelación u oposición, pues existen unos plazos muy ajustados para atender este tipo de peticiones.

No obstante, no debemos limitar la formación en seguridad únicamente al correcto tratamiento de los datos personales. Existen otros muchos aspectos a considerar en la formación del personal de nuestra organización:

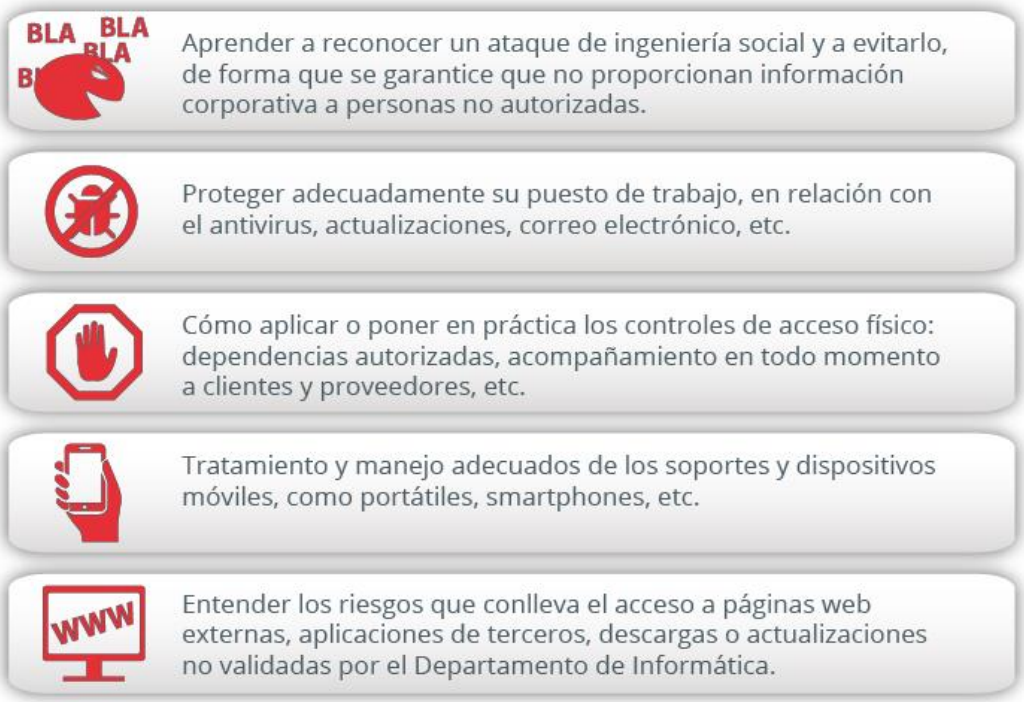

Ilustración 3: Formación para usuarios

En definitiva, todo el personal de la organización con acceso a los sistemas de información corporativos debe recibir formación relacionada con buenas prácticas en materia de seguridad en su puesto de trabajo y en el desempeño de sus funciones.

2.2 Establecer políticas, normativas y procedimientos de seguridad.

Los conocimientos adquiridos en materia de seguridad por parte del personal encargado de definir cómo se deben hacer las cosas debemos traducirlos en diferentes procedimientos y protocolos de actuación a seguir dentro de la organización.

Por ejemplo, **cuando se incorpora un nuevo empleado** a la organización, es necesario que llevemos a cabo una serie de tareas relacionadas con el proceso de alta para que pueda empezar a desarrollar sus funciones:

- **Tareas técnicas**: alta del usuario en el dominio corporativo, asignación del ordenador personal, instalación del software que necesite, permisos de acceso a carpetas del servidor, acceso a aplicaciones, etc.

- **Tareas administrativas**: el nuevo empleado deberá firmar su contrato de trabajo y demás documentación relacionada con su alta laboral, documentación relacionada con el RGPD, el **acuerdo de confidencialidad**, y

otras tareas como formación en temas de prevención de riesgos laborales, etc.

Todos estos pasos hay que formalizarlos, documentando todas las etapas, y contemplando en ellas los aspectos relacionados con la seguridad que se deben tener en cuenta y aplicar adecuadamente, sobre todo en aquellas en las que el nivel de rotación de empleados sea alto.

