UNIVERSIDAD MIGUEL HERNÁNDEZ
FACULTAD DE CIENCIAS SOCIALES Y JURÍDICAS DE ELCHE
GRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS
TRABAJO DE FIN DE GRADO

IMPLANTACIÓN DE CIBERSEGURIDAD

AUTOR: Cerdán Fernández, Salvador
TUTOR: Miralles Soler, Ramón
Curso Académico 2022-2023
Convocatoria Junio

Índice

1. Resumen

En el actual panorama empresarial, las organizaciones desarrollan su actividad en un entorno cada vez más tecnológico y digitalizado. Sin embargo, este entorno conlleva nuevos riesgos y desafíos que pueden tener consecuencias devastadoras tanto a nivel económico como reputacional. En este contexto, los datos se han convertido en un activo de gran valor para las organizaciones.

Ante esta realidad, resulta imprescindible contar con un plan de seguridad informática sólido y eficiente que permita a las organizaciones protegerse de estos riesgos, garantizar una gestión adecuada de los datos y adaptarse de manera ágil a los rápidos cambios tecnológicos que caracterizan este entorno.

Por ello, el presente documento tiene como objetivo desarrollar una estrategia enfocada en la ciberseguridad de las organizaciones. Para lograrlo, es necesario profundizar en el conocimiento de la ciberseguridad y comprender los términos asociados, como los ciberataques y los riesgos cibernéticos. Asimismo, es fundamental comprender las consecuencias que pueden sufrir las organizaciones cuando son víctimas de un ciberataque, ya que esto permite tomar conciencia de la importancia de protegerse adecuadamente.

Una vez adquirido este conocimiento, se abordará el diseño de un plan de ciberseguridad que garantice la protección de las organizaciones. Es importante destacar que este plan no se enfocará en aplicaciones informáticas específicas, sino en los procedimientos y las prácticas que deben implementarse para asegurar la

ciber protección y la gestión adecuada de los datos. Además, se promoverá una cultura innovadora en torno a la ciberseguridad, fomentando la conciencia y la participación de todos los miembros de esta.

Para respaldar las estrategias propuestas, se analizarán datos y tendencias de diferentes empresas en distintos países, lo que permitirá identificar las medidas más efectivas y comprender cómo se benefician las organizaciones que las han implementado.

A continuación, se detallará el proceso de implantación mediante la propuesta de diferentes métodos y modelos utilizados en dicho proceso, los cuales servirán de guía para aquellas organizaciones que estén enfocadas en elaborar e implementar un plan de ciberseguridad. Se prestará especial atención a la importancia del liderazgo y la comunicación como variables esenciales en el proceso de implantación estratégica y en la gestión de una crisis de ciberseguridad con el objetivo de mitigar los distintos efectos en los diversos grupos de interés.

El plan diseñado y el proceso de implantación se basan en diferentes procesos de control para asegurar que el control de toda la estrategia no sea una actividad separada, sino que esté intrínsecamente incorporado en la propia estrategia, fomentando así una cultura de control y mejora continua. Esto implica detectar y abordar cualquier desviación o contratiempo de manera oportuna. Asimismo, se revisarán todas las medidas implementadas para garantizar dicho control, considerándolas no solo como una parte del plan, sino también como un

proceso independiente y complementario que garantice el éxito y la adaptación de la estrategia a largo plazo.

Además, es importante resaltar la relevancia del aspecto presupuestario en la ciberseguridad empresarial. Se destacará la cantidad de recursos económicos que las empresas destinan a esta actividad, reconociendo que la inversión en ciberseguridad es cada vez más significativa. Se analizarán los motivos que respaldan esta tendencia y, asimismo, se abordarán las razones por las cuales se espera que esta asignación presupuestaria continúe en aumento en el futuro, ya que la ciberseguridad se ha convertido en una prioridad estratégica para las empresas en la era digital.

La ciberseguridad se ha convertido en una preocupación fundamental para las organizaciones, y su correcta implantación contribuye a proteger los activos y la reputación de la organización en un entorno digital cada vez más complejo y desafiante.

2. ¿Qué es la ciberseguridad?

En plena revolución industrial 4.0 las empresas están incorporando nuevas tecnologías en todos sus procesos (productivo, administrativo…). Estas tecnologías de la información facilitan la recolección y gestión de datos, lo que permite ser más eficiente y flexible. Estos datos se han convertido, por tanto, en uno de los activos más valiosos para las compañías.

Estas nuevas tecnologías pueden ser atacadas con el objetivo de conseguir la información que en ellas se almacena, estos ataques realizados se denominan “ciberataques”. Según la empresa *International Business Machines Corporation* (IBM) los ciberataques son intentos no deseados de robar, exponer, alterar, inhabilitar o destruir información mediante el acceso no autorizado a los sistemas.

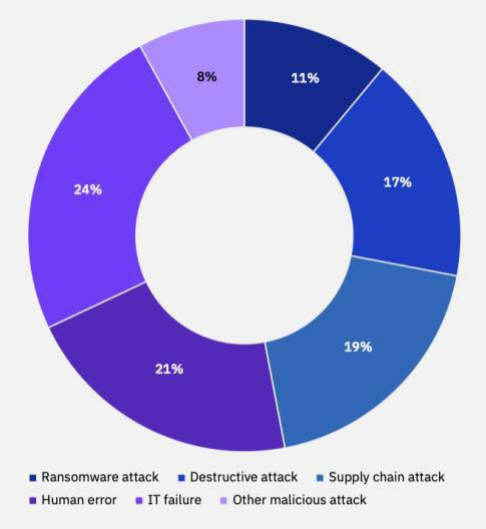
Dado la importancia que tienen los datos y las tecnologías de la información, las empresas ya no están solamente expuestas a los riesgos existentes por el hecho de operar en un mercado si no que aparecen otros nuevos denominados “ciberriesgos”. Centrándonos en el ámbito empresarial, se considera ciberriesgo a la amenaza de una posible interrupción de la actividad empresarial o daño en la reputación de una compañía debido a un ciberataque (Grupo atu, 2022).

Por tanto, surge la necesidad de protegerse de estos riesgos y ataques, y cada vez un mayor número de empresas recurren a implementar mecanismos de “ciberseguridad”. La ciberseguridad es la práctica de proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales (Amazon Web Services, s.f.).

3. Ciberataques y riesgos

Parece conveniente conocer cuáles son aquellos ciberataques y ciberriesgos de los cuales deben defenderse las empresas.

Ilustración 1 Tipos de ataques experimentados por organizaciones



Nota. International Business Machines Corporation. (Julio de 2022). *Cost of a data breach 2022*. Sitio Web de IBM: https://www.ibm.com/reports/data-breach

En la ilustración 1 se puede observar cómo un 21% del total de incidentes experimentados por organizaciones son causados por errores humanos y un 24% por errores de las tecnologías de la información. Además, se observa como un 19% es provocado por un socio comercial que ha sido atacado.

En ambas figuras se puede observar la importancia que tienen algunos ciberataques como son el ransomware, el malware y el phishing. Este último representa el 19% de las amenazas más habituales como puede observarse en la ilustración 2, dada su sencillez y bajo coste para llevarlo a cabo.

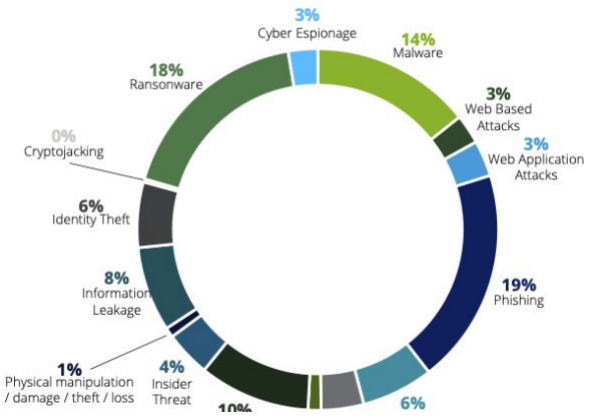
A continuación, se destacan algunos tipos de ciber ataques y ciber riesgos:

- Malware y ransomware

  Dan acceso a los atacantes a datos o causan daños en los sistemas informáticos.

- Phishing

Ilustración 2 Porcentaje de amenazas más habituales



Nota. Deloitte. (2022). *El estado de la ciberseguridad en España* . Sitio web de Deloitte: https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html

Trata de engañar a los usuarios para que “voluntariamente” den sus datos a los atacantes o descarguen un programa que le de acceso a los mismos. Suele ser habitual a través de correos electrónicos o SMS que parecen ser de una empresa legítima.

- Denegación de servicio distribuido (DDoS)

  Sobrecarga los servidores de una empresa con solicitudes de acceso falsas para que la empresa no pueda acceder a la información contenida en los servidores. Puede provocar que la empresa no sea capaz de realizar sus tareas más cotidianas.

- Amenazas persistentes avanzadas (APT)

  El atacante se “cuela” en el sistema de la empresa con la intención de permanecer en él sin ser detectado durante el mayor tiempo posible y robar datos.

- Amenaza interna

  Esta amenaza puede ser consciente si alguien de dentro de la organización proporciona datos a terceras personas o inconsciente si por algún error humano terceras personas son capaces de colarse en los sistemas de la empresa.

- Ataques de día cero.

  Si la empresa se encuentra en un momento de vulnerabilidad ya que se ha defendido o se está defendiendo de un ciberataque, se aprovecha está situación para lanzar otro ataque.

- Fallos del sistema.

  Debido a errores en los sistemas la empresa puede verse envuelta en una situación de perdida de datos, que, aunque no son robados, nos encontramos ante una situación igual de perjudicial y sobre la que se requiere protección, ya que los datos son un activo valioso.

4. Consecuencias de un ciber ataque

Según el Informe de Ciber preparación de Hiscox 2022, la amenaza ciber ya es considerada como el riesgo número uno para las empresas, de ello se deriva la importancia de contar con una estrategia de ciberseguridad, pues las consecuencias de un ciberataque para las compañías pueden ser numerosas y devastadoras.

Para comprender la importancia de desarrollar una estrategia de ciberseguridad, tanto en grandes empresas como en pymes, es importante profundizar en cada una de las consecuencias en las que se pueden ver envueltas durante y después de un ciberataque.

La consecuencia que parece más evidente es el aumento de costes, que puede provocar problemas de liquidez y si persiste a largo plazo, de solvencia. Una de cada cinco empresas atacadas dice que su solvencia se vio amenazada (HISCOX, 2022), aunque esto depende en gran medida de la capacidad de la empresa de gestión de los costes extraordinarios, así como de su liquidez y del fondo de maniobra disponible para hacer frente a estos costes no ordinarios.

Los costes que se derivan de un ciberataque son innumerables, aunque podemos destacar los costes de detección, de erradicación, de recuperación de datos dañados o perdidos, de reemplazo de equipos, de comunicación a los clientes afectados de que sus datos han sido comprometidos, así como los costes derivados de la pérdida de clientes debido al ataque, la perdida de socios comerciales y la

búsqueda de otros nuevos, etc. También es importante no olvidar los costes que se pueden derivar de multas impuestas por organismos públicos por el incumplimiento de la legislación vigente como el Reglamento General de protección de datos. Por ejemplo, Meta en relación con Instagram por presuntos fallos en la protección de datos personales de niños recibió una multa de 405 millones de euros impuesta por el Comisario de Protección de Datos irlandés (Hill, 2023), y es que de hecho, los reguladores de datos europeos impusieron multas por un importe récord de 2.920 millones de euros, un 168% más que en 2021 (Hill, 2023), por lo que este tipo de costes tampoco pueden pasar desapercibidos.

Según la empresa IBM en su reporte sobre el coste de una filtración de datos de 2022 el coste medio global de una filtración es de 4.35 millones de USD. Los costes pueden ascender tanto que una empresa del Reino Unido sufrió costes totales por ataque por un importe de seis millones de euros (HISCOX, 2022).

