Iª Encuesta sobre Gestión de Brechas de Seguridad

Un documento de

isms forum | INTERNATIONAL INFORMATION SECURITY COMMUNITY

dpi DATA PRIVACY INSTITUTE

COORDINADORES:
Susana Rey Baldomir
Javier Lomas Sampedro

ÍNDICE DE CONTENIDOS

1 Alcance y Objetivos de la Encuesta 4

2 Sobre la encuesta 6

3 Brechas de seguridad 8

4 Planifica 10

4.1 ¿Estamos preparados? 10

4.2 Trabajo en equipo 14

5 Gestiona 16

5.1 Detección y contención 16

5.2 Análisis de riesgos 17

5.3 Ciberseguros 17

6 Notifica 18

6.1 ¿Notificamos? 18

6.2 Transparencia 20

6.3 Resultado de la notificación 21

6.4 Resultado del proceso de gestión de la brecha 22

6.5 Impacto en el negocio 23

7 Conclusión final 25

Anexo. Encuesta - Guía Práctica para la Gestión y Notificación de Brechas de Seguridad 26

1 ALCANCE Y OBJETIVOS DE LA ENCUESTA

Cuando dentro de las actividades de la DPO Community de ISMS Forum se propuso realización de la Guía (práctica) para la gestión y notificación de brechas de seguridad, nuestro objetivo primordial era dar en ella respuesta a las principales inquietudes y dudas que los profesionales de la protección de datos tuviesen sobre esta.

Para poder establecer objetivamente cuales eran estas inquietudes, definimos una Encuesta con los siguientes objetivos principales, alineados con las fases de la Gestión de Brechas que la propia Guía ha identificado:

- **Planifica: ¿Cuán preparados nos creemos para afrontar nuestras brechas?**

  Conocer con qué tipos de grandes medidas se están preparando las empresas para responder, cuando llegue el momento, ante incidentes que supongan brechas de datos personales. Y, obviamente, la precepción sobre si las medidas en cada caso son suficientes y correctas.

- **Gestiona: ¿Cómo hemos gestionado las brechas reales y el grado de satisfacción con la planificación previa?**

  Necesitamos conocer cómo se detectan las brechas de datos personales y si se aplican adecuadamente los procesos y procedimientos definidos en la fase de planificación. Pero, sobre todo, saber para aquellas organizaciones que ya han sufrido una brecha, su percepción de si su capacitación era correcta o ha cambiado.

- **Notifica: ¿Por qué comunicamos tan pocas brechas en España?**

  Que en España se notifican muchas menos brechas de datos personales que en el resto de Europa es un hecho, constatado por la Agencia Española de Protección de Datos a través de sus informes anuales. Queríamos indagar en las causas y poder extraer conclusiones que nos ayuden a mejorar en este apartado en nuestro país.

- **Resuelve: ¿Cuál ha sido el impacto [positivo o negativo] de las fases previas?**

  Resolver una brecha de datos personales no solo es contener y eliminar el incidente que la ha provocado, aunque esto es parte fundamental obviamente de la resolución. Cuestiones menos técnicas y más relacionadas con las fases previas nos pueden dar una idea de cuan eficaz ha sido nuestro procedimiento de Gestión de Brechas y permitir mejorarlo.

La encuesta se ha lanzado intentando tener el mayor número posible de respuestas en todos los sectores de actividad, tamaño de la empresa, área territorial de trabajo, etc. Así como el de obtener información no solo de profesionales de la protección de datos, sino también de los que se dedican a la ciberseguridad.

Es obvio en estos momentos que la gestión de las brechas de datos personales, aunque sean una obligación legal establecida en la legislación sobre protección de datos, están íntimamente relacionadas y ligadas a la ciberseguridad. La gran mayoría de brechas que se producen diariamente en todo el mundo están relacionadas con incidentes de ciberseguridad, de la misma forma que la digitalización cada vez mayor de los procesos empresariales nos llevan a tenerlos relacionados directamente con sistemas informáticos. Es por ello por lo que nos pareció muy interesante contrastar el punto de vista de ambos tipos de profesionales ante eventos y sucesos iguales, y su capacidad de cooperar y entenderse en un entorno en el que están condenados a trabajar juntos.

Una vez realizada esta primera Encuesta hemos considerado interesante repetirla periódicamente dentro del Observatorio de la Privacidad de ISMS Forum, de forma que podamos conocer cómo evoluciona en el tiempo la Gestión de Brechas, a medida que todos los implicados vayamos ganando la madurez que el tiempo proporciona a todos los procesos. Con el objetivo para años futuros de mejorar la encuesta con las observaciones que sus participantes nos han hecho llegar, y, sobre todo, de conseguir llegar a la pequeña y mediana empresa.

2 SOBRE LA ENCUESTA

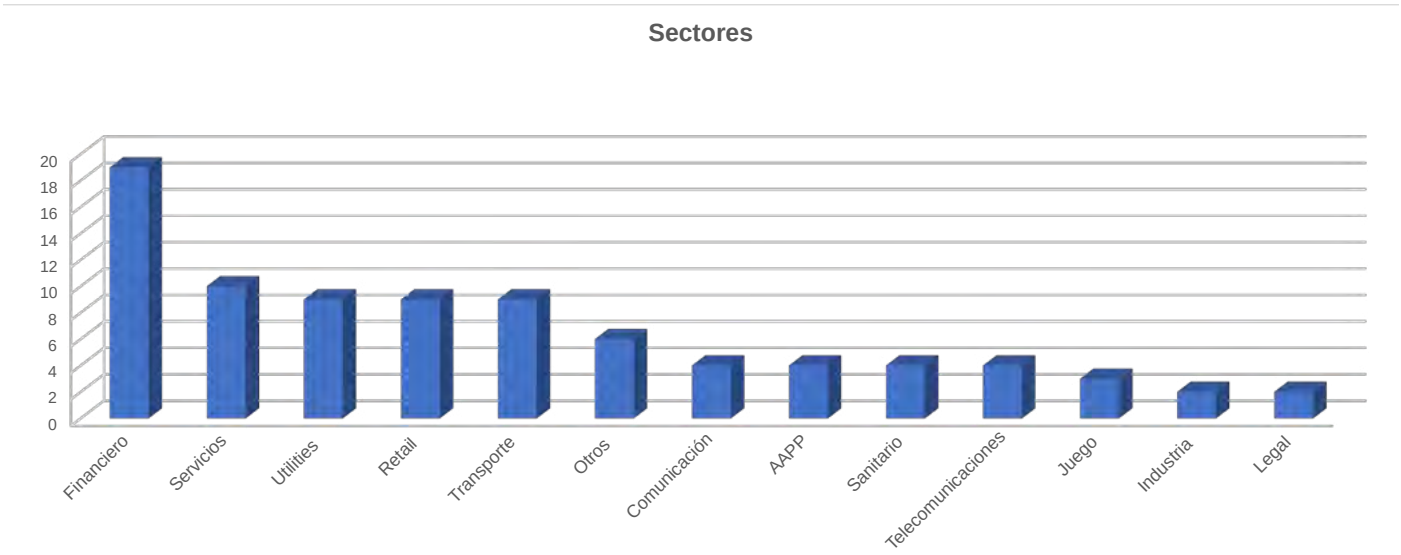
La encuesta ha constado de 32 preguntas repartidas entre los datos demográficos que hemos querido utilizar para comparar las conclusiones de los diferentes apartados, y las preguntas propiamente dichas.

Hemos obtenido 85 respuestas, de las que lo primero que hemos de decir es que hemos fracasado en nuestro objetivo de acceder también el estado de los procesos de gestión de brechas de datos personales en las pequeñas y medianas empresas, sector básico en la economía española, por el pequeño porcentaje de respuestas que nos han llegado de ellas: tan solo un 5%. Es por lo que hemos decidido no segmentar las conclusiones siguientes de la encuesta en base a este factor.

Ha de tenerse en mente que todas las conclusiones que hemos podido obtener de la encuesta se refieren a Empresas grandes, y, por lo tanto, a priori, con una capacidad de gestión y preparación mayor.

Para futuras ediciones de la encuesta uno de los principales puntos de mejora será el de llegar a la pequeña y mediana empresa.

Por otra parte, sí hemos obtenido un abanico bastante representativo de los diferentes sectores de actividad dentro de la Gran Empresa española:



Aunque hemos de decir, que de forma general, no se ha observado prácticamente diferencias en las respuestas obtenidas en función del sector de actividad, excepto en un caso que veremos más adelante.

También hemos contado con información sobre empresas que operan únicamente en España, otras que lo hacen a nivel europeo y empresas de carácter internacional; lo que nos ha permitido comparar la situación en España con otros países.

Constatando, como veremos más adelante, que sí existen diferencias reseñables en función del ámbito de actuación mercantil.

Y, por último, destacar también que hemos podido obtener información tanto de profesionales de la protección de datos, de la ciberseguridad, e incluso de aquellos que tienen ambos roles en sus compañías. Así como la visión de profesionales con cargos más directivos, frente a otros más técnicos.

Hemos de decir, que hemos concluido que sí hay divergencias importantes en algún caso, entre las respuestas de profesionales que tienen atribuciones en protección de datos frente a los que solo las tienen de ciberseguridad. Pero no hay divergencia alguna en función de si se tienen en exclusiva atribuciones de protección de datos o conjuntamente con las de ciberseguridad.

3 BRECHAS DE SEGURIDAD

El primer resultado que hemos de resaltar de la encuesta es quizás el más sorpresivo, ya que el 34% de los encuestados indican que no han sufrido ningún incidente en los dos últimos años. Lo que en un principio podría interpretarse positivamente como un grado muy elevado de seguridad en las empresas, lo que en realidad muestra es una situación mucho menos halagüeña.