Lo mismo aplica a los diferentes **protocolos de actuación de la empresa**, que debemos procedimentar y documentar por escrito. Es decir, documentar cómo se deben hacer las cosas de una forma establecida y adecuada.

Y de la misma manera que documentamos **cómo se hacen las cosas**, hay que especificar **lo que se puede y lo que no se puede hacer** en la organización, con el correo electrónico, con el acceso a Internet, con los recursos corporativos, etc. Debemos escribir los **usos permitidos y aceptados** de los recursos corporativos, así como los **procesos disciplinarios o sanciones** a aplicar en caso de un uso indebido de alguno de ellos. En definitiva, debemos poner por escrito la normativa de la empresa en materia de seguridad que contemple la filosofía y cultura de la empresa, de manera consensuada con los distintos departamentos de la organización.

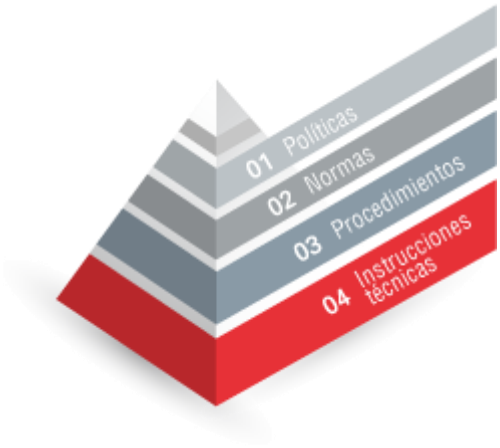

Ilustración 4: Documentos de seguridad por niveles en la organización

Dichas **normas y procedimientos** deben formar parte de la **Política de Seguridad** definida por nuestra empresa. Éste es un documento que recoge las intenciones y objetivos que la organización marca en cuanto a Seguridad de la Información y cuyo propósito es declarar formalmente que la seguridad es una parte fundamental de la cultura de nuestra empresa. Por este motivo, los procedimientos y las normativas que definamos deben ser formalmente aprobados por la Dirección de la empresa, ya que rigen el funcionamiento de la organización y aplican a todos los departamentos y usuarios sin distinción.

Es muy importante que una vez aprobadas de manera formal las normativas de uso de los recursos corporativos las comuniquemos también a los empleados. De nada sirve que se redacten y se aprueben si no son conocidas por sus destinatarios, pues no se conseguirá ni la concienciación de los empleados ni la implantación de las normativas.

De hecho, es recomendable su entrega a los empleados y que la empresa disponga de una evidencia de que esa entrega se ha producido. Para ello existen diversas fórmulas: desde la entrega de la normativa en soporte papel con acuse de recibo cuando el empleado se incorpora a la empresa, hasta que se proporcione el acceso a la parte de la Intranet corporativa en la que reside la normativa y que el empleado tenga que marcar una casilla declarando conocer y aceptar el contenido de la misma.

2.3 Supervisar que se cumplen las buenas prácticas en seguridad

La formación y la normalización de los protocolos de trabajo en nuestra empresa forman parte de los controles preventivos orientados a mejorar el nivel de seguridad de la organización. Una vez definido el marco de trabajo y trasladado a las partes afectadas, será necesario comprobar que efectivamente se está siguiendo y aplicando. Para ello, deberá existir un **Responsable de Seguridad** encargado de velar por:

- La **vigencia** y correspondiente **actualización** de las normas y procedimientos definidos, atendiendo a la detección de nuevas situaciones, de cambios legislativos u organizativos, de prácticas tecnológicas en la organización que recomienden la revisión de los mismos.

- La **implantación** de los mismos y su cumplimiento por parte de los empleados.

Este Responsable de Seguridad podría ser un «**Comité de Seguridad**» integrado por representantes de diferentes departamentos (no únicamente el Departamento de Informática o Sistemas) en el que debería figurar también una representación de la Dirección.

Por otro lado, también dispondremos de mecanismos para comprobar que los empleados siguen los procedimientos definidos y que cumplen las normativas vigentes. Para ello realizaremos **auditorías**, ya sean **internas o externas**. Además podemos emplear **herramientas de auditoría informática** que registren las operaciones que realizan los usuarios en las aplicaciones y bases de datos corporativas, con objeto de garantizar la trazabilidad de esas operaciones.