No solo las compañías se encuentran con una gran cantidad de costes si no que estos, además, van en aumento. En el último año, el coste mediano de todos los ciberataques sufridos por cada empresa aumentó un 30% (HISCOX, 2022).

Ilustración 3 Coste medio total de un ciber incidente

Medido en millones de dólares

Nota. International Business Machines Corporation. (Julio de 2022). *Cost of a data breach 2022.* Sitio Web de IBM: https://www.ibm.com/reports/data-breach

En la ilustración 3, se puede observar la evolución de los costes totales por filtraciones de datos en los últimos años. Cabe destacar el incremento de costes producido en los años 2020 y 2021 derivados del Covid-19 que obligó a las empresas a acelerar el proceso de

digitalización y a la incorporación de nuevas tecnologías de la información, lo que las dejo más expuestas a los ciberriesgos y permitió a los ciberdelincuentes aumentar sus ataques sobre estas.

Otra de las consecuencias que puede sufrir una empresa al ser atacada es la pérdida de confianza por parte de sus grupos de interés y el consiguiente daño en la imagen de la empresa y en el posicionamiento si se posiciona como una empresa “segura” en cuanto a la información digital se refiere.

Los consumidores cada vez están más comprometidos con la privacidad y el uso que se hace de sus datos, por lo que verse envuelto en una filtración de datos no es una buena publicidad para la compañía. Conocer que sus datos han sido expuestos puede llevar a los clientes a no querer mantener su relación comercial con la empresa por muy bueno que sean los productos que comercializa o los servicios que ofrece, buscando a algún competidor que cubra su necesidad. De hecho, una de cada tres pymes reconoce que ha perdido clientes como resultado de un ciberataque (HISCOX, 2022). Y no solo debemos centrarnos en los clientes perdidos si no en la dificultad añadida tras un ciberataque para la captación de nuevos clientas debido a la inseguridad de que algo así pueda volver a pasar.

En esta situación la empresa no solo puede perder clientes si no también socios comerciales, ya que los ciber atacantes pueden conseguir atacar a un socio comercial a través de los canales que estos compartes con la empresa atacada para poder llevar a cabo su relación comercial. Por ejemplo, algunas empresas comparten aplicaciones informáticas con sus proveedores para realizar un servicio

post venta o incluso para la contratación de servicios, si un atacante consigue infiltrarse en el sistema informático de la empresa le será más sencillo infiltrarse a través de estas aplicaciones en los sistemas de sus socios comerciales.

Esto también puede influir en la creación de valor de la empresa provocando que los accionistas/propietarios no consigan sus objetivos y se empiece a elevar su coste de oportunidad por invertir en la empresa atacada y no en otro tipo de inversión, por lo que pueden decidir retirar dicha inversión para realizarla en otro activo.

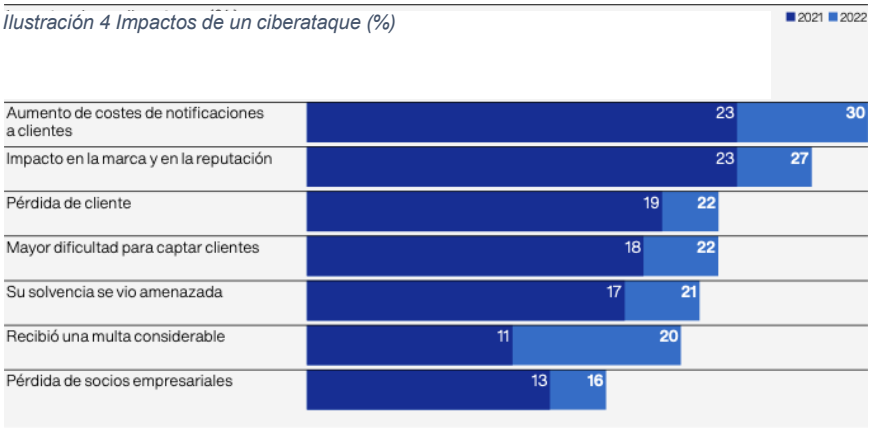
Si hablamos de empresas cotizadas, el daño en la reputación de la empresa va a afectar al precio de cotización de las acciones y, por tanto, perjudicando a los accionistas que verán sus inversiones disminuidas. Cuando se trata de recuperar la imagen perdida se pueden tardar años.

La información que las empresas obtienen acerca de las preferencias de sus consumidores, frecuencia y patrones de compra, uso de sus productos, comportamiento de compra e incluso del “feedback” que generan, entre otros, es una fuente de ventaja competitiva. La información es tan importante para las empresas que son numerosas aquellas que se dedican a vender los datos de sus clientes como es el gran ejemplo de aquellas que sustentan las redes sociales. Pero no solo debemos centrarnos en los datos generados por los clientes si no también en aquellos generados por la propia empresa y los empleados de esta, pues estos datos pueden ayudar a optimizar procesos dentro de la organización, reduciendo costes, aumentando la flexibilidad, etc.

Saber lo que otros no saben es una fuente de ventaja competitiva que permite satisfacer mejor y más eficientemente que la competencia las necesidades de los consumidores, por tanto, podremos imaginar el daño que puede causar que debido a un ataque informático la información de la que disponía la empresa y el tan importante “Know How” terminé vendida a través de internet o simplemente publicada en la red.

Por último, es importante el tiempo que se dedica a la detección y a la erradicación del ataque pues afecta directamente a la actividad de la empresa. En algunos casos el ciber atacante puede provocar la paralización de su actividad pues los empleados, por ejemplo, no pueden acceder a las aplicaciones básicas que permiten desarrollar la actividad normal de la empresa como sería el caso de un ataque DDoS. En este caso es crucial el tiempo que dure el ataque ya que afecta directamente a la interrupción de la actividad de la empresa, las consecuencias podrían ser catastróficas, de hecho, el 71% de los CISO considera que la interrupción de las operaciones de negocio se alza un año más como el riesgo que más preocupa en sus compañías (Deloitte, 2022).

Ilustración 4 Impactos de un ciberataque (%)



Nota. HISCOX. (05 de 2022). *Informe de Ciberpreaparación de Hiscox 2022.* Sitio web de Hiscox: https://www.hiscox.es/informe-de-ciberpreparacion-de-hiscox-2022

En la ilustración 4, podemos observar el impacto de alguna de las consecuencias mencionadas anteriormente y su evolución entre los años 2021 y 2022. Cabe destacar el aumento del impacto de las multas que creció de un 11% a un 20% y como han aumentado los costes de notificación de los clientes desde un 23% a un 30%, lo que indica que las empresas están optando por notificar a los clientes lo ocurrido en vez intentar ocultarlo.

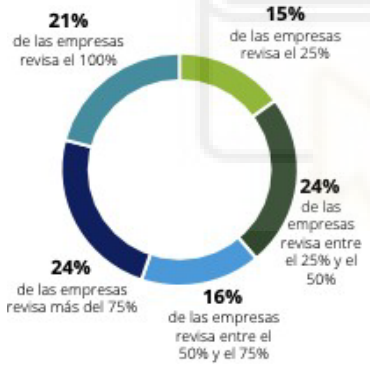
5. Plan de ciberseguridad diseñado

Una vez descritos los ciberriesgos a los que está expuesta una empresa gracias a la situación actual y las consecuencias que se pueden derivar de un ataque, profundizaremos en una serie de acciones que pueden ayudar a las organizaciones a prevenir estos riesgos, tenerlos más presentes y, por tanto, poder combatirlos de mejor manera y reducir aquellas consecuencias en las que se pueden encontrar envueltas.

Una de las primeras dudas que pueden surgir al implantar diferentes aplicaciones para proteger los equipos y al empezar a desarrollar un plan de ciber seguridad es si lo que tenemos realmente funciona y si funcionará ante un futuro

ataque. Por lo que la primera medida a adoptar son las **pruebas de ataques periódicas**, y es que no hay mejor manera de probar lo que se tiene, sino que, sometiéndolo a una situación de estrés, parecido a como se hace en otras situaciones, por ejemplo, con los simulacros de incendios. No solamente nos sirve con tener las aplicaciones necesarias para protegernos si no que revisar nos asegura que todo funciona como debe y que ante un ataque todo va a ir como debería ir, no conviene enterarnos de que algo no funciona cuando se produce un ataque pues derivaría en un aumento de las consecuencias y del aumento de una variable fundamental como es el tiempo.

Ilustración 5 Porcentaje de empresas que revisa sus aplicaciones críticas



Nota. Deloitte. (2022). *El estado de la ciberseguridad en España.* Sitio web de Deloitte: https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html

En ilustración 5, se aprecia como solamente el 21% de las empresas revisa el 100% de sus aplicaciones críticas y el 39% de las empresas revisa menos de la mitad de estas aplicaciones. Estos datos resultan más que preocupantes ya que revisar las aplicaciones y someter el proceso a un simulacro periódico puede beneficiar a la empresa en varios aspectos. En primer lugar, permite acostumbrarse al proceso y de esta manera que no cunda el pánico si se produce un ataque real dentro de la organización y que cada persona conozca cuál es su deber ante esta situación y como debe de comportarse y actuar, por lo que también ayuda a que cada uno conozca su función en tal situación y que es lo que se espera de él/ella. Además, nos permitirá conocer si el proceso diseñado funciona correctamente, si las aplicaciones destinadas a la defensa ante los ataques son válidas o fallan en algún punto y si es necesaria su

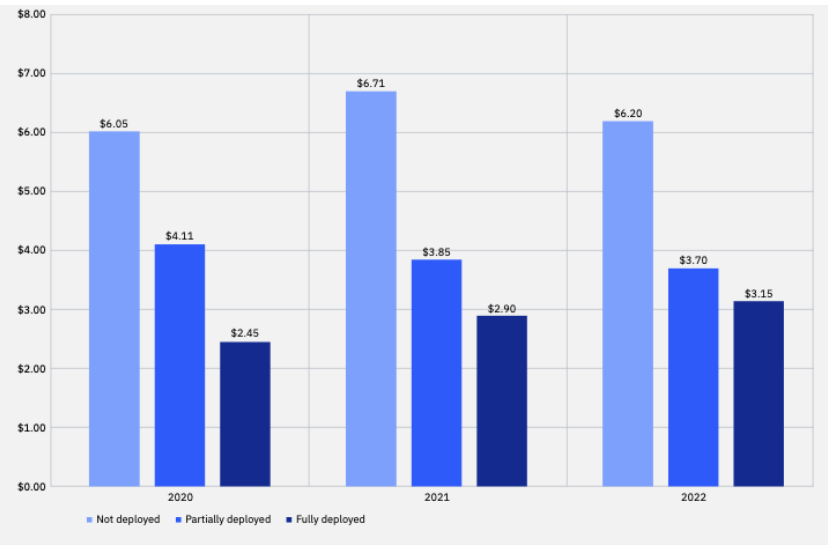
actualización. En conclusión, permitirá sacar conclusiones acerca de si estamos o no preparados para un posible ataque, pero no solo eso, ya que también podremos tener en cuenta si el proceso de defensa es eficiente en cuanto a recursos y tiempo empleado y si, por tanto, hay algo que se puede mejorar.

También ayudará a fomentar la cultura de la empresa entorno a la ciberseguridad, al tenerla más presente periódicamente y recordar a los equipos como deben actuar ante un ataque así cómo recordar de qué manera deben evitar que se produzca. De esta manera, aseguramos que los planes de ciberseguridad no caigan en el olvido ya que se convertirán en parte de la cultura.

Si seguimos por la línea de aquellas acciones relacionadas directamente con los ataques, otra medida fundamental es su pronta identificación. Con ello, se reduce el tiempo de duración del ataque que de media se sitúa en 277 días, de los cuales 70 corresponden a su identificación (International Business Machines Corporation, s.f.), por tanto, reduciendo el tiempo de duración conseguimos aminorar las consecuencias, sobre todo los costes derivados del ataque. Esto se puede conseguir mediante inteligencia artificial y con personal encargado de la ciberseguridad.