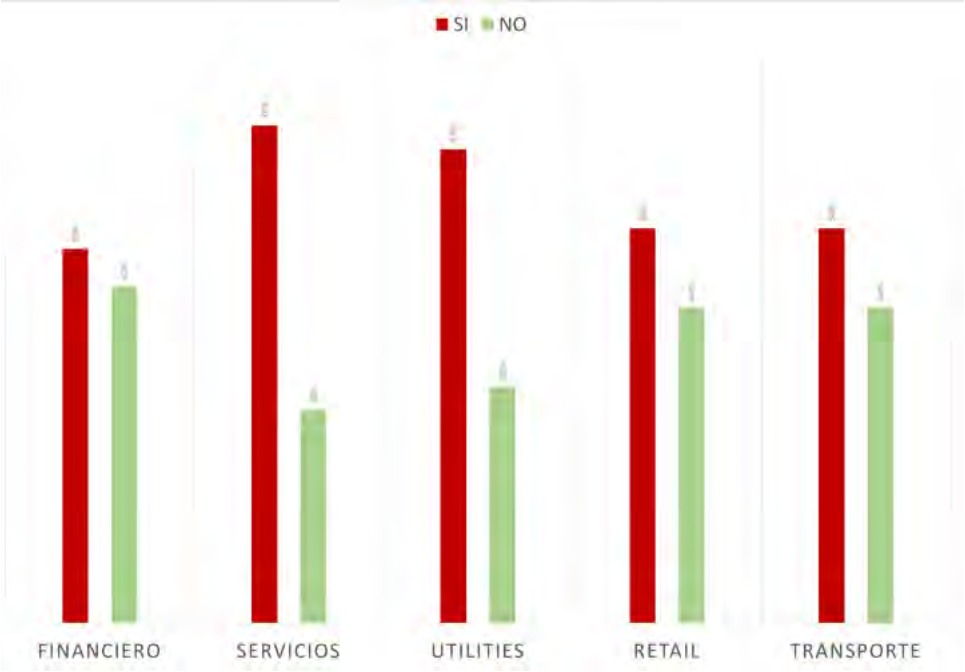
La realidad de la ciberseguridad nos enseña que, si dices que no has tenido incidentes en los últimos dos años, realmente es que no eres capaz de detectarlos.

Lo primero que se puede observar es que, curiosamente, son los profesionales que se dedican a la protección de datos, bien en exclusiva o en función conjunta con ciberseguridad, los que reportan un porcentaje muy superior de empresas con incidentes en los dos últimos años, frente a los profesionales de la ciberseguridad que se sitúan en un 45% de empresas sin brechas.

Esta disparidad muestra criterios diferentes entre Protección de Datos y Ciberseguridad a la hora de reportar incidentes, lo que puede llevarnos a situaciones en las que no se comuniquen al DPD, o no se haga a tiempo, con graves consecuencias para la organización: No hay peor brecha que la que no se gestiona. Con los datos actuales no podemos extraer conclusiones sobre la causa de esta disparidad tan importante: miedo a ser responsabilizados de incidentes por parte de las áreas técnicas, criterios demasiado estrictos en las áreas de protección de datos, falta de encaje en las organizaciones de la “nueva” figura del DPD, problemas de comunicación entre ambas funciones, etc. Pero está claro que es un punto de mejora dentro de las organizaciones construir un lenguaje, unos criterios comunes y un entorno de trabajo colaborativo fluido entre Protección de Datos y Ciberseguridad.

PLANIFICA: formación y concienciación, construyendo un lenguaje claro a lo largo de la organización y unos criterios comunes.

En cuanto a esta falta de incidentes para aquellos sectores con una muestra de respuestas suficiente para hacer el análisis, resulta especialmente curioso comprobar que para los sectores más regulados como el financiero el porcentaje de empresa sin incidentes se dispara hasta valores de casi el 50%, mientras que otros sectores con menor control suben hasta valores más acordes con las estadísticas internacionales, de hasta un 70% con incidentes.



Nos surge la duda sobre si la presión regulatoria y la exposición a la opinión pública de ciertos sectores no será precisamente un factor que limite el reconocimiento, y por lo tanto la gestión adecuada, de los incidentes.

También nos encontramos un dato clarificador al comparar las empresas que operan en exclusiva en España, frente a los que lo hacen el Europa. Mientras que en España las empresas sin incidentes en dos años se sitúan en el 33%, en Europa este valor baja al 20%. Y dado que las estadísticas internacionales sobre ataques y ciberincidentes sitúan a nuestro país entre los primeros de Europa, parece de nuevo que existe un problema de reconocimiento, y de gestión, por ende, en España que empieza a explicar el por qué se reportan menos brechas de datos personales a la autoridad de control.

PLANIFICA: En España aún no hemos alcanzado el grado de madurez de otros países europeos en la detección e identificación de brechas de datos personales.

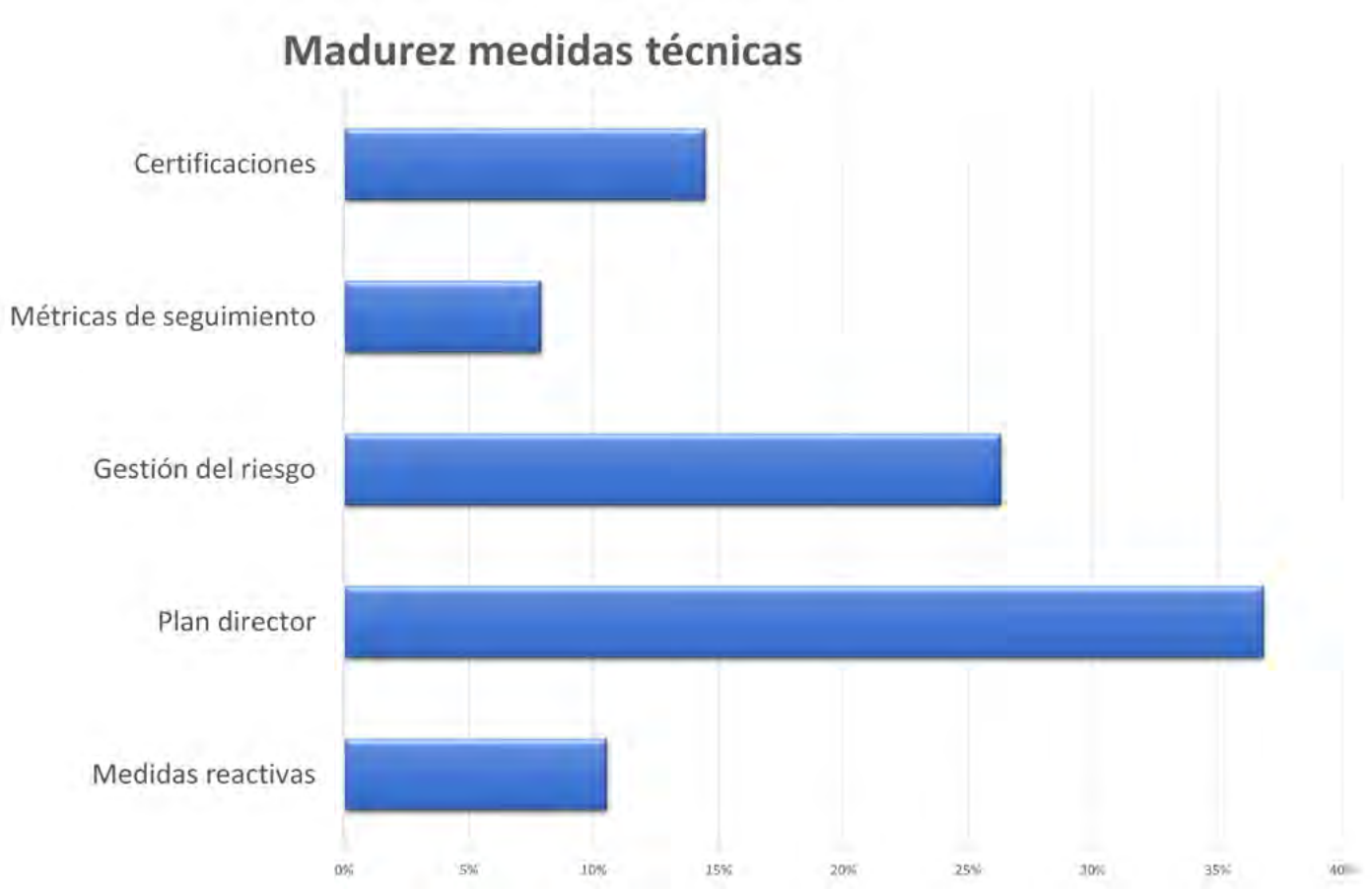
4 PLANIFICA

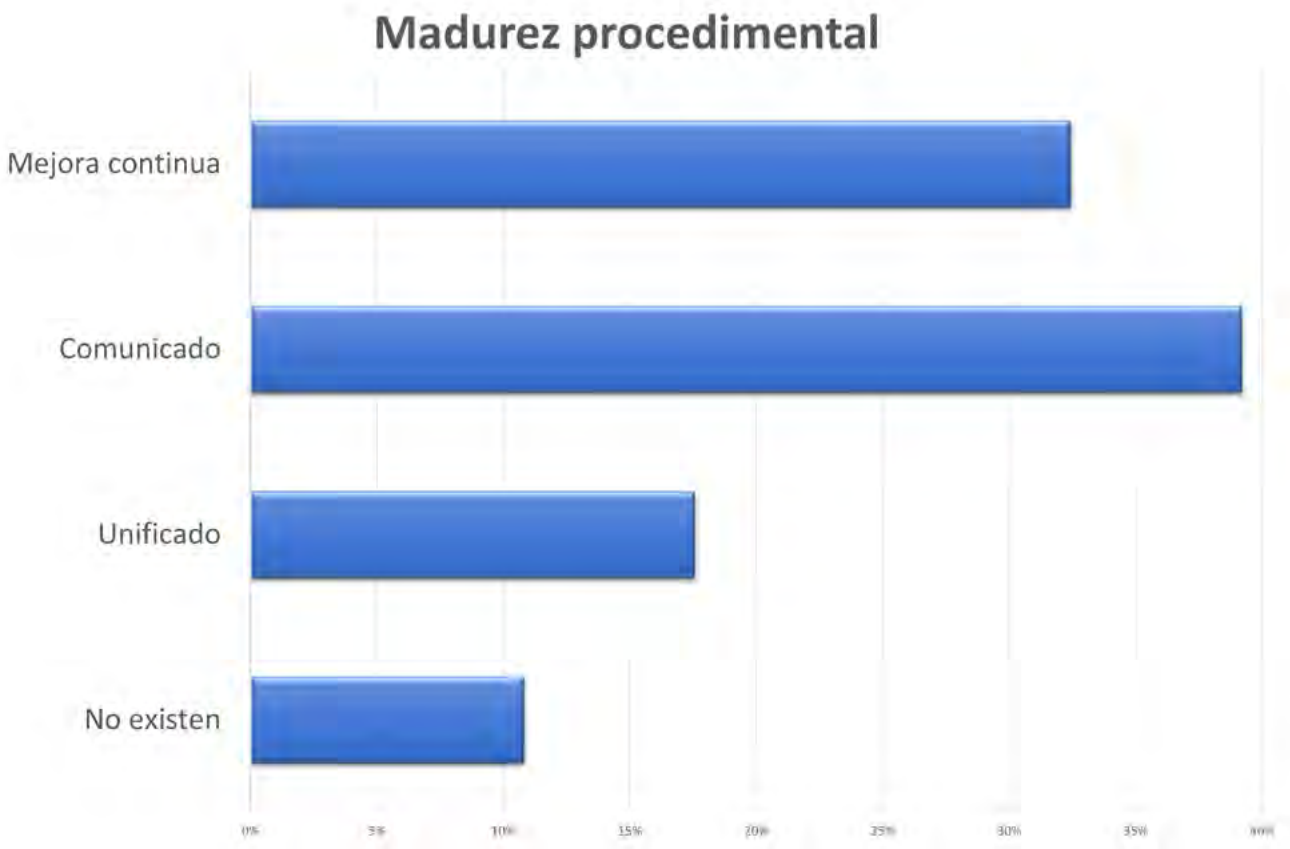
4.1. ¿Estamos preparados?