En caso de querer comprobar el correcto uso de los recursos que se ponen a disposición de los empleados para el desempeño de sus funciones, podemos implantar diferentes soluciones tecnológicas, que además nos ayudarán a impedir que se realicen acciones que no están permitidas en las políticas de la empresa. Es muy

importante destacar que, para poder llevar a cabo este tipo de análisis con **herramientas de monitorización**, es necesario haber informado previamente y de una manera clara a los empleados de su existencia y finalidad.

En relación con el **control del uso del correo electrónico**, debemos tener en cuenta que la situación es más delicada, dado que habitualmente los empleados dan al correo corporativo un uso mixto profesional/privado. Esta situación puede provocar un conflicto entre el derecho al control del uso de los recursos corporativos que el Estatuto de los Trabajadores otorga a las empresas y el derecho a la privacidad de los empleados.

Actualmente no existe legislación que regule este acceso al correo electrónico, pero existe doctrina del Tribunal Constitucional que determina que el uso de esta potestad por parte de la empresa debe basarse en un principio de proporcionalidad; es decir, se considera «proporcionada» su utilización cuando la empresa tiene sospechas fundadas de que se está haciendo un uso no autorizado de este recurso corporativo. En cualquier caso, la empresa deberá haber informado previamente de manera clara del uso que permite para el correo electrónico corporativo.

Es conveniente que, con independencia de cómo hayamos trasladado a los empleados la normativa existente, regularmente se les recuerde la existencia de dicha normativa y se les proporcione un enlace al repositorio en el que se puede consultar.

Habitualmente, el conocimiento por parte de los empleados de la existencia de sistemas de monitorización o de un **régimen sancionador asociado al incumplimiento** de las normas tiene un efecto disuasorio, que también debe formar parte de la cultura de la seguridad.

2.4 Realizar acciones de sensibilización y concienciación en seguridad para empleados

Hasta ahora, hemos tratado la necesidad de que determinadas personas en la organización reciban formación en materia de seguridad, en sus diferentes vertientes (técnica, organizativa y legal). Se ha subrayado también la necesidad de definir una estructura organizativa de seguridad así como un sistema de normas y procedimientos detallados y estandarizados.

Pero todo esto no es suficiente para que el ámbito de la seguridad se integre en la cultura de la empresa. El establecimiento de normas y procedimientos, la formación del personal encargado de definirlos, la existencia de un Comité de Seguridad que dé soporte a todo lo anterior, son una condición necesaria pero no suficiente.

Sea cual sea nuestro negocio, es importante que la cultura de la seguridad sea una de las bases de la filosofía de la empresa. Por este motivo, es fundamental que la Dirección se asegure de la **implicación de todos los empleados**. Éstos deben ser conscientes de la importancia que tiene la información que manejan, tanto la propia como la de los terceros con los que hacen negocios (clientes, proveedores,…). Para conseguir esta implicación, es necesario emprender **acciones de sensibilización y concienciación**, necesarias para el mantenimiento de los niveles de seguridad adecuados.

Si los empleados no se consideran parte fundamental de este proceso, el fracaso está garantizado, ya que ellos son los grandes protagonistas de esta historia. No sólo porque son los encargados de cumplir las normas y los procedimientos, sino porque también son parte fundamental en el mecanismo interno de revisión y mejora proactiva del nivel de seguridad.

En algunos casos los empleados no necesitan «formación en seguridad» en el sentido tradicional, sino «información sobre seguridad». Se trata sobre todo de informar a los empleados de cómo aplicar ciertos aspectos relacionados con la seguridad en el desempeño cotidiano de sus funciones. **Nuestro objetivo debe ser concienciarles sobre el papel que juegan en el mantenimiento de la seguridad de la información de la empresa.**

A la vez que la tecnología evoluciona, también evolucionan los riesgos asociados a la seguridad de la información. Un ejemplo es el ***BYOD*** (*Bring Your Own Device*), que consiste en la utilización de dispositivos propios del empleado como *smartphones* o *tablets*, que se conectan a la red corporativa, ya sea para leer el correo electrónico, acceder a servidores de ficheros o trabajar con documentos ofimáticos. La conexión a la red corporativa de dispositivos «no controlados» o el almacenamiento de información corporativa confidencial en estos dispositivos sin las adecuadas medidas de seguridad son aspectos sobre los que hay que concienciar a los empleados, establecer políticas de seguridad para estas situaciones y, en caso de ser necesario, crear medidas de seguridad para evitarlo.