En primer lugar, la inteligencia artificial encargada de la seguridad es una nueva tendencia que cada vez está ganando más fuerza y puede que sea la opción más interesante, porque no solo ayuda a la empresa a identificar un ataque, sino que incluso puede llegar a identificar como van a atacarla en el futuro, es decir, es capaz de encontrar un punto débil antes de que otros lo hagan permitiendo a la empresa “jugar” con ventaja.

Ilustración 6 Coste medio de un ataque según el nivel de AI y automatización desarrollado



Medido en millones de dólares

Nota. International Business Machines Corporation. (Julio de 2022). *Cost of a data breach 2022*. Sitio Web de IBM: https://www.ibm.com/reports/data-breach

En la ilustración 6, se puede observar la reducción de costes medios que experimenta una empresa que ha desarrollado una inteligencia artificial encargada de la ciberseguridad y aquellas empresas que no lo han hecho o que la tienen parcialmente desarrollada. En 2022 las empresas con inteligencia artificial totalmente desarrollada se ahorraron de media 3.05 millones de dólares frente a aquellos que no la tienen, esto deja ver los beneficios que esta medida puede aportar a la empresa.

Por otro lado, contar con un equipo de **personas** encargadas de la ciberseguridad en la empresa es algo que a las organizaciones que cuentan con ellos les supone un ahorro medio de 2.66 millones de dólares frente a aquellas empresas que no lo tienen (International Business Machines Corporation, s.f.). Este equipo puede encargarse de que las normas y el plan de ciberseguridad se están cumpliendo, revisar las aplicaciones y el sistema en busca de intrusos y de garantizar su buen funcionamiento, incluso en aquellos casos con los que se cuenta con una inteligencia artificial que revise los sistemas el equipo humano siempre será necesario para revisar que esta funcione correctamente, para supervisar, tratar de

ayudar al resto del personal con las casuísticas del día a día, dar formación, etc. En plena revolución industrial 4.0 las utilidades que puede ofrecer tal equipo son innumerables.

Al pensar en un nuevo equipo a introducir en la organización parece evidente realizar la siguiente pregunta *¿formamos un equipo interno o lo subcontratamos?* Pues se observa que lo más habitual es externalizar entre el 50% y el 80% del personal de ciberseguridad, lo cual evidencia la necesidad de hacer uso del talento externo para poder cubrir las capacidades internas en ciberseguridad (Deloitte, 2022). Esto es debido a que actualmente existe una reducida oferta de talento formado en esta materia en comparación con la demanda de este, por lo que las empresas aun teniendo los recursos para ello, se ven incapaces de conseguir dicho talento por lo que la opción que les queda es externalizarlo. Además, cuando nos encontramos en una situación de escasez de talento las empresas van a necesitar más recursos para poder captarlo, por lo que en muchas ocasiones puede que externalizarlo sea la opción más razonable.

Una posible solución ante este problema es que la empresa opte por formar a personal dentro de la organización en materia de ciberseguridad y desarrollar su propio talento interno, con lo que permitiría a la empresa desarrollar la carrera de las personas enfocada a sus necesidades y, a la vez, también ofrecerá a los empleados con conocimiento en materias similares la capacidad de desarrollar su carrera. Para ello, se deberá contar con el apoyo de la alta dirección ya que conllevará tiempo y recursos la formación de dicho personal.

De todas formas, la empresa siempre puede optar por externalizar ciertas funciones o incluso “auditores” de ciberseguridad que pongan a prueba los sistemas

y el trabajo del equipo interno. Por lo que parece que lo ideal puede ser externalizar parte del trabajo.

No solo debemos centrarnos en el personal encargado directamente de la ciberseguridad sino de todo el personal de la empresa, ya que como se mencionó al principio de este documento el 21% del total de incidentes experimentados por organizaciones son causados por errores humanos, por tanto, la formación es una variable clave. Se debe ofrecer al personal la **formación** necesaria para que se conviertan en una barrera contra cualquier ataque y dejen de ser uno de los puntos más débiles en materia de ciberseguridad en la empresa. Las empresas que imparten más de 20 horas anuales de formación y concienciación a sus empleados han recibido únicamente el 15% de los incidentes sufridos en el último año (Deloitte, 2022), por lo que, si tenemos en cuenta que por lo general las iniciativas de concienciación y formación suelen requerir de poca inversión frente a la gran efectividad que presentan, hace que el aumento de nivel de madurez en ciberseguridad de los empleados y, por ende, su nivel de ciber conciencia deba priorizarse en los planes directores de ciberseguridad anualmente (Deloitte, 2022). En la mayoría de los casos son acciones que pueden ser tan simples como no abrir enlaces de correos sospechosos o correos que no pertenecen a la organización o no utilizar el disco duro que se usa en la empresa en cualquier otro ordenador, acciones sencillas que pueden ser llevabas a cabo por los empleados sin mayor dificultad pero que pueden causar una gran diferencia.

Aunque pueden ser acciones relativamente simples de llevar a cabo es necesario crear el hábito en todo el personal de la organización e interiorizar dichas acciones. Una de las formas en las que se puede conseguir que se preste atención a esto y que los empleados interioricen la ciberseguridad como una parte esencial de la organización es uniéndola a una retribución variable. Algunas empresas utilizan este tipo de retribución variable para conseguir diferentes objetivos, por ejemplo, algunas organizaciones comparten una prima de progreso en la que los empleados participan en los beneficios obtenidos por la empresa en un determinado periodo de tiempo pero el grado en el que estos participen puede estar asociado a otras variables, como los accidentes laborales, si en el periodo de tiempo establecido se producen accidentes el porcentaje de participación en los beneficios será menor. De esta manera, se incentiva a los trabajadores a tener en mente la seguridad, ya no solo por los evidentes beneficios que no tener accidentes tiene para la propia persona, sino que también por el echo de tener una participación mayor en los beneficios. La misma idea se plantea en torno a la ciberseguridad ya que fuerza al personal de la organización a cumplir con las medidas de ciberseguridad, además motiva para su cumplimiento, y ayuda a crear ciber-cultura al conseguir que la ciberseguridad este de una manera más presente en la organización. Según el informe *El estado de la ciberseguridad en España* de la empresa Deloitte en 2022, las empresas más concienciadas y con mayor nivel de ciberseguridad lideran la iniciativa de asignar una parte de la retribución variable del sueldo de todos los empleados si estos cumplen con los objetivos de ciberseguridad de la organización. Por tanto, parece conveniente unir una parte de la retribución

variable al número de incidentes de ciberseguridad para conseguir que los empleados cumplan con las medidas establecidas por la empresa.

Otra cuestión que debe ser analizada es la cantidad de **datos** que la empresa va a recopilar. En el informe *El estado de la ciberseguridad en España* de la empresa Deloitte en 2022, se llega a la conclusión de que las empresas están empezando a buscar un equilibrio correcto entre la recopilación de los datos de clientes (para ayudar al negocio) y que estos sean los mínimos necesarios (para contentar a los usuarios y disponer de menos información sensible a ser fugada de la compañía). En este sentido, el 91% de los encargados de ciberseguridad considera que sí se está llegando a dicho equilibrio (Deloitte, 2022). En resumen, ni muchos ni pocos, los necesarios. No todos los datos son valiosos para las organizaciones y, por tanto, mantener aquellos datos que no son valiosos y no aportan valor a la organización no tiene sentido, ya que aumentan los costes de conservación y mantenimiento de los datos, convirtiéndolos en un pasivo, así como las consecuencias ante una filtración de datos ya que es más información fugada de la organización. Los datos que sí son valiosos pueden ser usados y rehusados, incluso con varios propósitos en paralelo. El valor de los datos de calidad se incrementa con su uso y pueden ser compartidos sin que se pierda su valor; a mayor uso los costes marginales se achatan mientras el valor económico crece (Berrocal, 2022). Estos datos valiosos como cualquier activo requieren de inversiones para mantener e incrementar su valor, además son un activo perecedero, mientras más tiempo se conserven, mayor riesgo de volverse obsoletos y perder su utilidad (Berrocal, 2022).

La elección de los datos a conservar por la empresa es tremendamente importante, se deben eliminar aquellos datos que no son valiosos y que no aportando valor pueden convertirse en un pasivo, lo que además reducirá las consecuencias ante una fuga de datos al disminuir el número de información comprometida. Por otro lado, aquellos datos valiosos para que aporten valor a la empresa deben ser tratados en función de los objetivos de la empresa y actualizados ya que en este periodo de cambios acelerados aquellos datos que no se actualicen y renueven pronto acabarán obsoletos.

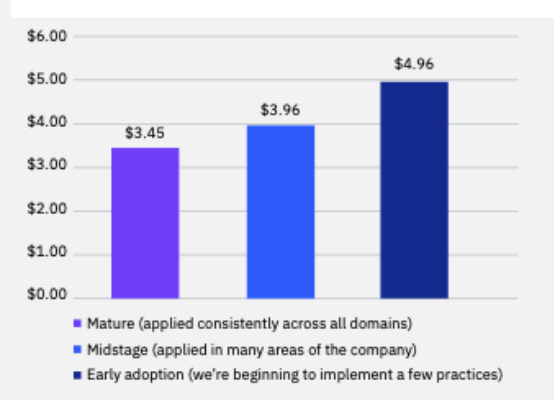
Otra acción que se plantea es la implementación de una estrategia "**Zero trust**". Como su propio nombre indica se trata de una estrategia en la que cada persona o dispositivo que trate de conectarse a la red de una organización es considerado como una amenaza, debiendo identificarse mediante diferentes factores para poder acceder a los sistemas. "Zero trust" se basa en tres principios básicos: verificar usuarios y dispositivos, usar el mínimo de privilegios y asumir la infiltración.

Dado que el sistema verifica usuarios y dispositivos es una buena opción que la empresa aporte a sus empleados los medios informáticos necesarios para realizar su misión dentro de la organización, de esta manera solo dispositivos reconocidos por la empresa como propios podrían conectarse al servidor haciendo el sistema más seguro y se evitaría traspasar al sistema de la empresa algún tipo de programa maligno que los dispositivos personales tuviesen previamente. Además, este sistema otorga de por sí los privilegios mínimos para realizar las funciones que son necesarias, por lo que, si se consigue entrar al sistema con el usuario de algún

empleado, el intruso no podrá tocar el sistema de la organización a su antojo, sino que estará limitado a las funciones autorizadas para ese usuario. Normalmente, en este tipo de estrategias los usuarios más completos son los administrativos.

El proceso también combina análisis, filtrado y registro para comprobar el comportamiento y para observar continuamente las señales de riesgo (Akamai, s.f.), por lo que los tiempos de detección de ataques se reducen ya que el sistema comprueba el comportamiento normal de los usuarios en la red, es decir, si hacen lo que normalmente hacen, si entran con el dispositivo con el que normalmente utilizan, si ingresan a la hora en la que normalmente lo hacen, etc. Esto reduce el riesgo de que se produzca un ataque y facilita el trabajo en cloud desde diferentes lugares, el cual se ha incrementado durante los últimos años de pandemia. De ahí viene el auge del sistema "Zero trust" ya que la empresa no puede controlar los dispositivos desde el departamento de las tecnologías de la información ya que puede que ya no se encuentren localizados dentro de la empresa.