Aunque en general la percepción de las empresas es buena, se ha detectado un desalineamiento entre la percepción general de la madurez a nivel de procedimiento de gestión y a nivel de medidas técnicas.

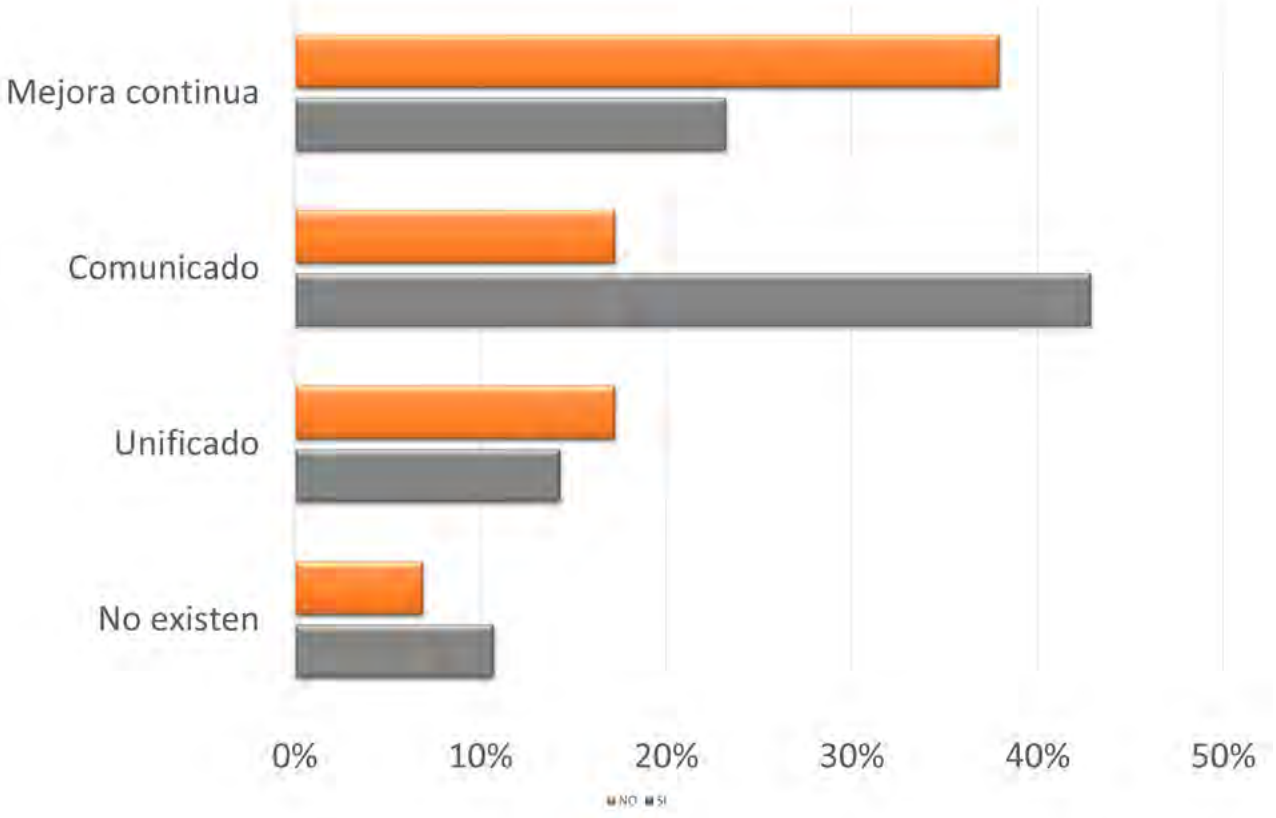
Parece que en general las empresas se perciben más preparadas en el área procedimental que en el de medidas técnicas, dónde los modelos de gestión más maduros, basados en la mejora continua, parecen no estar tan implantados como en los procedimientos de gestión.

El 30% de los encuestados tiene un proceso de gestión de brechas bien comunicado y que ha sido probado desde su definición. Un elevado grado de madurez atendiendo a que el concepto de brecha de datos personales es algo nuevo y como tal, en solo 3 años, parece difícil haber llegado a ese grado de madurez. Será interesante comprobar en futuras encuestas si estas respuestas obedecen realmente a pruebas proactivas o los encuestados que han sufrido brechas consideran que utilizar el procedimiento en una brecha real es una prueba reactiva.





Si comparamos la madurez procedimental en la gestión de brechas, vemos que aquellas empresas que ya han sufrido incidentes se ven con procedimientos generales menos maduros, y se decantan porque la comunicación de estos ha sido insuficiente. Lo contrario de lo que sucede con las que no han tenido la experiencia