También ha proliferado el uso de **técnicas de ingeniería social**, por parte de los ciberdelincuentes, para conseguir acceso a la información o a los sistemas corporativos. Estas prácticas se traducen, por ejemplo, en llamadas telefónicas supuestamente realizadas por el departamento de TI solicitando las credenciales del empleado para una prueba que se está realizando, o el envío de un correo electrónico suplantando a un remitente legítimo y conocido con un documento anexo que contiene un malware.

Es necesario que los empleados conozcan los riesgos a los que están expuestos, para que sepan reaccionar correctamente ante posibles situaciones similares. Si no conocen estas amenazas, no podrán identificarlas ni protegerse frente a ellas.

A continuación se citan algunos temas sobre los que hay que concienciar a los empleados:

- Uso seguro de redes wifi.
- Uso seguro del correo electrónico.
- Prácticas de navegación segura.
- Identificación de virus y malware.
- Gestión de contraseñas.
- Clasificación de la información.
- Borrado seguro de la información.
- Uso de dispositivos USB.
- Seguridad en dispositivos móviles.
- Uso de programas de mensajería instantánea.
- Riesgos de las redes sociales.
- Técnicas de ingeniería social.

Los temas a tratar no sólo están relacionados con el uso de la tecnología, sino que abarcan otros ámbitos:

- Mesas limpias.
- Destrucción segura de la documentación en soporte papel.
- Posibles escenarios de fuga de información.

El objetivo es que el empleado adopte una serie de **hábitos personales «saludables» en materia de seguridad** tanto a nivel personal como profesional, lo que redundará también en la mejora del nivel de seguridad de la empresa.

Si la formación se plantea como un trámite a cumplir, el empleado también lo vive igual; se limita a asistir a la charla, sin que la acción formativa tenga ninguna repercusión en sus hábitos. Es necesario dar al plan de concienciación la importancia que merece, y diseñar acciones formativas adaptadas y enfocadas a la realidad de la organización.

A la hora de abordar las acciones de concienciación y sensibilización de los empleados es recomendable evitar técnicas de formación «tradicionales» (como sí se usan en las acciones descritas en el apartado de Formación) y centrar estas acciones en la revisión de casos prácticos que representen riesgos a los que se pueda enfrentar en el día a día de su trabajo, lo que permitirá que se sienta identificado y que se involucre de manera más activa. Las acciones deben presentar tanto las amenazas, para su identificación

por parte del empleado, como las medidas de seguridad y pasos a dar para evitarlas y protegerse en cada caso. También puede ser interesante distribuir posters, trípticos u otros materiales recordando los principales consejos de seguridad.

En algunos casos, y en función del tamaño de la organización, se pueden definir acciones de concienciación paralelas que centren su enfoque en aquellos empleados con mayor acceso a información de carácter sensible: **el personal directivo de la compañía.**

En el caso particular del personal directivo es necesario que las acciones se centren en un enfoque personalizado, teniendo en cuenta su problemática, su entorno de trabajo, sus usuarios de confianza y los riesgos específicos asociados. Además, dichas acciones no deben reducir su alcance al entorno corporativo, sino que deben adaptarse a las características inherentes del trabajo del directivo, con propuestas y medidas de seguridad para éste y todo su entorno.

La concienciación incrementa el nivel de seguridad de la organización. Si incrementamos la seguridad corporativa mejoramos nuestra imagen como empresa ante nuestros clientes. Indudablemente estos aspectos inciden positivamente en los procesos de negocio de la empresa. Por tanto, **CONCIENCIAR EN SEGURIDAD DE LA INFORMACIÓN ES RENTABLE PARA LA EMPRESA**.

3 Referencias

[1]. BOE. Legislación. Códigos. Protección de datos de carácter personal. [https://www.boe.es/legislacion/codigos/codigo.php?id=55&modo=1&nota=0&tab=2]

[2]. BOE, Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico [https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758]

[3]. Incibe, Kit de Concienciación [https://www.incibe.es/protege-tu-empresa/kit-concienciacion]