Ilustración 7 Coste medio de un ataque según el nivel de "Zero trust" desarrollado



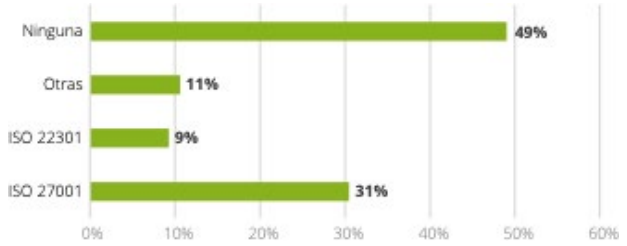
Medido en millones de dólares
Nota. International Business Machines Corporation. (Julio de 2022). *Cost of a data breach 2022*. Sitio Web de IBM: https://www.ibm.com/reports/data-breach

Como se puede observar en la ilustración 7, el uso de una estrategia "Zero trust" supone para aquellas empresas que tienen este proceso completamente establecido un ahorro medio de 1.51 millones de dólares frente a aquellas empresas que todavía están en proceso de implementación. Lo cual hace evidente por qué las empresas están optando por implementar cada vez más este sistema, además de la facilidad que

aporta al trabajo desde entornos cloud, que como ya se ha mencionado cada vez suponen una forma más frecuente de trabajo debido al COVID 19 y a la descentralización de diferentes procesos y servicios, que obligan a trabajar con diferentes equipos en diferentes partes del mundo siendo la opción cloud la única posible.

Cabe destacar la importancia de implementar en la empresa un plan de **calidad** enfocado a la ciberseguridad que fuerce a la mejora continua y a tomar acciones correctivas y preventivas enfocadas a esta área. La calidad establece un estándar mínimo que la empresa debe cumplir, lo que fuerza a realizar auditoría interna con el fin de comprobar periódicamente que todas las actividades relacionadas con la ciberseguridad se realizan de acuerdo con las acciones planificadas, dando de esta manera confianza a los grupos de interés de la empresa que ven como esta está enfocada en un proceso de mejora continua en torno a la ciberseguridad. En este caso, el plan de calidad se centraría en el proceso ya que debe estar enfocado a que las medidas de ciberseguridad y la forma de hacer las cosas en torno a ella cumplan con esos estándares mínimos que desde el plan de calidad se establecen. De esta manera, se deberá establecer un manual de calidad en el que se recoja además del sistema de gestión de la calidad elegido por la empresa aquellas medidas de ciberseguridad implantadas y a través de las cuales se consigue el estándar de calidad para que cualquier miembro de la organización conozca que acciones debe llevar a cabo para cumplir con dicho estándar establecido.

Ilustración 8 Porcentaje de empresas que poseen un certificado de calidad en ciberseguridad



Nota. Deloitte. (2022). *El estado de la ciberseguridad en España* . Sitio web de Deloitte: https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html

Como se puede observar en la ilustración 8, el 49% de las empresas todavía no disponen de ningún tipo de certificación en calidad, lo que supone desperdiciar la oportunidad de creación de valor y mejora continua que un plan en calidad puede aportar a la empresa, mejora continua, que ahora cobra una gran relevancia. Además, se observa como la ISO27001 es la certificación de calidad más elegidas por las empresas en esta materia.

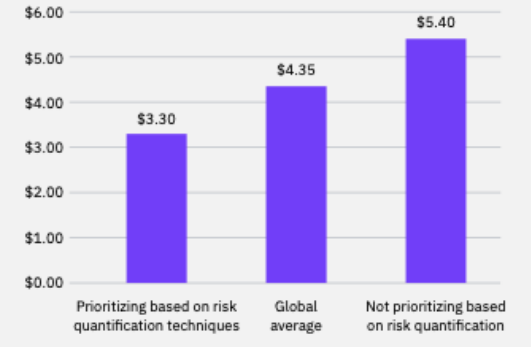
Adicionalmente, se ha identificado que existe una correlación muy clara entre el hecho de disponer de certificaciones de ciberseguridad y el sufrir menos incidentes, ya que estas certificaciones ayudan a robustecer las medidas de seguridad y a aumentar el nivel de madurez de ciberseguridad de las compañías; aunque no son ninguna garantía ante ciberataques (Deloitte, 2022). El 69% de los ciber incidentes son sufridos por aquellas empresas que no disponen de ninguna certificación en materia de ciberseguridad (Deloitte, 2022).

La norma ISO 27001 está dedicada a Sistemas de Gestión de la Seguridad de la información. Esta norma recoge todos los requisitos necesarios con los que una organización debe contar para poder garantizar que realiza una gestión adecuada de la información, asegurando su confidencialidad, integridad y disponibilidad (Sustant, s.f.). Un sistema de Gestión de la información consiste en un conjunto de medidas y requisitos orientados a asegurar la protección de la

información dentro de una organización frente a cualquier amenaza, como pueden ser ataques cibernéticos, malas prácticas de los propios empleados, intrusos o catástrofes naturales; a través de la aplicación de controles y el establecimiento de procedimientos de seguridad (Sustant, s.f.). Esto permite a la empresa prevenir un ataque y sus consecuencias, establecer un proceso de mejora continua en el que se establezca el plan a seguir por la empresa y con el cual se aporta valor, así como el aumento de confianza por los grupos de interés de la empresa como ya se ha mencionado anteriormente.

Otra medida que se propone es la utilización de un sistema de **cuantificación de riesgos**. Esto permitirá priorizar los riesgos en función de las perdidas potenciales que puedan provocar a la organización y la probabilidad de ocurrencia, así como dirigir los esfuerzos y recursos a aquellos riesgos que pueden tener un mayor impacto. Si, por ejemplo, el phishing es el que mayor impacto puede generar en la organización, da una idea clara hacía donde se deben dirigir los esfuerzos y recursos, para luego dirigirlo a otros riesgos que tengan menor probabilidad de ocurrencia y, por tanto, menos prioritarios. Además, crea una base sobre la que la empresa se puede ayudar a la hora de comunicar y justificar la posición adoptada en cuanto a los ciberriesgos ante los diferentes grupos de interés de la empresa. El 81% de las empresas dicen que les ayuda a incrementar la productividad y centrarse en asuntos estratégicos (PWC, 2021).

Ilustración 9 Impacto de técnicas de cuantificación de riesgos en el coste medio de un ataque



Medido en millones de dólares

Nota. International Business Machines Corporation. (Julio de 2022). *Cost of a data breach 2022*. Sitio Web de IBM: https://www.ibm.com/reports/data-breach

Como se observa en la ilustración 9, priorizar los riesgos en función de técnicas como la cuantificación de riesgos (risk quantification) produce un ahorro medio de 2.10 millones de dólares frente a aquellas empresas que no utilizan este tipo de técnicas.

Pero no debemos pensar que la utilización de este tipo de técnicas se resume a los costes ahorrados sino por la gran utilidad que pueden aportar al equipo de dirección de la empresa para la gestión de la ciberseguridad y la defensa de dicha gestión hacía los grupos de interés, ya que aporta una idea clara de hacía donde debe focalizar sus esfuerzos, dando una justificación estadística en base a la probabilidad de ocurrencia de algún ciberriesgo. Ayuda a priorizar recursos, los cuales no son ilimitados.

Como la empresa se encuentra inmersa en un entorno en el que encontramos diferentes organizaciones inmersas en un entorno similar, otra acción que se puede llevar a cabo es el **Benchmarking**, este es un proceso por el que se va a tomar como referencia los procedimientos en materia de ciberseguridad, en este caso concreto, del resto de organizaciones para compararlos con los de la propia empresa y posteriormente realizar mejoras e implementarlas. Es importante resaltar que no vale copiar, sino que se tiene que mejorar, la empresa que opte por la utilización de esta técnica debe mejorar aquello que quiere incorporar, por tanto, es complementario al proceso de mejora continua (calidad) ya que fuerza a la

comparación periódica con aquellas empresas que lo están haciendo “bien” con la intención de observar que están haciendo ellos que la empresa no o que están haciendo diferente, analizarlo, mejorarlo, introducirlo y controlarlo. Se propone la utilización de un benchmarking funcional ya que se comparará con aquellas empresas que sean excelentes en el área de ciberseguridad independientemente que la organización pertenezca al mismo sector o sea competidora o no. En definitiva, nos ayuda a pensar sobre lo que se está haciendo en la empresa y como se está haciendo, así en como la manera en la que se puede mejorar.

La última acción propuesta es la contratación de un **seguro ciber**, una cobertura cada vez más conocida por las empresas, el 64% de las empresas tienen actualmente coberturas ciber, con un seguro ciber específico o como parte de otra póliza, frente al 58% de hace dos años (HISCOX, 2022). La contratación de un seguro ciber es interesante ya que ayuda a reducir las consecuencias de un ciberataque, dando cierto grado de seguridad a la empresa, ya que, aunque cuente con un plan de ciberseguridad ante cualquier incidente que se pueda producir tendría un respaldo que mitigaría las consecuencias y a la vez le ayudaría a solventar el problema. Además, ayuda a adquirir experiencia en la gestión de crisis y ciberseguridad ya que la mayoría de las coberturas ofrecen asesoramiento en esta materia y apoyo en el momento de un ataque.

Las compañías que ofrecen este tipo de coberturas ofrecer, entre otras, lo siguiente:

- Restauración del sistema.
- Ante el robo de datos, investigan el origen y el alcance para no repetir en el futuro.

- Ante un robo de los datos de las cuentas bancarias, devuelven la cantidad que han robado.
- Cobertura de los gastos de crisis.
- Abono de sanciones, como las impuestas por la RGPD.
- Responsabilidad civil subsidiaria.

Alguna compañía ofrece de manera opcional dos opciones bastante interesantes:

- Indemnización diaria en caso de paralización de la actividad.
- Servicio de suministro de equipos de sustitución.

Por tanto, ayuda a la empresa a "cubrirse las espaldas" en caso de que algo falle y consigan involucrarse en sus sistemas. De hecho, los ciberseguros guardan una estrecha relación con los ciber incidentes sufridos: a mayor número de ciber incidentes, mayor es la contratación de estos seguros por parte de las empresas (Deloitte, 2022).

6. Implantación

Para que el plan elaborado tenga efecto en la organización debe ser implantado, y tan importante es este proceso como la elaboración de dicho plan, pues ante una estrategia bien elaborada una pobre implantación puede llevar a la empresa a un problema y que dicha estrategia fracase (Bonoma, 1984). Por lo que para asegurar el existo de la estrategia elaborada se debe realizar una correcta implantación.

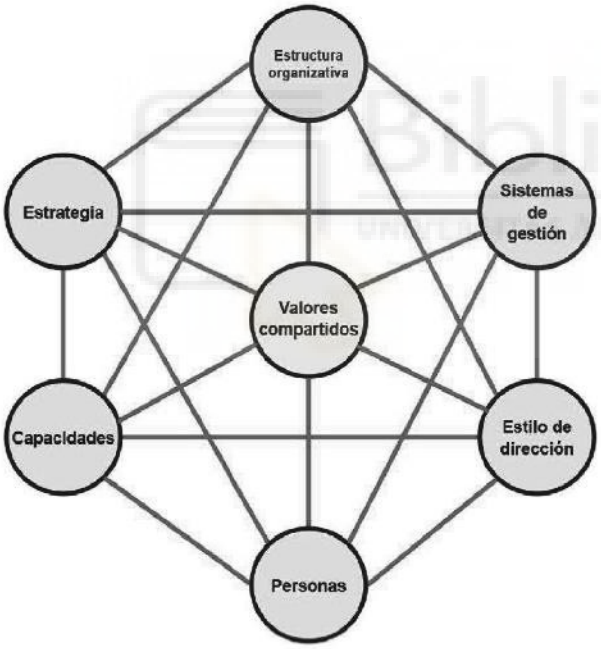
Antes de la implantación del plan anteriormente desarrollado se debe comprobar como su implantación va a afectar al resto de componentes de la

organización y actuar en consecuencia para que todos ellos estén alineados y si no lo están incorporar modificaciones que ayuden a su alineación y, por tanto, a su implementación. Para ello se propone utilizar el **modelo de las 7S de McKinsey**.

El modelo de las 7S es desarrollado en el libro “En busca de la excelencia” por McKinsey & Company en 1980, se trata de un modelo en el cual se relacionan 7 factores básicos de una organización.