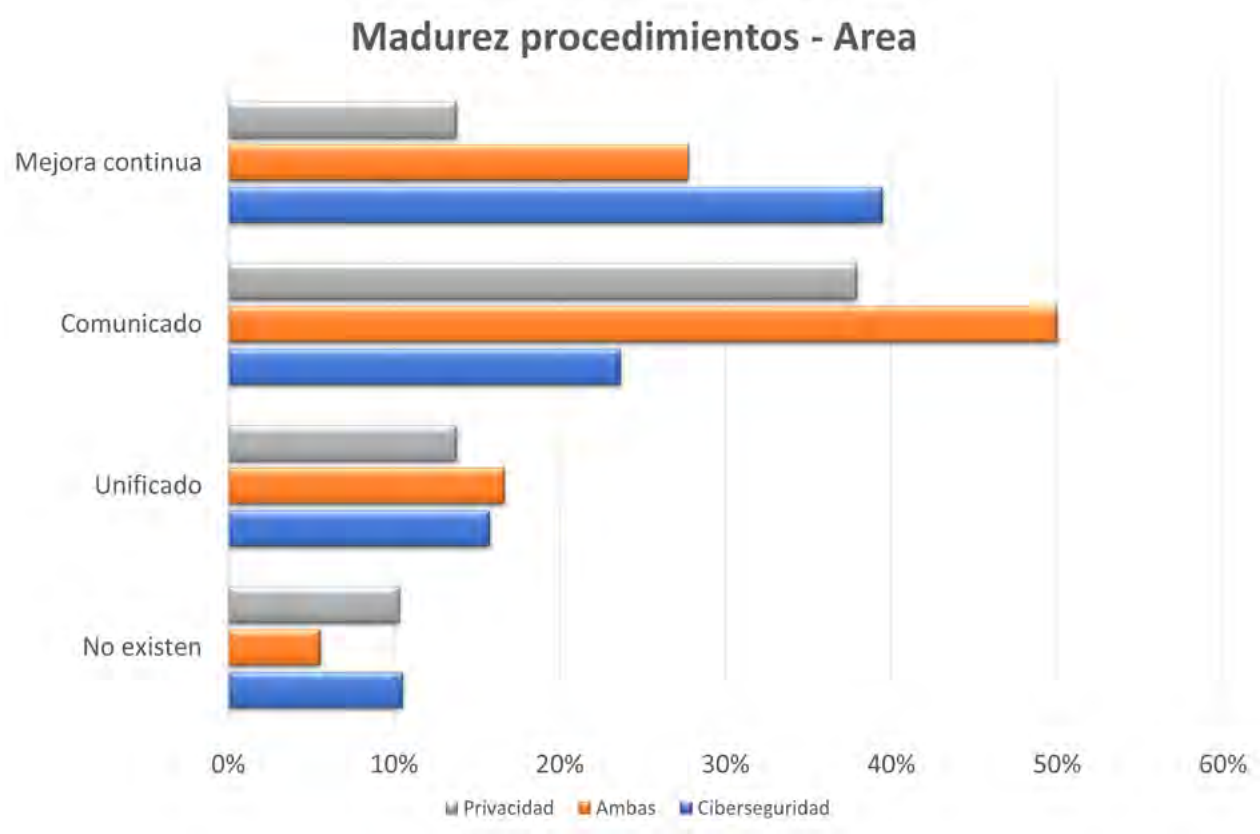


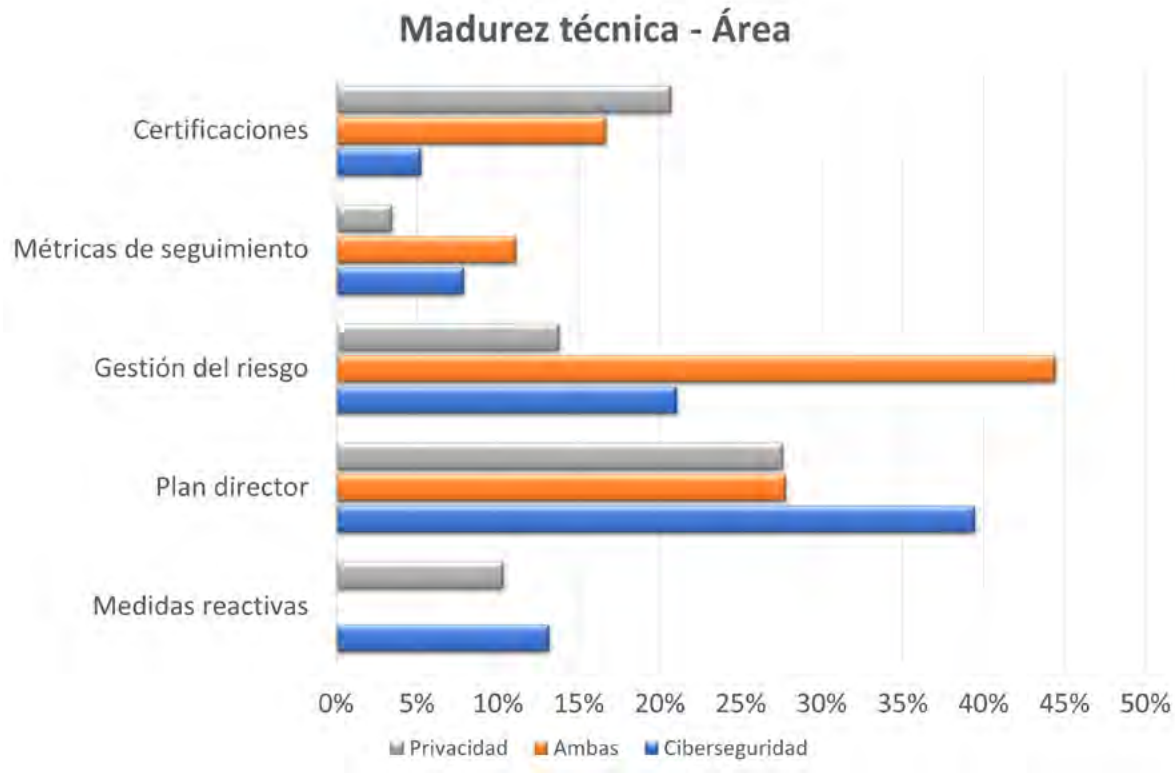
PLANIFICA: la prueba periódica de los procedimientos de gestión en entornos controlados es la única forma de conocer realmente si estamos o no preparados.

También hemos detectado que los profesionales de la ciberseguridad se ven con unos procedimientos más maduros que los de protección de datos o aquellos se realizan ambas funciones.

Esta disparidad puede deberse a que el proceso de gestión de incidentes de ciberseguridad lleva años documentándose, reportándose y gestionándose. Es posible que el DPD se sienta inseguro con un modelo de gestión nuevo para él en muchos casos y que lo perciba como menos maduro. Mientras que los CISOs se sienten seguros en su rol, llegando inclusive a decidir por sí mismos que es o no es una brecha de datos personales, y no informando al DPD con los peligros que ello supone.

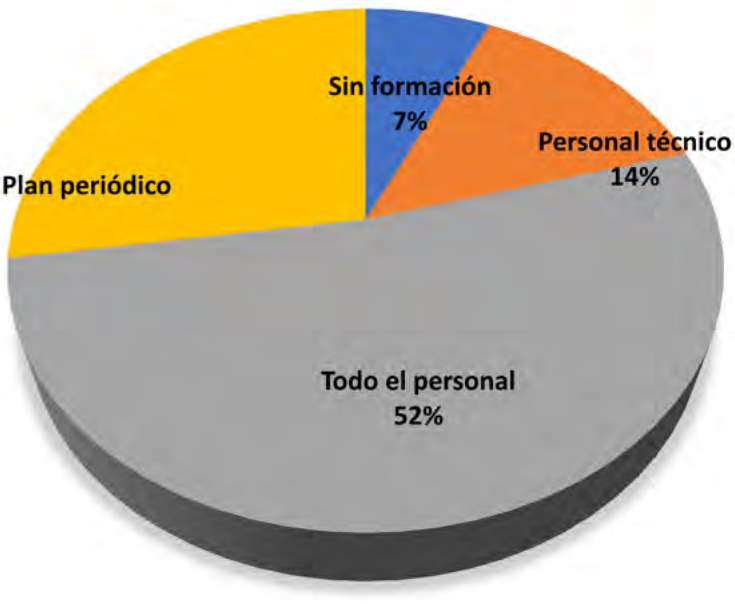
Mientras que curiosamente son los profesionales de la ciberseguridad los que tienen una peor percepción de la madurez de la gestión técnica.





Otra cuestión que quizás sea interesante resaltar es que los técnicos tienen una visión de la madurez en la gestión de riesgos inferior a los directivos, lo que únicamente puede explicarse por un problema en la comunicación de los procedimientos, que no fluyen a todos los implicados adecuadamente.

Lo que es coherente con los datos sobre los planes de formación. Dónde todavía tenemos un elevadísimo 7% de las compañías dónde no se da formación alguna sobre ciberseguridad a sus empleados, que en todos los casos son empresas que dicen haber sufrido brechas, o el 15% que solo se lo dan al personal técnico.

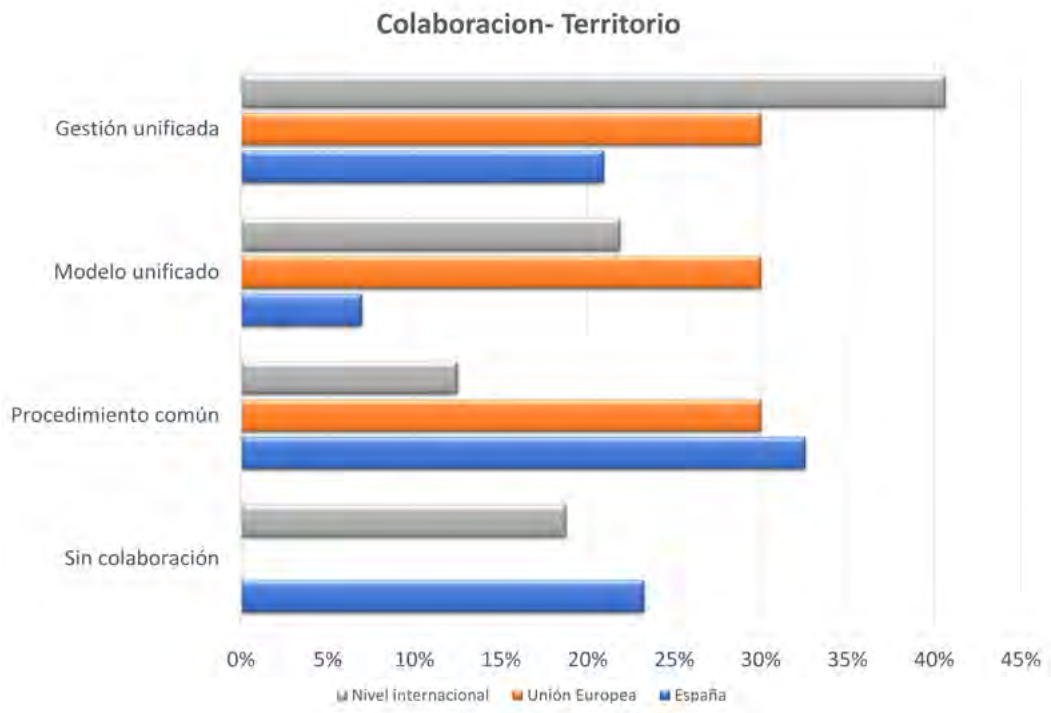


La mayor parte de las empresas cuentan con planes de formación genéricos, normalmente de terceros, que sí hace todo el personal pero que no se adaptan a los riesgos propios de la compañía y menos aún se segmentan en función de los riesgos y necesidades de las áreas destinatarias.

PLANIFICA: Debemos reforzar a cada eslabón de la cadena para aquello a lo que va a enfrentarse. Adaptar la formación a nosotros y a cada empleado la hará mucho más eficaz.

4.2. Trabajo en equipo

Uno de los mayores mitos sobre la protección de datos en las empresas es el del desencuentro entre CISO y DPD, como si ambas figuras fueran enemigos necesarios, cuando ambos gestionan las mismas situaciones y con los mismos objetivos para sus compañías, pero con un foco diferente simplemente.



Sin embargo, en la encuesta lo que vemos es que son muy pocas empresas en las que ambas figuras no colaboran en la fase previa de planificación para la gestión de brechas. Llegando inclusive a más de 45% de ellas a prepararse conjuntamente para estas con procedimientos e incluso modelos de gestión de riesgos conjuntos.

Si hay una gestión de riesgos aislada, lo que sucede en más de un 20% de los casos, luego las medidas de seguridad pueden estar viciadas. Muchas empresas han hecho los análisis de riesgos ya pensando en reciclar las medidas de seguridad que ya tenían implantadas y no al revés, lo que cumple con la obligación de establecer las medidas en base a los riesgos para los derechos y libertades de los interesados. Pocas nuevas medidas de seguridad que hayan supuesto inversión o coste han aflorado tras los preceptivos análisis de riesgos.

Obviamente en las organizaciones con personal asignado a ambas, ciberseguridad y protección de datos, su porcentaje con modelo de gestión de riesgos y de brechas unificado es muy superior, llegando casi al 70%.

Otras cuestiones que resaltar de los resultados obtenidos hacen referencia a un mayor grado de colaboración entre áreas en el caso de organizaciones internacionales frente a empresas que operan en exclusiva en -España.

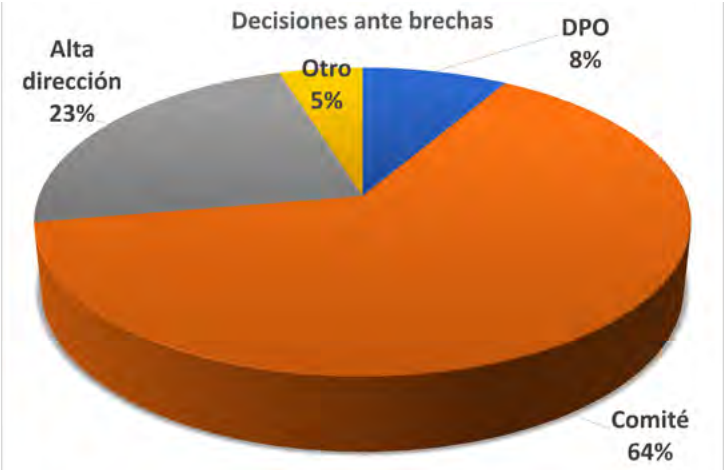
De nuevo surgen indicios que parecen indicar un menor grado de madurez en la gestión de brechas en organizaciones españolas.

