Informe rating BitSight

BHC
BASQUE HEALTH CLUSTER

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad

Euskal Herriko Zibersegurtasun Industriak

Contenido

Introducción

La ciberseguridad engloba muchos ámbitos distintos, no solo la informática y las telecomunicaciones, sino también aspectos relacionados con la gestión del riesgo y la protección estratégica de las organizaciones. En un entorno cada vez más digitalizado e interconectado, cualquier debilidad puede suponer una oportunidad para un atacante y derivar en un impacto importante para las compañías, tanto a nivel operativo como económico o reputacional.

Dentro de la protección de redes y comunicaciones existen diversas herramientas que ayudan a identificar qué se está haciendo correctamente y en qué aspectos sería necesario mejorar. Entre ellas se encuentran los tests de penetración, las pruebas de redes u otras actividades técnicas que permiten evaluar de forma directa el estado de la seguridad. Sin embargo, este tipo de acciones no siempre ofrece una visión continua ni comparativa del nivel de ciberseguridad de una organización frente a otras similares.

Una de las herramientas que ha ido ganando relevancia en los últimos años son las soluciones de rating de ciberseguridad. Estas plataformas utilizan **escáneres no intrusivos** que permiten analizar distintos indicadores de las redes corporativas expuestas a Internet y asignar una puntuación en función de lo observado. De este modo, es posible obtener una visión objetiva del nivel de ciberseguridad, identificar tendencias y comparar resultados entre empresas o sectores. En este ámbito han surgido diversas compañías, cada una con su propio algoritmo y sistema de puntuación.

En este caso, desde Cybasque se han obtenido varias licencias de la herramienta **BitSight**, una de las empresas pioneras en este tipo de soluciones y una de las referencias actuales en el sector de la ciberseguridad. Para calcular sus puntuaciones, BitSight analiza distintos parámetros agrupados en los siguientes campos:

- Sistemas comprometidos
- Comportamiento del usuario
- Divulgación pública
- Diligencia

Dentro de cada uno de estos campos, BitSight aplica distintos controles técnicos y análisis continuos que permiten evaluar de forma objetiva el nivel de ciberseguridad de las organizaciones a partir de información observable desde el exterior. La puntuación final no se obtiene a partir de un único elemento, sino de la combinación y

ponderación de múltiples indicadores, que se actualizan de forma periódica en función de los cambios detectados.

En el ámbito de sistemas comprometidos, BitSight identifica posibles señales de compromiso en los activos expuestos, como la presencia de malware, comunicaciones con infraestructuras maliciosas conocidas o la pertenencia de sistemas a redes de bots. Este análisis se basa en la correlación de datos procedentes de fuentes de inteligencia de amenazas y en la observación del comportamiento de las direcciones IP y dominios asociados a la organización.

En cuanto al comportamiento del usuario, se analizan patrones que pueden indicar prácticas inseguras, como el uso de credenciales débiles, configuraciones que facilitan accesos no autorizados o servicios expuestos sin las medidas de protección adecuadas. Estos indicadores permiten detectar situaciones que, sin ser necesariamente vulnerabilidades técnicas, aumentan el riesgo de incidentes de seguridad.

El apartado de divulgación pública se centra en la información y los servicios que la organización expone a Internet. En este campo se evalúa la existencia de servicios innecesarios o mal configurados, la exposición de datos sensibles y la presencia de vulnerabilidades conocidas en sistemas accesibles públicamente. Para ello, BitSight tiene en cuenta bases de datos de vulnerabilidades y analiza el nivel de actualización y configuración de los servicios detectados.

Por último, el campo de diligencia mide la capacidad de la organización para mantener una correcta higiene de ciberseguridad a lo largo del tiempo. En este apartado se valora, entre otros aspectos, la rapidez con la que se aplican actualizaciones y parches, la gestión adecuada de certificados y cifrados, la eliminación de servicios obsoletos o inseguros. Este conjunto de indicadores refleja el grado de atención y mantenimiento continuo que la organización dedica a su postura de seguridad.

La puntuación final de BitSight se consigue a través de un proceso en el que la información técnica observada se transforma, paso a paso, en un indicador de riesgo comprensible y comparable. En primer lugar, la plataforma recopila señales externas asociadas a la organización, como direcciones IP, dominios o infraestructuras que BitSight atribuye a esa entidad. Estas señales proceden de observación pasiva de Internet, de fuentes abiertas y de la monitorización de actividades maliciosas conocidas. Cabe destacar que no se realizan auditorías internas ni escaneos intrusivos, sino que todo el análisis se basa en lo que es visible desde el exterior.

Una vez recopiladas estas evidencias, no se evalúan de forma aislada, sino que se contextualiza estadísticamente. Cada hallazgo se compara con el comportamiento del conjunto de organizaciones monitorizadas, de modo que una misma configuración o debilidad puede tener un impacto distinto en función de lo habitual o excepcional que resulte en el mercado. De esta forma, el modelo no responde a una lógica de cumplimiento normativo, sino a una evaluación relativa del riesgo.