Como podemos apreciar en la ilustración 10, estos 7 factores con los que el modelo recibe nombre son: Estructura organizativa, estrategia, sistemas de gestión, capacidades, estilo de dirección, personas y valores compartidos (recibe el nombre de las 7S por su traducción en inglés). Además, podemos apreciar como cada uno de estos factores está relacionado con el resto, de manera que si se realiza una modificación en alguno de ellos tendrá efectos en todos los demás. Mediante este modelo se aprecia que la estrategia no se encuentra aislada en las organizaciones, sino que se relaciona con el resto factores, y si queremos que la implantación de esta estrategia tenga éxito, deberemos tener en cuenta como se

Ilustración 10 Modelo 7S de McKinsey



Nota. Guerras Martín, L. A., & Navas López, J. E. (2022). *La dirección estratégica de la empresa. Teoría y aplicaciones* (Vol. 6). ARANZADI.

está relacionando la estrategia con los demás factores pues para que la implantación se lleve a cabo con existo, todos estos aspectos deben estar alineados.

Se plantea realizar el modelo de las 7S con la situación en la que queremos que la empresa se encuentre al implantar la estrategia de ciberseguridad y se realizará dicho modelo durante el proceso para comprobar que se asemeja al modelo “ideal” en el cual querremos estar en algún momento. De esta forma, podremos tener en cuenta las desviaciones que se están produciendo con respecto a la situación ideal, permitiendo realizar modificaciones y correcciones a tiempo para rectificarlas. Así, el modelo no solo nos servirá para asegurarnos que la estrategia planteada en ciberseguridad se alinea con el resto de los factores de la organización facilitando el éxito de dicha estrategia, sino que también nos permitirá llevar un control sobre la implantación de esta.

A continuación, se presenta un ejemplo del modelo de las 7S para la implantación del plan de ciberseguridad anteriormente descrito:

1. Estrategia (Strategy)

   Introducir la ciberseguridad en la empresa como una medida necesaria y que aporta valor, mediante el plan de ciberseguridad diseñado anteriormente.

2. Estructura (Structure)

   Se crea un nuevo equipo de trabajo dedicado a la ciberseguridad que se encarga de dar apoyo al resto de la organización y del mantenimiento de los diferentes sistemas, así como de la actualización y renovación de los procedimientos para

adaptar a la empresa a los acelerados cambios producidos en esta área. Introducción del puesto de *Chief Information Security Officer (CISO)* encargado de la adecuada gestión y protección de la información ante ciberataques, del cual dependerá el equipo anteriormente mencionado. Dicho CISO acudirá a los diferentes comités de la empresa, incluyendo el comité de dirección. La participación del CISO en el Comité de Dirección ha aumentado en un 12% respecto al año anterior, lo que refleja un mayor nivel de involucración con la Alta Dirección (Deloitte, 2022).

3. Sistemas (Systems)

   Los sistemas están descritos en el plan de ciberseguridad anteriormente desarrollado y que se encontraran especificados en el manual de calidad de ciberseguridad de la empresa.

   Se implementará el uso de la inteligencia artificial para potenciar el sistema de ciberseguridad y se establecerá un buzón electrónico a través del cual se podrán esclarecer dudas y hacer sugerencias por parte del personal de la organización. También se realizará un seguimiento de los sistemas y procesos por parte del equipo encargado de la ciberseguridad y se auditará a través de la subcontratación de una empresa externa especializada en esta materia.

4. Valores compartidos (Shared values)

   Dentro de los objetivos, la misión y la visión de la empresa se incorporará la ciberseguridad, implantándola como una necesidad para la empresa y forma de progreso que deberá ser comunicada e incentivada de tal manera por el equipo

directivo y los diferentes líderes formales e informales dentro de la organización. La ciberseguridad como parte esencial de la organización.

5. Habilidades (Skills)

   Se establecen planes de formación periódicos para aportar las habilidades necesarias a todo el personal.

6. Estilo (Style)

   Se apostará por un liderazgo transformacional en el que se acute como modelo a seguir, motivando e impulsando a todo el personal de la empresa. Creando un clima comunicativo y de trabajo en equipo que fomente la implicación del personal en el proceso de implantación de la ciberseguridad, la colaboración y el cambio organizativo hacía interiorizar el nuevo valor organizacional.

7. Personal(Staff)

   Se establece un plan de compensación por logro de objetivos en torno a la ciberseguridad y se establece formaciones para satisfacer sus necesidades.

Una vez comprobadas las relaciones que se establecen entre los diferentes factores básicos de la organización y planteadas aquellas medidas que serán necesarias llevar a cabo para fomentar la implantación de dicho plan se procederá a comenzar con el proceso de implantación propiamente dicho. Para ello se seguirá el **modelo desarrollado por John Kotter** en su libro “Liderando el cambio” publicado en 1995, en el cual estableció las siguientes 8 fases:

1. Crear sentido de urgencia
2. Formar una coalición
3. Crear una hoja de ruta
4. Comunicar de forma efectiva
5. Eliminar los obstáculos
6. Asegurar triunfos a corto plazo
7. Construir sobre el cambio
8. Anclar el cambio a la empresa

Para la implantación de la estrategia de ciberseguridad se seguirán estos 8 pasos dentro de los cuales se prestará especial atención a dos variables fundamentales en la introducción de un cambio organizacional: el liderazgo y la comunicación.

Crear sentido de urgencia y formar una coalición

Es necesario presentar la ciberseguridad en la organización como una medida necesaria ya que el 48% de las empresas informaron de un ciberataque en los últimos 12 meses (citar HISCOX) así como de las consecuencias que puede conllevar enfrentarse a un incidente de este tipo. Se debe presentar como una medida necesaria que aporta valor a la organización y no como un mero capricho organizacional que tan solo sirve para añadir nuevos procedimientos. Es necesario que el personal de la empresa entienda que la situación a la que se enfrentan las

empresas en la actualidad demanda un protocolo de ciberseguridad ante el cual tanto la información propia de la empresa y de los propios empleados como la privacidad de los clientes esté protegida en todo momento y se gestione de la manera más responsable y rentable posible.

Para hacer llegar este mensaje a toda la organización se requiere de formar una coalición identificando a los líderes que se comprometan con el proceso y ayuden a su implantación.

En primer lugar, el equipo directivo como líder formal dentro de la organización tiene que comprometerse con la nueva estrategia, si no están comprometidos y actúan dando ejemplo es muy complicado que los subordinados se comprometan con el proceso de implantación y, por tanto, que termine fracasando. Además, la implantación de una nueva estrategia requiere destinar recursos limitados por lo que el apoyo de la alta dirección es fundamental.

Por otro lado, se identificarán los líderes informales para que apoyen este proceso de cambio y fomenten la nueva estrategia destacando su necesidad y utilidad.

Cuando nos encontramos ante un proceso de cambio organizacional el estilo de liderazgo que rige en la organización es una variable fundamental que puede terminar determinando el éxito o fracaso de dicho proceso de cambio. Por tanto, se apostará por el liderazgo transformacional definido por James McGregor Burns en 1978 en su libro “Leadership”. Este tipo de liderazgo trata de fomentar la motivación y el compromiso de los empleados con la visión y misión de la organización, consiguiendo que las entiendan como suyas. Los trabajadores no harán lo que

hacen por una recompensa si no que lo harán porque entienden que es necesario y el porqué de hacerlo.

Para llevar a cabo este estilo de liderazgo en la organización los líderes deben ser un modelo a seguir, si una de las medidas adoptadas por el plan de ciberseguridad es la utilización de dispositivos propios de la empresa y la no utilización de fuentes ajenas a esta, el líder NO puede usar ningún dispositivo que no sea propio de le empresa ya que de esta manera muestra su compromiso con la estrategia, actúa como ejemplo a seguir y desprende confianza en dicho plan al resto de la organización. Se debe fomentar la comunicación, la participación de los empleados en los planes establecidos y la aportación de "feedback" que puede ayudar a una mejor implantación, una mejora del plan y que los trabajadores sientan dicho plan como propio lo que sin duda ayuda a su establecimiento dentro de la organización. En definitiva, se debe desarrollar una cultura innovadora dentro de la organización que no solo facilitará la implementación del plan desarrollado si no su futura modificación ya que la ciberseguridad está sujeta a numerosos cambios en el tiempo, muchos de los cuales podrán y deberán ser propuestos por los propios empleados a través de los canales establecidos.

Comunicar de forma efectiva, crear una hoja de ruta y construir sobre el camino

Uno de los inconvenientes principales encontrados en un proceso de implantación o cambio organizacional es la incertidumbre que se puede generar en la organización al no saber qué es lo que va a pasar. Para poder solventar esta

situación nos centraremos en otra de las variables fundamentales propuestas para este cambio: la comunicación.

La comunicación planteada en la implantación del plan de ciberseguridad es bidireccional:

- De la dirección al resto de la organización (descendente) de manera que la estrategia en ciberseguridad planteada sea comunicada y conocida por toda la organización.
- De los empleados a la dirección o líderes (ascendente) de manera que se desarrolle un clima en el que los trabajadores se sientan capacitados para proponer mejoras en el plan e incluso nuevas adicciones que lo complementen. Así como la resolución de cualquier duda que pueda sugerir entre ellos.

La comunicación ascendente fomenta el sentimiento de participación de los trabajadores en la estrategia lo que ayuda a que sientan dicha estrategia como propia lo que incentiva el compromiso con dicho plan y su éxito. Los objetivos pasan a ser percibidos como propios, ya no son solo objetivos organizacionales. Para ello se establece un canal de comunicación online a través del cual se planteará el "feedback" de la estrategia planteada. Cuando una sugerencia sea seleccionada para formar parte de la estrategia el trabajador que la planteó podrá formar parte de su desarrollo y será recompensado en consecuencia.

Para la comunicación descendente, desde la alta dirección al resto del personal, se plantea la utilización del mapa estratégico.

El mapa estratégico facilita la comunicación de la estrategia elaborada por la empresa y contenida en el cuadro de mando al resto de la organización. Además de facilitar la comunicación de la estrategia al resto de la organización permite comunicar las relaciones de causa y efecto entre las diferentes medidas, así como su nivel de cumplimiento.

Antes de plantear el mapa estratégico se plantea la creación del cuadro de mando ya que el mapa estratégico parte de este. A continuación, se muestra el cuadro de mando desarrollado en base al plan de ciberseguridad diseñado.

Perspectiva	Objetivo	Metas	Indicador
Financiera	Reducción de posibles costes y aumento de ventas	Aumento 2% cifra de ventas	Estados financieros
Clientes	Aumentar confianza y satisfacción y mejorar la identificación con la empresa	Aumento satisfacción cliente a 7 puntos en una escala de 0 a 10 puntos	Estudios de mercado