Otra cuestión muy interesante, y que se puede observar en diferentes apartados de la encuesta, es como cambia la percepción entre las empresas que dicen haber sufrido brechas y aquellas que no. En este caso, tenemos que el porcentaje de no colaboración crece enormemente para las compañías que han sufrido brechas.

Podríamos pensar que menos colaboración nos hace más susceptibles de sufrir brechas, pero lo más probable en nuestra opinión, es que probar en entorno real los modelos muestran un grado de colaboración menor del esperado cuando se está planificando o preparando sin brecha real aún.

PLANIFICA: La colaboración entre ciberseguridad y protección de datos es imprescindible, y también hay que prepararse en conjunto y estar preparado para trabajar así en su momento.

Una brecha de datos personales es un evento crítico para la compañía, y muy complejo, que va a requerir de un equipo con personas de diferentes áreas trabajando al unísono. Pero estos equipos de trabajo o comités de crisis deben ser liderados y alguien debe ser el responsable de tomar las decisiones que sea necesarias a lo largo de la gestión de la brecha.



En este sentido, la mayor parte de las empresas se decantan por comités, reuniones de crisis donde se convoca a los responsables/representantes de todas las áreas implicadas, para entender y analizar los riesgos y en función de este análisis tomar decisiones.

Obviamente la coordinación puede ser del DPD, o suele y debe serlo, pero esta figura es la de un asesor cualificado que da su opinión al Comité o los directivos de la compañía que son los que, en última instancia, deben decidir cómo se va a gestionar la brecha.

5 GESTIONA

En este apartado hemos intentado conocer cómo gestionamos las brechas de datos personales en todas las fases de un incidente: detección, contención, análisis y resolución.

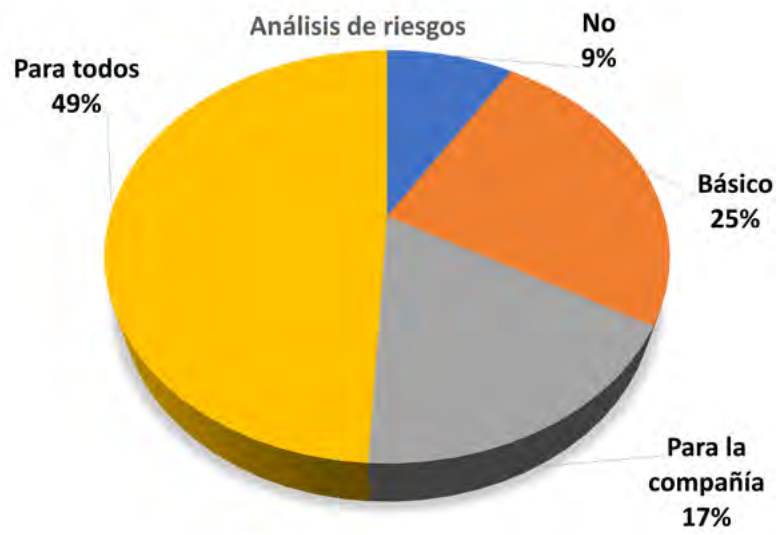
5.1. Detección y contención.

En cuanto a la detección parece que la detección de las brechas es fundamentalmente proactiva, es decir, que se detectan por los procesos de vigilancia interna y no por eventos externos a la organización, una vez ya se han materializado las mismas. Lo cual contrasta con el elevadísimo porcentaje de casos en los que se desconoce el tiempo transcurrido desde que se produce hasta la detección de la misma.

Parece que la pregunta sobre el tipo de detección ha dado lugar a diferentes interpretaciones y ha de mejorarse en siguientes ediciones, para evitar estos desalineamientos.

De gran interés resulta las respuestas obtenidas en cuanto al tiempo de contención de los incidentes, de las brechas de datos personales, es decir, cuánto tiempo transcurre desde que se detecta una brecha hasta que se ponen las medidas suficientes para evitar que siga produciendo algún impacto. No coincide con la resolución, que incluye el cierre de todas las actuaciones necesarias tras la brecha, sino la limitación de sus impactos negativos.

PLANIFICA: Aunque 72 horas parezcan suficientes para contener la brecha, sin una planificación previa no podremos preparar la notificación simultáneamente.



5.2. Análisis de riesgos

En cuanto al análisis de riesgos a realizar durante la gestión de la brecha de datos personales, la ley hace obligatorio realizar un análisis de riesgos para los derechos y libertades de los interesados. Cualquier análisis de riesgos para la compañía, financieros, reputacionales o de sanción, caen fuera de las previsiones legales y serán o no realizados en función de los procesos internos que haya decidido cada empresa.

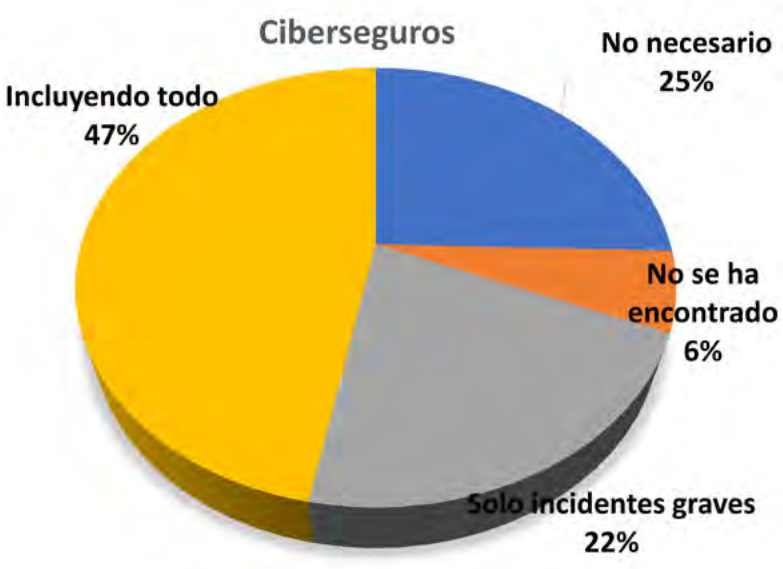
Sin embargo, parece que esta obligación de analizar los riesgos para los interesados no está aun correctamente asimilada en los procesos de las empresas, puesto que todavía tenemos más de un 25% de empresas que no han realizado ningún análisis de riesgos durante la brecha o solo lo han hecho para los riesgos internos de la misma; incurriendo en un incumplimiento en su deber de analizar las brechas desde la perspectiva de las personas y del impacto de la brechas en ellos.

Quizás esta sea otra de las causas del reducido número de notificaciones a la entidad de control que se producen en nuestro país.

> ***GESTIONA: No olvides el análisis de riesgos para los derechos y libertades de los interesados cuyos datos se han visto afectados por la brecha.***

5.3. Ciberseguros

Se les ha llamado incluso la última línea de defensa dentro de los incidentes de seguridad y la fórmula de gestión de riesgo más sencilla, transfiriendo este a las empresas aseguradoras. Pero en los últimos meses hemos visto como las primas se incrementaban hasta en más de un 30%, y a las grandes aseguradoras dejando fuera a los incidentes más típicos y de más impacto, como el Ransomware. Y el incremento de sanciones y de su cuantía en España posiblemente haga crecer más esta tendencia en los próximos meses.



Pero, al menos de momento, nos encontramos que en las grandes empresas los ciberseguros están muy extendidos, y que no se ha tenido problemas por el momento para su contratación.

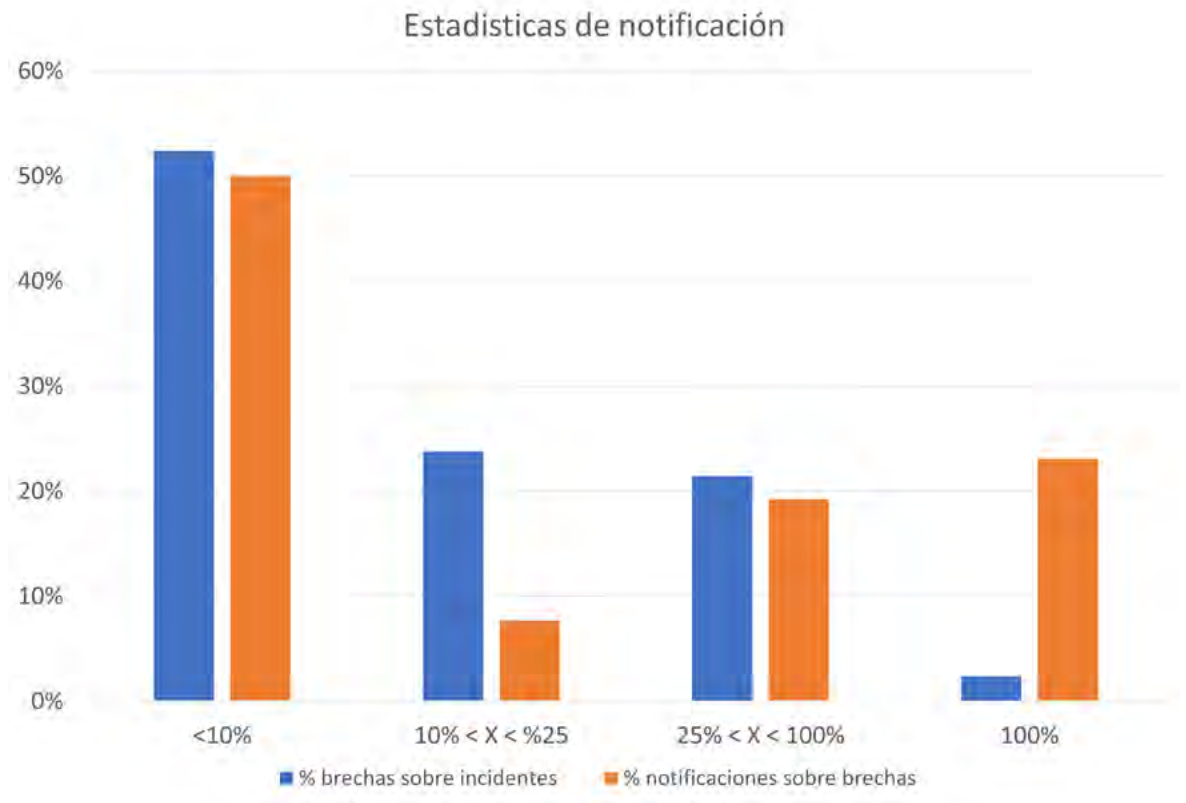
6 NOTIFICA

Uno de los objetivos propuestos en la encuesta era el de conocer el porcentaje de incidentes que se consideran brechas de protección de datos, y de estas las que se notifican a la autoridad de control. Con el fin de poder buscar causas al escaso número de notificaciones en España frente a nuestros vecinos europeos. Sin embargo, los resultados obtenidos en la encuesta han sido incoherentes, siendo imposible sacar conclusiones de los mismos. Se trata de un punto de mejora en siguientes ediciones de la encuesta.