Después, el sistema pondera cada evidencia en función de su gravedad y de su persistencia en el tiempo. No tiene el mismo efecto un problema puntual que una situación mantenida durante semanas o meses, ni una debilidad menor que una evidencia clara de compromiso, como la presencia de malware o comunicaciones con infraestructuras de control. Además, se tiene en cuenta la recurrencia de los eventos y el alcance dentro de la superficie digital de la organización, lo que puede provocar que un número reducido de activos con problemas graves tenga un impacto significativo en la puntuación global.

Después de este análisis, las evidencias se agrupan por grandes áreas de riesgo y se combinan para generar puntuaciones parciales. Estas puntuaciones no tienen el mismo peso entre sí, ya que BitSight otorga una importancia especialmente alta a los indicadores que demuestran compromisos reales o comportamientos que históricamente se asocian con incidentes de seguridad. El resultado es una valoración agregada que refleja la probabilidad de que la organización experimente un incidente, más que su nivel de madurez o el esfuerzo realizado en seguridad.

Finalmente, el valor resultante se ajusta teniendo en cuenta el grado de confianza estadística del análisis, para evitar penalizaciones derivadas de una visibilidad limitada y se traduce a la escala numérica de 250 a 900 que BitSight utiliza como rating final. Esta cifra permite comparar organizaciones entre sí de forma sencilla, pero siempre debe interpretarse como un indicador de riesgo observable desde el exterior y no como una evaluación completa del estado real de la ciberseguridad interna.

En origen, este tipo de servicios estaba pensado principalmente para que las propias organizaciones conocieran su nivel de ciberseguridad y para facilitar la evaluación del riesgo asociado a sus proveedores. En los últimos años, este enfoque ha cobrado mayor importancia debido al aumento de incidentes relacionados con la cadena de suministro (supply chain), donde las debilidades de terceros pueden afectar directamente a empresas de mayor tamaño o criticidad.

Este aspecto está estrechamente ligado a la Directiva NIS2, que introduce nuevos requisitos en materia de ciberseguridad y establece la necesidad de que los

proveedores de determinados sectores cumplan con unas medidas mínimas de seguridad. En este contexto, herramientas como BitSight permiten disponer de una visión general del nivel de ciberseguridad de las organizaciones y facilitan la gestión del riesgo de terceros.

En el caso de Cybasque, el objetivo del uso de esta herramienta es generar información sectorial que permita dar servicio de dos maneras principales:

- Informar a los clústeres del nivel de ciberseguridad de sus empresas.
- Disponer de un mapa general de los niveles de ciberseguridad en los sectores económicos más relevantes.

Con esta información, las empresas socias de Cybasque pueden contar con una visión global que les ayude a identificar oportunidades, orientar mejor sus esfuerzos y comprender el estado general de la ciberseguridad en el territorio vasco.

Campañas

El uso que se le va a dar a esta herramienta será el de monitorizar a compañías de clústeres con los que Cybasque colabora, se ha estipulado un calendario para ir viendo sectorialmente el índice general de cada sector. Estos informes serán de gran utilidad tanto para los clústeres, para que vean cómo se encuentran sus socios y su sector a nivel de ciberseguridad con el resto de sectores, como para empresas de ciberseguridad.

Será también beneficioso para las empresas socias de Cybasque, ya que podrán dirigir sus esfuerzos a sectores que se sepan que están en niveles más bajos de ciberseguridad y necesiten ayuda para poder securizar mejor sus redes y sistemas.

Para la realización de estas campañas se han enumerado muchos de los clústers con los que se mantiene relación, tanto desde Cybasque como desde GAIA. Esta lista se ha elaborado pensando en posibles congresos que tengan cada clúster y poder buscar algún sitio para contar los datos obtenidos en estos informes.

AÑO	MES	SECTOR
2025	Septiembre	Robótica
	Octubre	Químico
	Noviembre	TEIC
	Diciembre	Transportes, Movilidad y Logística
2026	Enero	Financiero
	Febrero	**Salud**
	Marzo	Automoción
	Abril	Energía
	Mayo	Alimentación
	Junio	Máquina-Herramienta

Tabla 1: sectores a monitorizar, hecho desde el G.T. Generación de demanda de Cybasque

Con este calendario se irán creando distintos informes, para que al finalizar junio de 2026 se pueda hacer un informe general de toda la información que se ha ido obteniendo a lo largo de este tiempo. Para así, ver los niveles de ciberseguridad en los que se encuentran cada uno de los sectores que se han examinado, ese informe final puede ser utilizado tanto para las empresas de ciberseguridad, como para administraciones públicas, clústeres o las propias empresas de dicho sector.