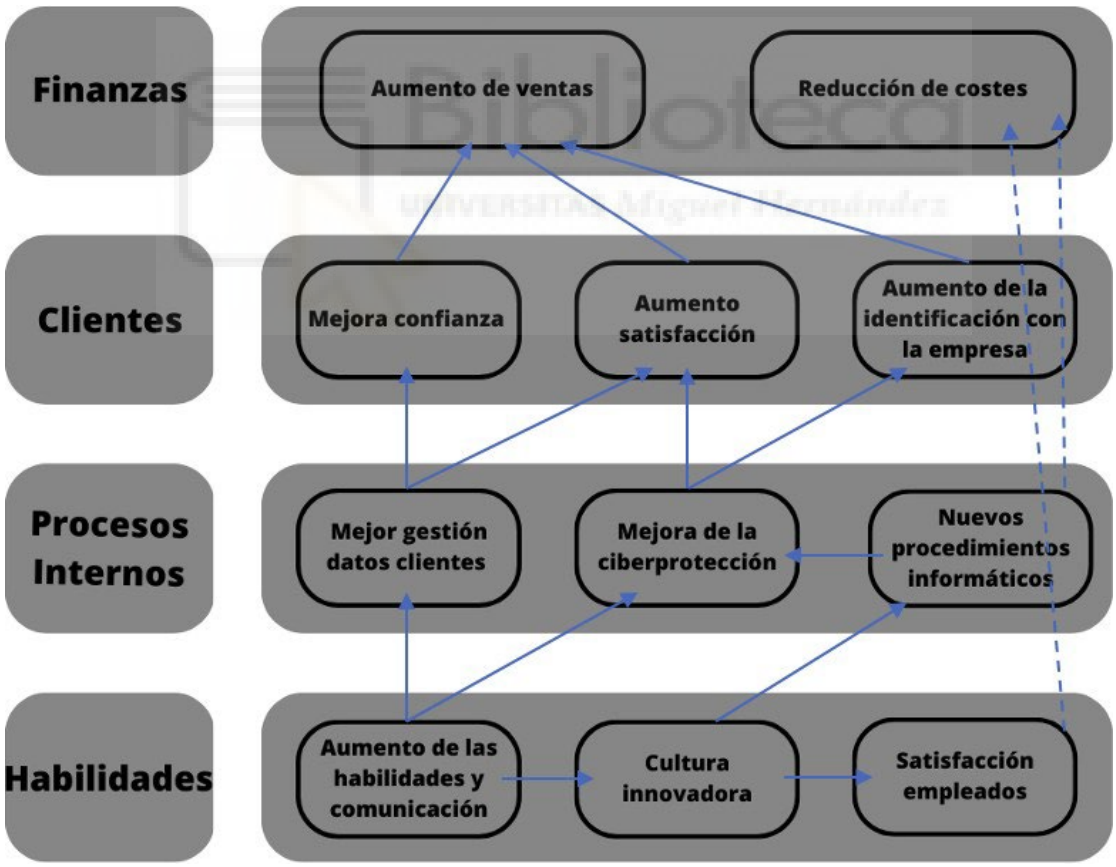
Procesos internos	Mejorar la gestión de los datos de los clientes, aumentar la ciber protección de la empresa e implementar nuevos procedimientos informáticos	Reducir los ciber incidentes en un 5%	Número de ciber incidentes sufridos y auditoría interna
Aprendizaje y crecimiento	Aumentar habilidades, fomentar comunicación, implementar cultura innovadora y aumentar la satisfacción de los empleados	Alcanzar 30 horas de formación y 40 horas de actividades en grupo	Número de formaciones completadas y análisis interno de cultura y clima
	*Todas las metas se establecen en el periodo de 1 año		

A través del cuadro de mando se puede observar como la implementación de la estrategia de introducción de la ciberseguridad en la empresa no solo se resume a los procesos internos a llevar a cabo y desarrollados en el plan de ciber seguridad, sino que también tiene diferentes propósitos en otros ámbitos de la organización. Como toda estrategia implementada debe tener un retorno económico en la organización que se hace visible a través de los beneficios generados a los clientes y trabajadores de la organización.

Los procesos internos desarrollados en el plan de ciberseguridad serán comunicados a toda la organización a través del manual de calidad elaborado, en el cual se resumirán estos procesos y la manera de llevarlos a cabo. Este manual estará disponible para todo el personal en todo momento de manera online en la intranet de la organización.

La estrategia planteada a llevar a cabo y desarrollada en el cuadro de mando se comunicará a través del mapa estratégico, desarrollado a continuación:

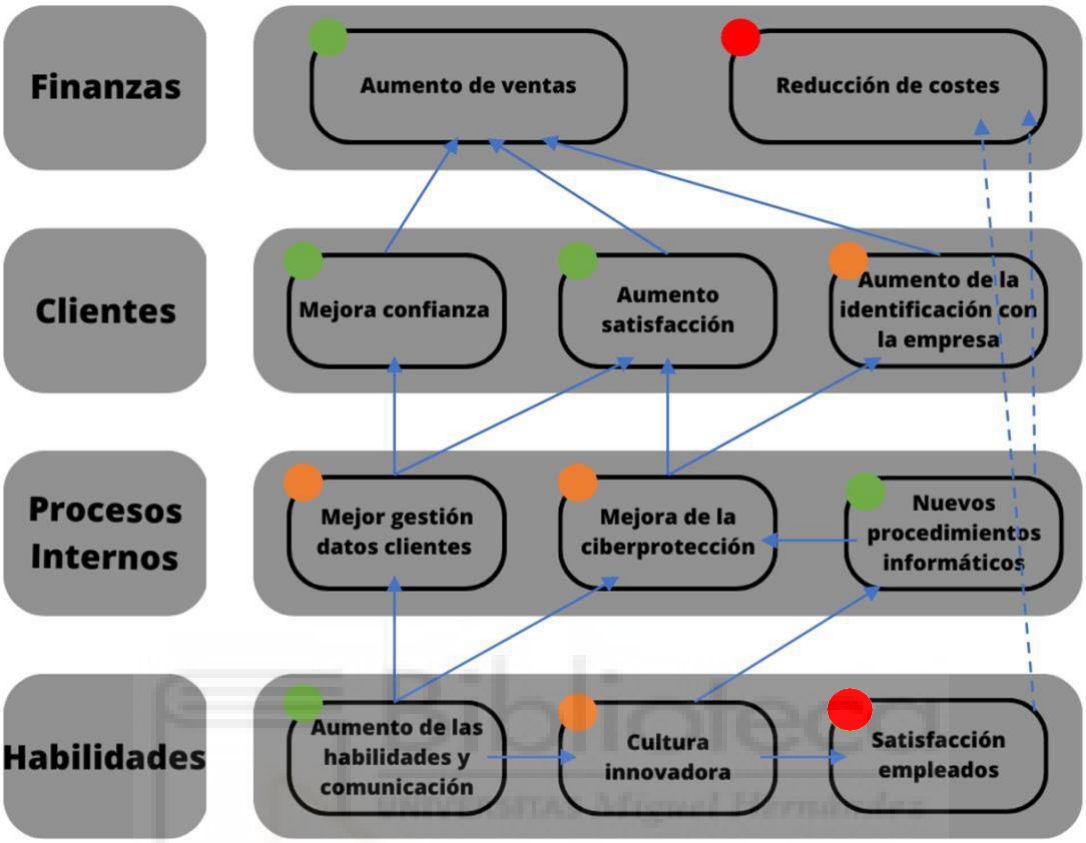
Ilustración 11 Mapa estratégico



Nota. Elaboración propia 2023

En el mapa estratégico se pueden observar los objetivos a conseguir planteados en el cuadro estratégico y como se relacionan estos objetivos, es decir, que objetivos intervienen en otros. Por ejemplo, el aumento de las habilidades y de la comunicación de los empleados influye en la cultura innovadora y a su vez en la satisfacción de los empleados. Dicho aumento en las habilidades permite conseguir a la organización la mejora en la gestión de los datos de los clientes y en ciber protección, lo que se traduce en una mayor satisfacción y confianza por parte de los clientes y en una mejora en la identificación de estos con la empresa. Esto se terminaría traduciendo en un aumento de las ventas por parte de la empresa y, por tanto, en un retorno de la estrategia implementada pues en caso contrario no tendría sentido su implantación. A su vez, el aumento en la satisfacción de los empleados se traduce directamente en una reducción de costes dada su implicación con el proceso lo que hace del trabajo más eficiente y reduce por consiguiente el número de ciberataques y sus consecuencias. De esta manera, se comunica a la organización los objetivos a conseguir y a través de qué objetivos se pueden conseguir el resto de ellos, pero esto no se queda solo aquí, ya que a través del mapa estratégico también se puede comunicar como de alcanzados están los objetivos. Esto se puede apreciar a continuación:

Ilustración 12 Mapa estratégico 2



Nota. Elaboración propia 2023

De esta forma se puede mostrar el progreso a través de los colores verde, naranja y rojo. Entendiendo verde como conseguido, naranja como parcialmente conseguido y rojo como no conseguido (los colores utilizados en el gráfico anterior son a modo orientativo). Además, conseguimos crear una hoja de ruta a seguir manteniendo aquellas medidas que están haciendo cumplir los objetivos en verde y prestando especial atención a aquellas en rojo y naranja para conseguir alcanzar el objetivo previsto en el periodo de tiempo previsto, y en caso de ser necesario, realizar alguna modificación.

Asegurar triunfos a corto plazo

El mapa estratégico anteriormente planteado muestra la evolución en la implantación de la estrategia a largo plazo ya que la ciberseguridad en la empresa es un proceso que también se plantea a largo plazo, pero para que la implantación tenga existo y se consiga motivar al personal se deben establecer objetivos a corto plazo que ayuden a incentivar el sentimiento de que se está avanzando en el proceso.

Se plantean los siguientes ejemplos:

- Cumplimiento por parte del personal de las medidas de ciberseguridad trimestralmente.
    - En el primer trimestre deberán ser cumplidas por el 25% del personal.
    - En el segundo trimestre por el 50%.
    - En el tercer trimestre por el 75%.
    - En el cuarto trimestre por el 100%.
- Mantener mensualmente el número de incidentes por debajo 5%.
- Mantener la satisfacción cliente por encima de 7 puntos en una escala de 0 a 10 puntos.

Como estos se pueden plantear varios objetivos a corto plazo que ayuden a mantener motivado al personal y creen un camino que si se cumple lleve a la organización al cumplimiento de los objetivos estratégicos planteados en el cuadro de mando y el mapa estratégico.

Eliminar los obstáculos

Al implementar una nueva estrategia dentro de una organización pueden surgir conflictos de interés entre los diferentes grupos de interés. Por ejemplo, la propiedad de la empresa puede estar centrada en la creación de valor a largo plazo, pero la dirección está centrada en la rentabilidad a corto plazo, dando lugar a un conflicto de interés entre ambos. La misma situación puede darse entre trabajadores, proveedores, clientes, etc.

En primer lugar, para conseguir eliminar estos obstáculos volveremos a recurrir a la función del líder y la comunicación. Es necesario que el líder consiga influir en la organización para que el conjunto entienda la estrategia como propia y necesaria, por lo que es fundamental una buena comunicación como ya se ha mencionado anteriormente. Fundamental fomentar una cultura innovadora, por parte del líder, en la que el cambio se vea como una oportunidad y no como un obstáculo.

Además, se debe replantear cuales son los intereses que tienen los diferentes grupos de interés para comprobar si se pueden modificar algunos aspectos con los cuales todas las partes salgan beneficiadas, con ello incluso puede que el plan en su conjunto salga reforzado y mejorado.

Por último, se debe considerar la opción de si interesa mantener la relación comercial con aquellos grupos que se mantengan opuesto al plan si la empresa quiere seguir adelante con dicho plan. Por ejemplo, si en el plan de ciberseguridad se incluyen ciertos requisitos a los proveedores para trabajar con la empresa, pero

estos se niegan a implementar dichas medidas, una opción es considerar buscar otro proveedor que sí implemente dichas medidas y, por tanto, se alinee con la estrategia, objetivos y la misión y la visión, siempre que sea posible.

En resumen, es necesario comprobar si dichos conflictos pueden ser resueltos introduciendo modificaciones al plan desarrollado que pueden incluso complementarlo y mejorarlo. En caso contrario, se debe replantear el mantenimiento de la relación comercial.

Anclar el cambio a la empresa

En el modelo de Congelamiento del filósofo estadounidense Kurt Lewin se establecen 3 fases para el cambio organizacional: descongelamiento, cambio y congelamiento.

En este punto el descongelamiento ya se ha producido pues se ha detectado la necesidad de implementar un plan de ciber seguridad en la empresa, se ha desarrollado dicho plan y se ha introducido en la organización la necesidad de cambio. El cambio se ha producido durante el proceso de implantación recientemente desarrollado, el cual tendrá lugar con objetivo al largo plazo.

Por último, debemos congelar de nuevo la situación con las nuevas prácticas introducidas en la organización. En este último punto de nuevo se destaca la importancia del líder en todo el proceso. Para anclar el cambio introducido en la organización el líder debe actuar de ejemplo indefinidamente, motivando al equipo a continuar con las prácticas introducidas en el tiempo para conseguir que las

medidas implementadas no se pierdan, fomentando la cooperación. Además, se debe tratar de asentar la cultura innovadora y de calidad en torno a la ciberseguridad que asentarán las medidas establecidas y facilitarán el cambio futuro.