6.1. ¿Notificamos?

La gráfica siguiente pone de manifiesto, ya no solo el bajo número de incidentes de seguridad detectados en las empresas, sino también el muy bajo número de estos que se identifican como brechas de datos personales, reduciéndose aún más el de brechas de datos personales con riesgos para los interesados que deban ser notificadas.

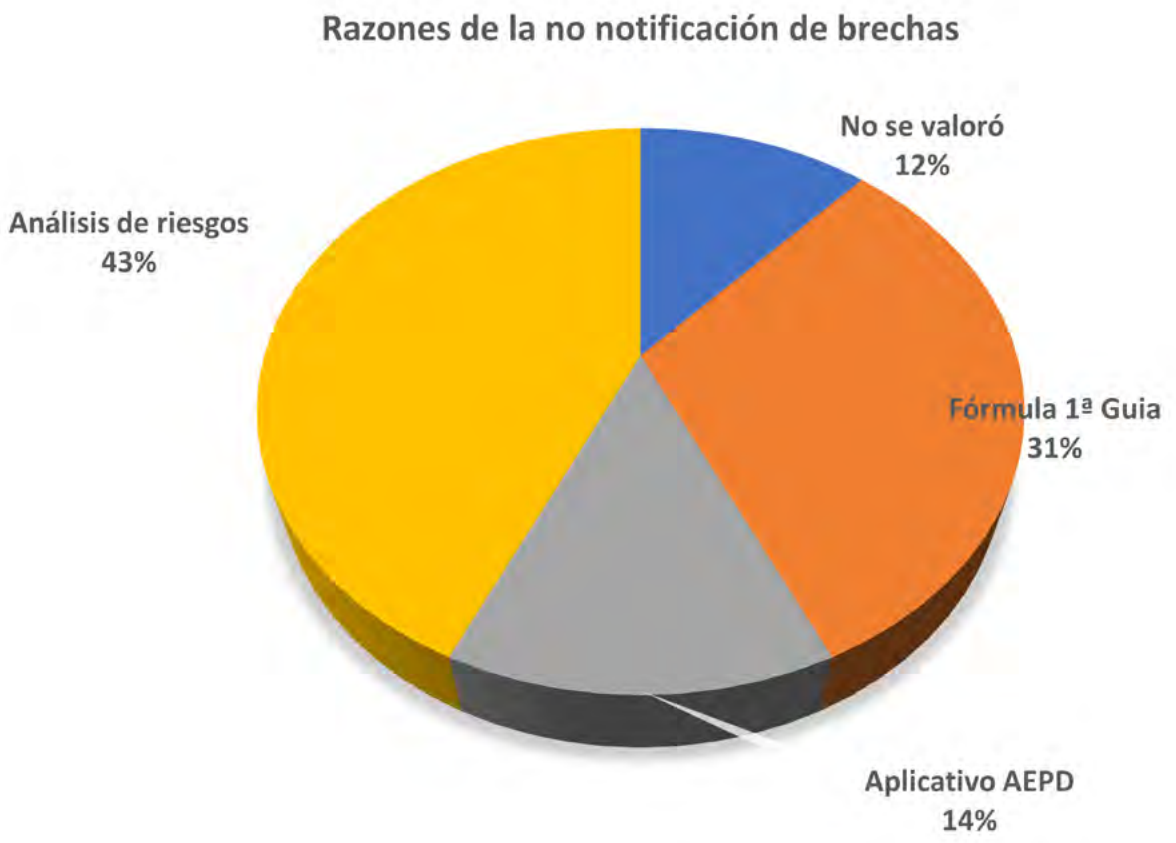
Dado que en la mayor parte de los procesos de negocio de la era digital hay datos personales implicados, sobre todo atendiendo a la amplia definición que hace el RGPD, como todo dato que permita identificar personas físicas, resulta muy extraño que la mayor parte de los incidentes de ciberseguridad que se sufren en nuestro país no afecten a datos personales.



NOTIFICA: Identificar adecuadamente los datos personales implicados en incidentes de seguridad y el impacto en los interesados debe ser prioritario.

Si finalmente un incidente no identificado correctamente causa un impacto en los derechos y libertades de los afectados y acaba por hacerse público, el resultado será siempre mucho peor para las organizaciones que en aquellos en que sí se hubiesen identificado y gestionado desde el inicio como brecha de datos personales. Desde luego, si no se atiende a la dimensión de la protección de datos, la contención de estos incidentes no tendrá en cuenta los riesgos para los propietarios de los datos y su impacto siempre será superior.

Por otra parte, dado el elevado número de brechas que no se notifican, la cuestión es saber la razón exacta de la no notificación a la autoridad de control para intentar entender por qué sigue existiendo un porcentaje tan elevado. Y en este caso resulta sorprendente que en un 12% no se evaluase la necesidad de notificar una brecha, cuando es una obligación legal desde hace ya más de tres años.



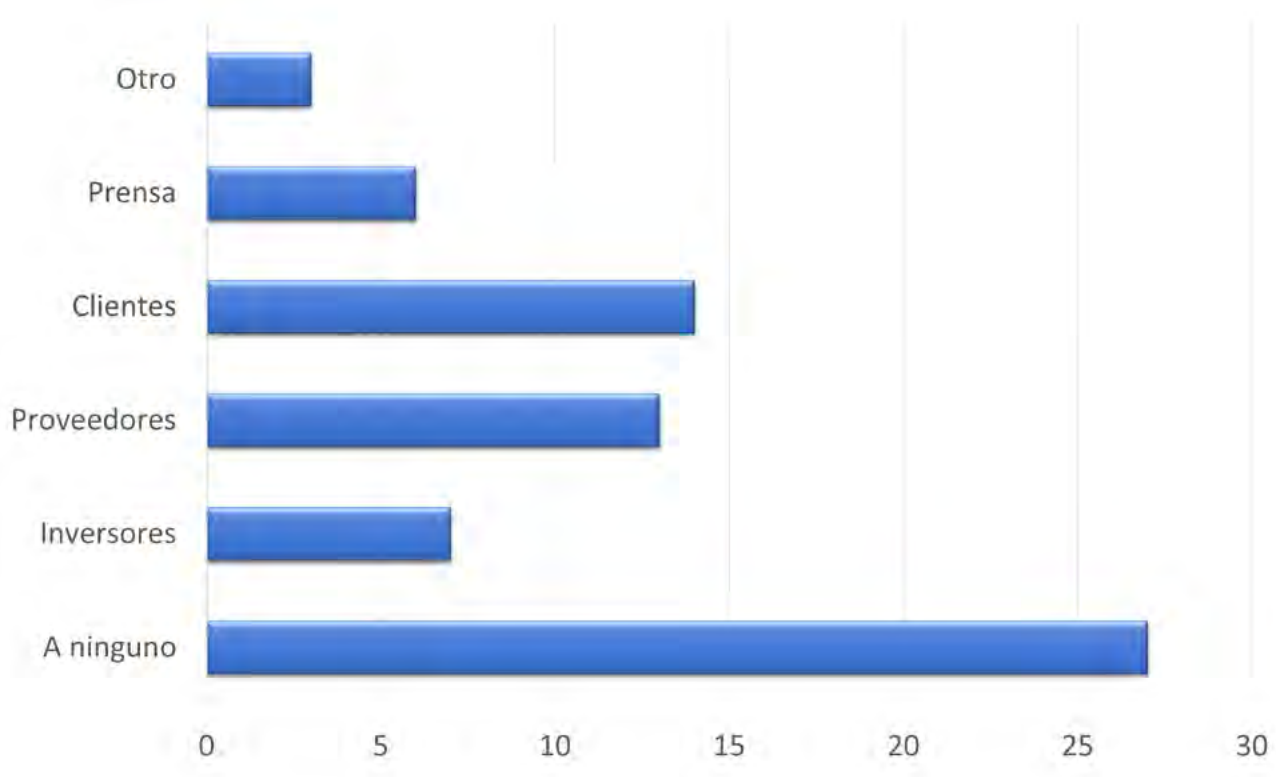
En cuanto a la comunicación de estas brechas a otros organismos, es escasa. Más del 50% de las brechas notificadas a la AEPD no son notificadas a ningún otro organismo, y solo el 20% se comunicaron también al INCIBE.

Causa extrañeza si, como parece, todos tenemos claro que la mayor parte de las brechas de protección de datos tienen su origen en incidentes y brechas de ciberseguridad, en los que INCIBE-CERT, como equipo de respuesta ante estos incidentes, debería tener acceso a la información sobre la misma y colaborar con su resolución.

Si la función de las notificaciones es la de incrementar la capacidad de respuesta del conjunto de la sociedad gracias al conocimiento que se adquiere de los diferentes eventos conocidos, parece que el grado de madurez en la sociedad española es bajo todavía a nivel de la administración de soporte de ciberseguridad.

6.2. Transparencia

Además de la notificación, tenemos que plantearnos la comunicación de las brechas de datos personales, en primer y prioritario lugar a las personas físicas afectadas como exige el RGPD, pero puede plantearse que las organizaciones empresariales existen también otros interesados, como: socios de negocio, proveedores que pueden ser impactados, etc.



Parece que lo mismo que sucede con las notificaciones a los organismos públicos, en este apartado también se aprecia una falta de madurez en cuanto a la comunicación proactiva a todos aquellos, que puedan verse impactados con las brechas que sufre una compañía.

De nuevo esta situación es muy diferente en España respecto al resto de la Unión Europea, dónde pasamos del 56% de los casos en los que no se comunica a nadie las brechas, frente al 8% europeo. También en este epígrafe parece que todavía tenemos margen de mejora.