Para fomentar a los trabajadores a mantener dichas medidas se cuenta en el plan desarrollado con objetivos a corto plazo y una retribución variable unida a la ciberseguridad y comentada en páginas anteriores que ayudarán al líder al mantenimiento de las medidas en el tiempo hasta que se interpreten como propias y queden interiorizadas en la organización en la nueva cultura.

El objetivo de este proceso es que no se pierda el nuevo comportamiento.

7. Comunicación

Una de las partes fundamentales de la implantación de una estrategia es la comunicación de esta como ya se ha mencionado, pero no solo la comunicación a los trabajadores de la organización, sino que también a sus clientes.

La confianza y satisfacción de los clientes no solo se consigue gracias al reducido o nulo número de ciberataques ocurridos desde la implantación de la estrategia. La comunicación de esta por parte de la empresa también ayuda e incluso facilita la identificación de los clientes con la empresa que, mediante el reducido número de ataques seria complicado. La empresa debe comunicar su posición ante los datos que recolecta sobre sus clientes y de qué manera los protege para asegurar que nadie fuera de la empresa pueda acceder a ellos o que incluso no todo el mundo dentro de la organización pueda acceder a ellos, en algunos casos

de empresas de equipos informáticos ni siquiera la propia empresa puede acceder a esos datos a no ser que el usuario de su consentimiento.

Empresas como Apple, Amazon, Google y Coca-Cola tienen un apartado en sus páginas web acerca de la política de privacidad de la empresa, sirviéndoles de oportunidad para compartir la posición y cultura de la empresa acerca de la utilización de los datos de sus clientes lo que ayuda a estos a sentirse o no identificados con la empresa. De esta manera, si los clientes se sienten identificados con la política y estrategia adoptada por la empresa aumenta, por consiguiente, las compras realizadas a esta en vez de a su competencia.

No solo es importante la comunicación de la estrategia a seguir, sino que también es fundamental la comunicación que se realiza a los clientes cuando un ciberataque tiene lugar y sus datos han sido comprometidos, así como a los grupos de interés. De hecho, una mala gestión de la comunicación de crisis suele ser el detonante de una crisis reputacional (Mañas-Viniegra y otros, 2019), que sin duda tendría el efecto contrario al perseguido por la empresa ya que si se encuentra envuelta en una crisis reputacional difícilmente se conseguirá aumentar el sentimiento de pertenencia con la empresa.

Es posible que una correcta comunicación y gestión de la crisis en una filtración de datos o de ciberataque a la empresa contrarreste en cierta medida los efectos negativos del propio ataque.

No solo puede ser perjudicial la no comunicación y ocultación de una crisis hacía los clientes, sino que también hacía otros grupos de interés de la empresa

como los accionistas de esta. En la actualidad las noticias vuelan aun cuando la organización ha decidido ocultar la situación, en este momento la incertidumbre que se genera puede provocar que algunos accionistas decidan retirar su inversión por el hecho de no conocer cuál es la verdadera situación de la empresa. En este sentido será fundamental la comunicación de la crisis, es decir, que ha sucedido y como se está trabajando para solucionarlo.

Se plantea realizar este tipo de comunicaciones a través de la página web de la organización y mediante comunicado en los diferentes medios de comunicación disponibles en el momento.

En resumidas cuentas, igual de importante es la comunicación que se realiza a cualquier grupo de interés. Aquellas organizaciones o personas que mantienen una relación comercial con la organización deben estar informadas del sentido que toma, así como de sus valores y objetivos y, cuando algo fuera de lo planeado ocurre también deben ser informados para que la incertidumbre no se adueñe de la situación y la empresa pueda mantener su reputación y posicionamiento.

8. Medidas de control

Una vez creado el plan de ciberseguridad a establecer y elaborado el proceso de implantación a seguir cabe centrarse en aquellas medidas que colaborarán a controlar tanto que al plan es funcional y eficiente, como que la implantación se está haciendo correctamente. Así, se detectarán las desviaciones ocurridas durante el proceso de implantación elaborando las medidas necesarias para continuar por el

camino elegido por la compañía y permitirá conocer si la estrategia elaborada es adecuada o si es necesaria también alguna modificación.

Como ya se ha mencionado reiteradamente en este documento, nos encontramos ante un momento en el que las tecnologías de la información, la ciberseguridad y los datos están sometidos a numerosos cambios continuamente. Debido a esto, requerimos de establecer un plan flexible que sea capaz de adaptarse ágilmente a los cambios producidos en su entorno. Por ello, se ha construido el plan de ciberseguridad, la estrategia y su implementación en torno a medidas de control que faciliten este proceso, dando especial relevancia a la importancia del líder que fomente no solo una cultura en torno a la ciberseguridad de la empresa, sino que también una cultura innovadora que facilite su adaptación a los numerosos cambios ocurrentes en las organizaciones, especialmente en ciber seguridad.

Las **medidas de control** implementadas para asegurar que el **plan de ciberseguridad** es útil y eficiente se han desarrollado en el apartado del plan, por lo que se repasarán brevemente. Estas medidas son el plan de calidad y las pruebas periódicas, también contará como medida de control el número de incidentes ocurridos, entendiendo que cuantos menos incidentes mejor es el plan, independientemente de su eficiencia.

El plan de calidad al establecer las medidas mínimas que la empresa debe respetar en torno a la ciberseguridad obliga a esta a realizar auditoría interna periódicamente para asegurar que dichas medidas se están cumpliendo. Además,

la calidad obliga a la empresa a la mejora continua por lo que también debe revisar como se encuentra su entorno para adaptarse a él, y si cabe área de mejora en el plan de ciberseguridad elaborado y de esta manera mejorar su eficiencia y utilidad.

De la misma forma, las pruebas periódicas ayudan a la organización a comprobar si lo implementado funciona y si es eficiente. También fuerzan a la compañía a comprobar si existe la posibilidad de mejorar el proceso y si los empleados conocen tanto su función como los procesos necesarios a llevar a cabo en una situación de crisis real, ya que si el encargado de realizar una tarea no la realiza puede ser tan crítico como si la empresa no tuviese ninguna medida de ciberseguridad implementada.

De la misma manera, las medidas destinadas al **control de la implantación** han sido incorporadas en el diseño del propio proceso para garantizar su correcto funcionamiento. Estas medidas son las 7S de McKinsey, el cuadro de mando y el mapa estratégico.

Aunque las 7S de McKinsey se plantean en un primer momento para garantizar la alineación de la estrategia con diferentes factores básicos de una organización, es un modelo que también puede ser utilizado para controlar el proceso de implantación ya que se puede realizar periódicamente para comprobar si la situación de la empresa se asemeja a la planteada.

Para controlar toda la estrategia de implementación de ciber seguridad se utilizará el cuadro de mando anteriormente planteado y, para ello, se debe completar

con aquellas medidas que permitirán comprobar el grado de cumplimento de los objetivos y metas planteados en el mismo. A continuación, se plantea el nuevo cuadro de mando con las medidas para el control de la estrategia incorporadas.

Perspectiva	Objetivo	Metas	Indicador	Medidas para el control	Medidas para el control
Financiera	Reducción de posibles costes y aumento de ventas	Aumento 2% cifra de ventas	Estados financieros	Cifra de ventas de la empresa y el importe neto de la cifra de negocio	Reducción de costes - ante un ciber ataque cuanto son los costes netos totales en comparación con otros ciber ataques ocurridos con anterioridad
Clientes	Aumentar confianza y satisfacción y mejorar la identificación con la empresa	Aumento satisfacción cliente a 7 puntos en una escala de 0 a 10 puntos	Estudios de mercado	A través de los datos recopilados de los clientes de la empresa realizar CAWI	Indicadores como el Net Promoter Score (NPS) y Costumer Satisfaction Score (CSAT)
Procesos internos	Mejorar la gestión de los datos de los clientes, aumentar la ciberprotección de la empresa e implementar nuevos procedimientos informaticos	Reducir los ciberincidentes en un 5%	Número de ciberincidentes sufridos y auditoria interna	Plan de calidad, pruebas periodicas y número de ciber incidentes	Revisión por los mandos de las prácticas de los empleados y contratación de empresa externa que revise que los procesos
Aprendizaje y crecimiento	Aumentar habilidades, fomentar comunicación, implementar cultura innovadora y aumentar la satisfacción de los empleados	Alcanzar 30 horas de formación y 40 horas de actividades en grupo	Número de formaciones completadas y análisis interno de cultura y clima	Medición del clima y la cultura a través de encuestas internas y dinámicas de grupos	Revisión del número de formaciones realizadas y aprobadas
	*Todas las metas se establecen en el periodo de 1 año				

Estas medidas de control recogidas en el cuadro de mando deberán ser realizadas periódicamente para garantizar el correcto desarrollo de la estrategia, pudiendo prestar especial atención e introduciendo modificaciones en aquella perspectiva que se esté desviando. Por ejemplo, si uno de los objetivos de la introducción de la estrategia de ciber seguridad es el aumento de la confianza y satisfacción de los clientes mediante la mejora de la gestión de sus datos y la

protección de estos, un indicador como el CSAT debería aumentar, indicando la correcta implantación de la estrategia.

9. Presupuesto

Como toda estrategia a implementar en las organizaciones requiere de recursos para ser implantada y garantizar su funcionamiento. Estos recursos pueden variar en función de las organizaciones pues no dispone de los mismos recursos una pyme que una internacional, por ello se hablará del porcentaje del presupuesto de la empresa a destinar en esta materia.

Según el informe del estado de la ciberseguridad en España de 2022 de la empresa Deloitte el presupuesto destinado a la ciber seguridad representa un 9,4% del presupuesto destinado a las tecnologías de la información. Aunque esto va a tender a aumentar con el tiempo debido principalmente a la escasez de talento ya comentada anteriormente y el previsible aumento de demanda que la ciberseguridad experimentará en años próximos debido al aumento de las amenazas, las nuevas formas de ataque cada vez mejor diseñadas y la necesidad de proteger los activos digitales como son los datos, la reputación y posicionamiento.

Ilustración 13 Presupuesto ciberseguridad frente a TI

Nota. Deloitte. (2022). *El estado de la ciberseguridad en España* . Sitio web de Deloitte: https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html

Además, cabe destacar, que, a mayor inversión en ciberseguridad, menor número de ciber incidentes: mientras que las empresas que destinan menos de 5 millones de euros en ciberseguridad reciben como mínimo 2,17 ciber incidentes, las empresas que más dinero destinan (30 millones de euros) consiguen reducir ese número a 1, 5 (Deloitte, 2022).

Por ello, y aunque en la actualidad en la mayoría de las empresas los recursos destinados rondan el 9,4% del presupuesto en tecnologías de la información, es necesario destinar recursos suficientes a esta materia ya que además de evitar que se produzcan ciber incidentes y sus consecuentes efectos, es una medida que aporta valor a la organización.

12. Conclusión

La ciberseguridad es un tema pendiente para un gran número de organizaciones, pero debido al creciente número de ciberataques y las numerosas consecuencias de estos, está obligando a muchas de ellas a implantar una estrategia en ciberseguridad.

Dicha estrategia no debe centrarse simplemente en las aplicaciones informáticas que revisan los sistemas para detectar si pueden estar siendo atacados, sino que precisa de introducir ciertas modificaciones en el comportamiento, introducir nuevos sistemas y equipos, tanto humanos como informáticos, y ciertas medidas que ayuden a tener una correcta cultura en torno a la ciberseguridad. Por ello, la empresa deberá reestructurarse internamente para garantizar la implantación de

dicha estrategia, asegurándose que la ciberseguridad se alinea con el resto de la organización como medida para el éxito.