6.3. Resultado de la notificación

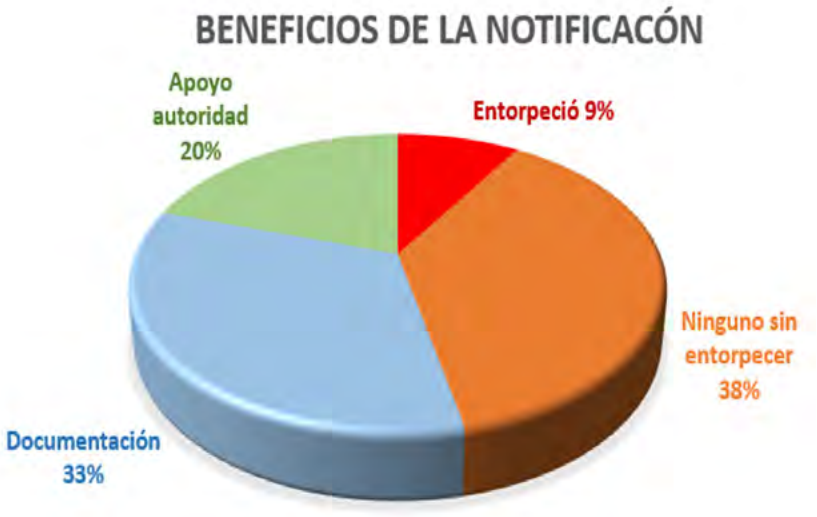
Es importante conocer también cual ha sido la experiencia de notificación a la autoridad de control tanto desde el punto de vista del resultado obtenido, como del esfuerzo que ha supuesto para la organización.

En cuanto al esfuerzo que ha supuesto el proceso de notificación en la gestión de la brecha, el 60% de los encuestados indican que no ha sido necesario desviar recursos de la gestión de las brechas a la notificación, y el porcentaje de empresas que han notado un impacto negativo en la gestión de la brecha a causa del esfuerzo de la notificación es realmente bajo, del 2%.

Sin embargo, creemos que este dato habrá que contrastarlo para el caso de pequeñas y medianas empresas, con menos recursos sobre todo en las áreas de ciberseguridad y protección de datos, que no han sido precisamente las que mayoritariamente han participado en esta encuesta.

En cuanto a los beneficios que las organizaciones han podido percibir por la notificación en sí, mayoritariamente se decantan por la no existencia de ningún beneficio, aunque sin llegar a tener una percepción negativa de la misma más que en un pequeño porcentaje.

Es necesario destacar que el porcentaje de casos en los que se ha considerado que la autoridad de control sirvió de ayuda y de apoyo durante la gestión de la brecha es todavía muy reducido, del 20%, mientras que dicho valor sube hasta el 30% para los casos ubicados en la Unión Europea. Parece que la mayor madurez en Europa en cuanto a la notificación de brechas no solo se sitúa en el ámbito empresarial, sino también en el de la autoridad de control.



Otro dato interesante extraído de la encuesta es que sólo el 3% de DPD considera que la autoridad de control ha sido un apoyo en la gestión de la brecha a través de la notificación.

RESUELVE: Es imprescindible mejorar la comunicación entre la AEPD y los DPD para que estos perciban el apoyo de la Agencia tras la notificación de una brecha.

6.4. Resultado del proceso de gestión de la brecha

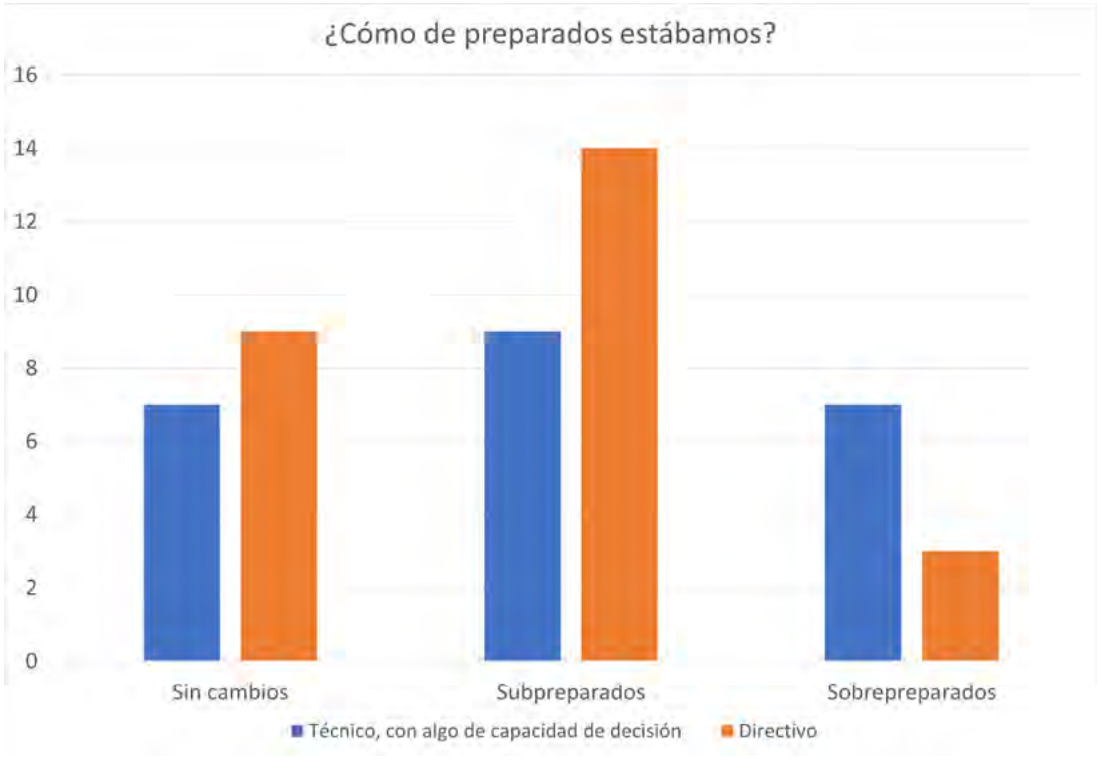
Una de las cuestiones que queríamos conocer era si, tras la experiencia de gestión de una brecha real, cambiaba o no la percepción en cuanto al nivel de preparación de la organización para acometer esta gestión.

Y el resultado es que casi en el 50% de los casos, los profesionales detectaron que no estaban suficientemente preparadas las compañías y su percepción de las capacidades de la empresa empeora tras la brecha. Por lo que, parece que la realización de simulacros o pruebas de los procedimientos y planes de gestión de brechas ayudaría a estar realmente mejor preparados y es la única forma de detectar ciertas deficiencias y arreglarlas, antes de que supongan impactos negativos durante la gestión de una brecha real y con impacto real en los interesados y en la compañía.

> ***RESUELVE: Hay que probar los procedimientos completos para poder conocer realmente el grado de preparación de la compañía ante casos reales.***

Otro dato interesante sobre el cambio de percepción de nuestros procedimientos y medidas es la diferente visión entre los profesionales técnicos frente a los dedicados a la gestión. Los técnicos, en general, mantienen una percepción mejor en cuanto a preparación previa.

Es posible que esta divergencia se deba a una mayor madurez en las áreas técnicas en la gestión de incidentes, con muchos años de experiencia en gestión de incidentes y con medidas técnicas más adaptadas ya a la realidad de las organizaciones. Frente a los procesos más de gestión o más enfocados a las nuevas obligaciones que implica el RGPD y la gestión de brechas personales, con menos tiempo de rodaje y mejora. Lo que nos lleva de nuevo, a la importancia de probar en entornos controlados también los procedimientos.



6.5. Impacto en el negocio

Una de las causas que siempre hemos creído en el colectivo de DPD que estaba detrás del escaso número de casos de notificaciones de brechas ante la Agencia Española de Protección de Datos, frente a otros países de Europa, es el miedo al impacto negativo de estas en la compañía.

En cuanto al impacto en sanciones los números aportados estos últimos años demuestran que es infundado, puesto que, de las más de 1.370 brechas notificadas en el 2020, sólo se abrieron 85 expedientes de requerimiento de información de los cuales 40 finalizaron en un proceso sancionador.

Por lo que resultaba relevante conocer la percepción de las empresas que han sufrido brechas de datos personales en cuanto al impacto de estas en el negocio, a nivel de clientes y de imagen de marca. Y el resultado es que tampoco resulta de un impacto negativo en absoluto, y que incluso se han producido impactos positivos en cuanto a la imagen de la compañía y la confianza de sus clientes.

RESUELVE: No hay impacto perceptible en el negocio por comunicar brechas.

Por otra parte, directamente en cuanto al impacto en las áreas de ciberseguridad y de protección de datos, y alineado con lo que ya vimos de la percepción de estar menos preparado de lo necesario, lo que observamos es que la mitad de las empresas que han sufrido brechas, tras estas, han incrementado sus inversiones en ciberseguridad.

Por otra parte, también resulta curioso observar que para los DPD también vemos que el porcentaje de incremento de recursos se reduce muchísimo. Parece que existe un desconocimiento por su parte de lo que sucede en ciberseguridad tras las brechas, es decir, que no se está gestionado por su parte la mejora continua que todo incidente debería generar en la compañía. Lo que será un error importante, no tomar las lecciones aprendidas en el ámbito de la protección de datos para mejorar las capacidades de la organización.

Si no se toman a tiempo las medidas adecuadas, las brechas de datos personales pueden entrañar daños y perjuicios para las personas físicas; responderemos no tanto por sufrirlas como por la gestión que hagamos de ellas.

CONCLUSIÓN FINAL

7

Como conclusión a esta Encuesta nos hemos permitido utilizar las conclusiones que nos han aportado en la propia encuesta y que consideramos que resumen muy bien todo lo observado:

> ***Las brechas ocurren y hay que gestionarlas.***
> ***Durante un ciberincidente no es momento de hacer experimentos ni de echar a correr: se trata de aplicar los procedimientos ya definidos y hacer frente a las responsabilidades públicas y privadas.***

ANEXO. Encuesta - Guía Práctica para la Gestión y Notificación de Brechas de Seguridad

Encuesta – Guía Práctica para la Gestión y Notificación de Brechas de Seguridad

Con el fin de clarificar los términos utilizados a lo largo de la presente encuesta hemos de tener que cuenta que se definen:

- Incidente de Ciberseguridad: todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información.

- Brecha de Seguridad: todo incidente de seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Encuesta – Guía Práctica para la Gestión y Notificación de Brechas de Seguridad

Datos demográficos

* 1. Tamaño de la empresa

- ○ Gran empresa
- ○ Mediana
- ○ Pyme
- ○ Micropyme

* 2. Área de trabajo

- ○ Ciberseguridad
- ○ Privacidad
- ○ Ambas

* 3. Grado de responsabiliad en la empresa

- ○ Técnico, con algo de capacidad de decisión
- ○ Directivo

* 4. Sector de la empresa

* 5. Territorio de trabajo

- ○ España
- ○ Unión Europea
- ○ Nivel internacional

* 6. ¿Ha sufrido algún incidente de ciberseguridad en los últimos dos años?

- ○ SI
- ○ NO

7. Cómo sería la toma de decisiones de su organización durante una brecha de seguridad'

- ◯ Alta dirección
- ◯ Comité multidisciplinar de protección de datos (incluyendo representantes de otras áreas como IT, Compliance, Asesoría Jurídica, etc,)
- ◯ DPO
- ◯ Compliance Officer
- ◯ Otro (especifique)

Encuesta – Guía Práctica para la Gestión y Notificación de Brechas de Seguridad

PLANIFICA

* 8. Como definirías el grado de madurez de tu empresa en cuanto a las medidas técnicas implantadas para evitar ciberataques

- ◯ Existen medidas que se van implantando en base a experiencias reactivas
- ◯ Se ha definido un plan director de seguridad y se están implantando medidas en base a este
- ◯ La organización dispone de una certificación en seguridad de la información
- ◯ Existe un proceso de implantación de medidas basado en la gestión del riesgo para la compañía de las diferentes amenazas en ciberseguridad (eliminar una)
- ◯ Se han definido métricas para para medir los resultados de mejora en base a las medidas implantadas según el proceso de análisis de riesgos en ciberseguridad y mejora continua (eliminar una)
- ◯ Otro (especifique)

* 9. Como definirías el grado de madurez de tu empresa en cuanto a los procedimientos de gestión de brechas de seguridad

- ◯ No existen procedimientos escritos, las brechas se gestionan en “best efford”
- ◯ Existe un procedimiento general único de gestión de brechas de seguridad que implica a todas las áreas de la compañía, pero que no se ha comunicado adecuadamente
- ◯ Existe un procedimiento general único de gestión de brechas de seguridad que implica a todas las áreas de la compañía, que sí se ha comunicado adecuadamente
- ◯ Existe un proceso de gestión de las brechas de seguridad enfocado a la mejora continua, que incluye pruebas del mismo y difundido adecuadamente en la organización
- ◯ Otro (especifique)

* 10. Como definirías el grado de formación y concienciación del personal de la organización en cuanto a la gestión de brechas de seguridad

- No existe formación ni concienciación específica en cuanto a brechas de seguridad para el personal
- Únicamente está formado el personal técnico directamente implicado en la gestión de las brechas
- Se han dado cursos sobre la importancia de la ciberseguridad a todo el personal
- Existe un plan anual de formación del personal que incluye capacitación en la gestión de brechas de seguridad específica según el puesto y para todo el personal
- Otro (especifique)

* 11. Como definirías el grado de colaboración entre las áreas de ciberseguridad y privacidad en la planificación previa a las brechas de seguridad

- Cada área gestiona sus riesgos y define sus procedimientos por separado
- Se ha definido conjuntamente un procedimiento de gestión de brechas de seguridad entre ambas áreas
- Se ha definido conjuntamente un modelo de gestión de riesgos entre ambas áreas
- Existe un único modelo de gestión de riesgos y un único procedimiento de gestión de brechas que contempla las prespectivas de ciberseguridad y privacidad conjuntamente
- Otro (especifique)

Encuesta – Guía Práctica para la Gestión y Notificación de Brechas de Seguridad

GESTIONA

12. ¿Qué porcentaje de los incidentes han sido detectados proactivamente por la organización?

- ◯ Ninguno
- ◯ 25%
- ◯ 75%
- ◯ Todos
- ◯ Otro (especifique)

* 13. ¿Ha contratado la organización un ciberseguro que cubra las posibles consecuencias de una brecha de seguridad?

- ◯ No lo ha considerado necesario.
- ◯ No ha podido conseguir en el mercado una aseguradora o póliza adecuada para suscribir.
- ◯ Sí, pero solo para los incidentes de ciberseguridad más graves.
- ◯ Sí, incluyendo toda clase de incidentes de ciberseguridad.
- ◯ Otro (especifique)

* 14. Se realizaron análisis de riesgos de la brecha durante su gestión

- ◯ No, no hubo tiempo
- ◯ Sí, pero solo para la compañía
- ◯ Sí, pero solo los análisis que la ley obliga a la compañía (comunicación de incidentes)
- ◯ Sí, tanto para la compañía como para los terceros afectados, a nivel de ciberseguridad y en protección de datos
- ◯ Otro (especifique)

* 15. ¿Qué tiempo medio de detección han tenido los incidentes?

- ○ No lo sabemos
- ○ 1 semana
- ○ 3 meses
- ○ Más de 3 meses
- ○ Otro (especifique)

* 16. ¿Tiempo medio de contención de las brechas graves sufridas?

- ○ Durante las primeras 72 horas
- ○ 1 mes
- ○ Más de 6 meses
- ○ No se pudo contener
- ○ Otro (especifique)

* 17. ¿Qué porcentaje de los incidentes sufridos han supuesto una “brecha de seguridad de datos personales”?

0% 100%

* 18. ¿Qué porcentaje de las brechas de seguridad ha comunicado a la autoridad de control?

0% 100%

* 19. ¿Cual ha sido la causa más común de no comunicación de brechas de seguridad a la autoridad de control?

- ( ) No se tuvo en cuenta, durante la gestión de la brecha, la necesidad de comunicación
- ( ) Se aplicó la fórmula de la guía de Gestión de Brechas de Seguridad de la AEPD y el resultado fue que no hacía falta comunicar
- ( ) Se utilizó la aplicación de la AEPD y el resultado fue que no era necesario comunicar
- ( ) Tras realizar un análisis de riesgo completo y documentado, no se observó un riesgo para los derechos y libertades de los interesados afectados
- ( ) Otro (especifique)

20. De entre las medidas citadas, marcar todas las que se han implantado en relación al proceso de Gestión de brechas de seguridad

- [ ] Existe un plan periódico de pruebas de los procedimientos y medidas técnicas implantadas ante posibles brechas
- [ ] Se ha hecho una asignación oficial y pública en la compañía de asignación de responsabilidades en caso de brechas de seguridad
- [ ] Se cuenta con proveedores especializados a los que contratar en caso de necesidad
- [ ] Se ha contratado un ciberseguro que cubra las posibles consecuencias de una brecha de seguridad
- [ ] Otro (especifique)

* 21. ¿Qué porcentaje de las brechas de seguridad sufridas ha comunicado voluntariamente a los interesados?

0% 100%

* 22. ¿Qué porcentaje de las brechas de seguridad sufridas ha comunicado a los interesados por orden de la AEPD?

0% 100%

23. ¿A qué otras administraciones ha notificado brechas de seguridad?

- [ ] Ninguno
- [ ] Incibe
- [ ] Banco de España
- [ ] LPIC
- [ ] Otro (especifique)

* 24. ¿A qué otros terceros ha notificado brechas de seguridad?

- [ ] Inversores
- [ ] Proveedores
- [ ] Clientes
- [ ] Prensa/Comunicación pública
- [ ] Otro (especifique)

* 25. : ¿Qué porcentaje de las brechas de seguridad ha comunicado voluntariamente a terceros (no afectados en sus datos personales): clientes, proveedores, socios, etc?

0% 100%

* 26. ¿Has tenido que desviar recursos desde la gestión de la brecha hacia obligaciones exclusivas de comunicación?

- ( ) Sí, y ha supuesto un impacto negativo en la mitigación de la brecha
- ( ) Sí, pero no ha supuesto un impacto negativo en la mitigación de la brecha
- ( ) Ha supuesto únicamente una dedicación parcial de algún recurso desde la gestión de la brecha a la comunicación
- ( ) No no ha sido necesario porque la documentación para la comunicación está alineada con la documentación de gestión de la brecha
- ( ) Otro (especifique)

* 27. ¿Qué beneficios considera que le ha proporcionado la comunicación de la brecha a la autoridad de control?

- Ninguno, ha entorpecido la gestión y resolución de la brecha por el desvio de recursos a la generación de informes específicos
- Ninguno, pero tampoco ha supuesto un entorpecimiento
- Obligar a la documentación exhaustiva de la brecha ayuda en su gestión
- He recibido apoyo de la autoridad de control, implicándose en las tareas de mitigación y resolución de la brecha
- Otro (cspccifiquc)

Encuesta – Guía Práctica para la Gestión y Notificación de Brechas de Seguridad

RESUELVE

* 28. ¿Cómo ha cambiado la percepción en la preparación de la organización tras sufrir una brecha de seguridad?

- ( ) En nada, estábamos tan preparados como pensábamos
- ( ) Se detectó que no estábamos suficientemente preparados
- ( ) Se detectó que el grado de preparación era superior al esperado
- ( ) Otro (especifique)

* 29. ¿Qué impacto ha supuesto para la organización la comunicación a los interesados de una brecha de seguridad?

- [ ] Ninguno
- [ ] Pérdida de clientes
- [ ] Pérdida del nivel de confianza de los clientes
- [ ] Mejora en el nivel de confianza de los clientes
- [ ] Otro (especifique)

* 30. ¿Qué impacto ha supuesto para la organización la comunicación pública de una brecha de seguridad?

- [ ] Ninguno
- [ ] Empeoramiento subjetivo de la imagen de marca
- [ ] Pérdida de clientes posterior
- [ ] Mejora subjetiva de la imagen de marca y ganancia de clientes
- [ ] Otro (especifique)

* 31. ¿Ha cambiado algo para las áreas de ciberseguridad y privacidad la experiencia tras la brecha?

- ( ) No, todo sigue igual
- ( ) La dirección ha hecho responsable a las áreas y ha tomado medidas disciplinarias
- ( ) La dirección ha asignado más recursos a las áreas implicadas
- ( ) La dirección ha decidido externalizar en todo o en parte la gestión de estas áreas
- ( ) Otro (especifique)

Encuesta – Guía Práctica para la Gestión y Notificación de Brechas de Seguridad

CONCLUSIÓN

* 32. Con la experiencia de ahora y en pocas palabras, ¿cómo definiría su experiencia y qué no volvería a hacer si sufriera otra brecha de seguridad?

Disponible en

www.ismsforum.es