El desarrollo de un plan de ciberseguridad y de un plan de calidad en torno a esta, es fundamental para que por un lado el conjunto de la organización conozca aquellas medidas que son necesarias implantar en su comportamiento diario que ayuden al propósito de la nueva estrategia y por otro, la implantación de un plan de mejora continua obliga a la organización a mantener un ojo en el entorno tecnológico para adaptarse ágilmente a los cambios o anticiparse a ellos y a encontrar aquellas nuevas medidas que ayuden a protegerse mejor, gestionar los datos mejor o hacer ambas de una forma más eficiente en la que sean necesarios menos recursos y, por tanto, mejoren la rentabilidad de la organización.

No solo basta con el desarrollo de dicho plan, sino que es necesario que toda la organización se involucre en su implantación como garantía para su existo. Para ello, el papel de los líderes de la organización es fundamental pues deben conseguir que dichos cambios no solo parezcan necesarios y urgentes, sino que los objetivos de la organización sean percibidos como propios aumentando el sentimiento de pertenencia a la organización. La utilización de sistemas de incentivos será tan importante como necesaria, por lo menos al principio, para interiorizar las nuevas acciones en el comportamiento ya establecido.

Papel del líder será también el fomento de una cultura innovadora y en la que la ciberseguridad forma parte de los valores de la organización. Con el desarrollo de la cultura innovadora no solo se facilitará la implantación del plan, sino que también

se agilizarán las adaptaciones que en el futuro se deberán producir pues si de algo la organización puede estar segura es que el entorno tecnológico va a cambiar rápidamente en el tiempo.

Otra medida fundamental es la comunicación que se haga tanto de la estrategia como de un ataque si en su caso se produce. En ambos casos, el enemigo principal es la incertidumbre que el no saber genera y, por tanto, la organización es responsable de mantener informados a los grupos de interés tanto de la situación en la que se encuentra la organización como de los planes pensados para la nueva estrategia. Saber que se va a hacer, porque se va a hacer, cuáles son los objetivos, en qué estado se encuentra la organización y cuál es el plan para resolver el problema/ataque son cuestiones fundamentales para mantener el apoyo de los grupos de interés y su confianza. Así como para evitar cualquier crisis reputacional que podría acabar con la vida de esta.

La construcción de todo este proceso estratégico es fundamental que se desarrolle con base a medidas de control, sobre todo con una materia sometida a numerosos y acelerados cambios. Saber que está pasando y adaptarse con la mayor brevedad posible es una fuente de ventaja competitiva frente a los competidores. Se debe detectar las desviaciones en torno al plan establecido para actuar en consecuencia y de esta manera acercarse a los objetivos estratégicos a la vez que se avanza con pasos firmes y seguros. También ayuda a observar los resultados que se están obteniendo con la estrategia, haciendo firme su utilidad y

aumentando el sentimiento de que se está consiguiendo lo propuesto, motivando de esta manera al personal.

Como toda estrategia necesita de una serie de recursos limitados en las organizaciones y que deberán ser retirados de otras partes de la organización por lo que el apoyo de la alta dirección es fundamental para su éxito. Se prevé que estos recursos necesarios aumenten con el tiempo debido a la escasez de talento y al aumento y sofisticación de los ataques por lo que el desarrollo de talento interno también puede generar una notable fuente de ventaja.

Con todo ello, debe entenderse la estrategia de ciberseguridad como una medida que aporta valor a la organización a largo plazo y que generará un retorno de la inversión realizada gracias al aumento de fidelidad de los clientes.

Bibliografía

ADP. (12 de 04 de 2019). *¿Cómo hacer un mapa estratégico y para qué sirve?* Sitio web de ADP: https://www.apd.es/como-hacer-un-mapa-estrategico/

Akamai. (s.f.). *Modelo de seguridad Zero Trust*. Sitio web de Akamai: https://www.akamai.com/es/our-thinking/zero-trust/zero-trust-security-model

Allianz. (s.f). *Seguro para ciber protección*. Sitio web Allianz: https://www.allianz.es/seguros/especialidades/seguros-ciberataques.html

Amazon Web Services. (s.f.). *¿Qué es la ciberseguridad?* Sitio web de Amazon Web Services: https://aws.amazon.com/es/what-is/cybersecurity/

AXA. (s.f). *Ciber Protección*. Sitio web AXA: https://www.axa.es/seguros-empresas/ciber-proteccion

Berrocal, A. (22 de Agosto de 2022). *¿Pueden ser los datos su activo más valioso?* El economista: https://www.eleconomista.com.mx/empresas/Pueden-ser-los-datos-su-activo-mas-valioso-20220822-0046.html

Bonoma, T. V. (1984). Making your marketing strategy work. *Harvard Business Review, 62*(2), 69-76.

CE consulting. (8 de 11 de 2022). *Todo lo que debes saber sobre retribución variable*. Sitio web CE consulting : https://ceconsulting.es/blog-ceconsulting/retribucion-variable/

CISCO. (s.f). *¿Cuáles son los ciberataques más comunes?* Sitio web CISCO: https://www.cisco.com/c/es_mx/products/security/common-cyberattacks.html

Dávalos, R. M. (2015). La influencia del factor humano, el liderazgo y la cultura de las organizaciones en los procesos de implementación y gestión del cambio organizacional. *Revista Internacional de Investigación en Ciencias Sociales, 11*(1), 102-114.

Deloitte. (2022). *El estado de la ciberseguridad en España* . Sitio web de Deloitte: https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html

Domínguez-Franco Abogados. (20 de Junio de 2022). *Retribución variable: conoce los tipos y sus ventajas*. Dominguez & Franco : https://www.dominguezfrancoabogados.es/blog/retribucion-variable

Ghiglione, F. A. (2021). El cuadro de mando integral como herramienta de eficiencia en la gestión empresarial. *Ciencias administrativas*(18), 87-93.

Grupo atu. (10 de 2022). *¿Qué es el cyber risk o ciberriesgo?* Sitio web de Grupo atu: https://www.grupoatu.com/que-es-el-ciberriesgo/

Guerras Martín, L. A., & Navas López, J. E. (2022). *La dirección estratégica de la empresa. Teoría y aplicaciones* (Vol. 6). ARANZADI.

Hill, M. (18 de Enero de 2023). *Las autoridades europeas de protección de datos imponen multas récord de 2.920 millones por el GDPR*. cso computerworld: https://cso.computerworld.es/tendencias/las-autoridades-europeas-de-proteccion-de-datos-imponen-multas-record-de-2920-millones-por-el-gdpr

HISCOX. (05 de 2022). *Informe de Ciberpreaparación de Hiscox 2022.* Sitio web de Hiscox: https://www.hiscox.es/informe-de-ciberpreparacion-de-hiscox-2022

HISCOX. (24 de Noviembre de 2022). *Una de cada tres pymes pierde clientes como resultado de un ciberataque*. Sitio web de Hiscox: https://www.hiscox.es/una-de-cada-tres-pymes-pierde-clientes-como-resultado-de-un-ciberataque

HISCOX. (s.f). *Ciberseguro*. Sitio web de Hiscox: https://www.hiscox.es/seguros/ciberseguridad

Iberdrola. (s.f). *Gestión del cambio*. Sitio web de Iberdrola: https://www.iberdrola.com/talento/que-es-gestion-del-cambio

Iberdrola. (s.f). *Liderazgo transformacional* . Sitio web de Iberdrola: https://www.iberdrola.com/talento/liderazgo-transformacional#:~:text=Su%20creador%2C%20el%20historiador%20norteamericano,transformación%20dentro%20de%20una%20organización.

Ingenio empresa. (s.f). *Las 7-S DE MCKINSEY*. Ingenioempresa.com: https://www.ingenioempresa.com/7s-de-mckinsey/

International Business Machines Corporation. (Julio de 2022). *Cost of a data breach 2022*. Sitio web de IBM: https://www.ibm.com/reports/data-breach

International Business Machines Corporation. (s.f). *¿Qué es la ciberseguridad?* Sitio web de IBM: https://www.ibm.com/es-es/topics/cybersecurity

International Business Machines Corporation. (s.f). *¿Qué es la industria 4.0?* Sitio web IBM: https://www.ibm.com/es-es/topics/industry-4-0

International Business Machines Corporation. (s.f.). *¿Qué es un ciberataque?* Sitio web de International Business Machines Corporation: https://www.ibm.com/es-es/topics/cyber-attack

Mañas-Viniegra, L., Niño González, J. I., & Martínez Martínez, L. (2019). La transparencia como variable reputacional de la comunicación de crisis en el contexto mediático del ciberataque WannaCry. *Revista de la SEECI*(48), 149-171.

Martín, J. (29 de Septiembre de 2016). *¿Un congelador para gestionar el cambio?* Sitio web CEREM: https://www.cerem.es/blog/un-congelador-para-gestionar-el-cambio

Mclean, M. (6 de MARZO de 2023). *2023 Must-know cyber attack statistics and trends*. Sitio web EMBROKER: https://www.embroker.com/blog/cyber-attack-statistics/

Microsoft. (s.f). *Embrace proactive security with Zero Trust*. Sitio web de Microsoft: https://www.microsoft.com/en-us/security/business/zero-trust

Microsoft. (s.f). *¿Qué es la ciberseguridad?* Sitio web Microsoft: https://support.microsoft.com/es-es/topic/-qué-es-la-ciberseguridad-8b6efd59-41ff-4743-87c8-0850a352a390

NETSKOPE. (s.f). *¿Qué es "confianza cero"?* Sitio web Netskope: https://www.netskope.com/es/security-defined/what-is-zero-trust

Olarte, J. P., & García, A. (2009). Factores clave de éxito para una implantación exitosa del Sistema de Gestión Estratégica "Balanced Scorecard". *Escuela de Administración de Negocios* (65), 49-75.

Pérez-Vallejo, L. M., Vilariño-Corella, C. M., & Ronda-Pupo, G. A. (2017). El cambio organizacional como herramienta para coadyuvar con la implmentación de la estrategia. *Ingeniería Industrial , 38*(3), 323-332.

PWC. (Junio de 2021). *Cyber-ready-today and for tomorrow.* Sitio web de PWC: https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/assets/pwc-us-dti-2021.pdf

Quarterly, M. (1 de Marzo de 2008). *Enduring Ideas: The 7-S Framework*. Sitio web de McKinsey & Company: https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/enduring-ideas-the-7-s-framework#

Roncancio, G. (s.f). *¿Qué es un mapa estratégico en el Balanced Scorecard y cómo se hace?* Sitio web de pensemos: https://gestion.pensemos.com/que-es-un-mapa-estrategico-en-el-balanced-scorecard-y-como-se-hace

Rubiano, M. G. (2011). Liderazgo transformacional y la facilitación de la aceptación al cambio organizacional. *Pensamiento Psicológico, 9*(16), 41-54.

Santander Universidades. (15 de 06 de 2022). *Liderazgo transformacional: cómo pasar de ser el jefe a un auténtico líder*. Sitio web de Santander: https://www.becas-santander.com/es/blog/liderazgo-transformacional.html

Simla. (27 de Septiembre de 2021). *¿Qué es el Cuadro de Mando Integral (CMI), para qué sirve y cómo crearlo paso a paso?* Sitio web de Simla: https://www.simla.com/blog/cuadro-de-mando-integral

Sordo, A. I. (02 de Junio de 2022). *Cuadro de mando integral o blanced scorecard: qué es, usos y ejemplos*. Sitio web de Hubspot: https://blog.hubspot.es/marketing/cuadro-mando-integral

Sustant. (s.f.). *ISO 27001: Beneficios para la empresa y requisitos*. Sitio web de sustant: https://sustant.es/iso-27001-requisitos-y-beneficios-para-las-organizaciones/

Zurich. (s.f). *Seguro de Ciberriesgo*. Sitio web de Zurich : https://www.zurichempresas.es/seguro/ciberriesgos/?utm_source=google&utm_medium=cpc&utm_campaign=tck_zuem_google_performance-max_total_prs&gclid=EAIaIQobChMI_OL256f1_QIVV49oCR0QBA9aEAAYAiAAEgJZBvD_BwE