Ese informe final dará la visión global de la situación en Euskadi, ayudando a mejorar la ciberseguridad de una región que ha sufrido distintos ataques. Un territorio muy industrial, donde hay muchas plantas y muchas fábricas, entornos críticos, los cuales

son propensos a recibir ataques. Las consecuencias de que esto suceda pueden llevar a meses de parón, miles de euros perdidos, incluso peligros físicos para aquellas personas que vivan cerca.

El País Vasco se está convirtiendo en un foco esencial y con muchos profesionales muy concienciados con la ciberseguridad, más específicamente centrados en la ciberseguridad industrial. Cada vez son más las empresas de ciberseguridad que trabajan aquí y muchos los sectores que necesitan de sus servicios.

Sector sanitario

Con el acceso que tiene Cybasque a esta plataforma (BitSight), se han generado distintos informes de los socios del Basque Health Cluster, uno de ellos es el Portfolio Overview, que muestra la puntuación actual de todos los socios y los ordena de mayor a menor.

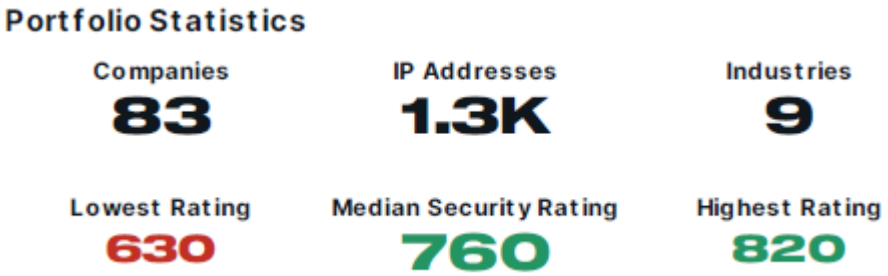
Este informe no sólo nos ayuda a saber la puntuación en la que se encuentra cada compañía, sino que da un ranking de cómo está cada compañía en seguridad y la puntuación general del sector de las finanzas y las inversiones. También nos enseña la progresión del último mes, muchas de las compañías se han mantenido estables, pero hay quienes han mejorado en su rating y otras muchas que lo han empeorado.

Un buen trabajo de ciberseguridad sería ver qué es lo que ha ocurrido para que estas empresas hayan perdido puntos en su rating y poder mejorarlo. En el informe podemos apreciar que hay tres tipos de ratings, los que están en verde (buenos), los amarillos (normales) y los rojos (bajos), se puede ver que hay muchos más verdes que rojos.

La mediana de puntos de rating de empresas de BHC está en 760, está en un punto bastante medio, teniendo en cuenta que lo mínimo es 250 y el máximo 900. Bien puntuada comparada con otros sectores económicos, pero en ciberseguridad siempre hay algo que puede mejorar, ahora con las nuevas normativas que vienen la ciberseguridad va a ser un punto diferencial para los clientes.

Es cierto que cuanto más ciberseguro se está es complicado mejorar mucho, es decir, una empresa que su rating es 400, es fácil que con varias acciones positivas pueda subir a 500, pero aquella empresa cuyo rating está en 700 tendría que hacer muchos más esfuerzos para llegar a 800. Esta es una de las partes complicadas de la ciberseguridad, la otra es que esa inversión suele ser bastante costosa.

Los valores importantes que han salido de este informe son los siguientes:

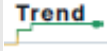


Tal y como vemos en las siguientes columnas, las empresas que se encuentran en los primeros puestos, por lo general, han mejorado sus puntuaciones en el último tramo antes de sacar el informe. Se puede apreciar que sólo hay una empresa en esa zona peligrosa (roja) de las 83 que se han examinado, aunque se puede apreciar cómo varias de las empresas vienen de haber pasado tiempo en zona baja.

El sector sanitario al ser un sector muy crítico debería de ser un sector muy ciberseguro y debería prevenir todos los posibles ataques o inconvenientes que le surjan, no únicamente de la parte de ciberseguridad, sino de cualquier posible inconveniente. Se conocen muchos tipos de ataques o boicots a centros u hospitales médicos, tanto de forma cibernética como presencial o de otras maneras, la salud en un tema importante y cuando se quiere hacer daño es uno de los puntos directos que utilizan los malhechores.

A continuación, la lista de puntuaciones:

Entidad 1		820	Entidad 2		800
Entidad 3		800	Entidad 4		800
Entidad 5		800	Entidad 6		800
Entidad 7		800	Entidad 8		800
Entidad 9		800	Entidad 10		780
Entidad 11		780	Entidad 12		780
Entidad 13		780	Entidad 14		780
Entidad 15		780	Entidad 16		780
Entidad 17		780	Entidad 18		780
Entidad 19		780	Entidad 20		780
Entidad 21		780	Entidad 22		780
Entidad 23		780	Entidad 24		780

	Trend	Rating
Entidad 25		780
Entidad 27		770
Entidad 29		770
Entidad 31		770
Entidad 33		770
Entidad 35		770
Entidad 37		770
Entidad 39		770
Entidad 41		760
Entidad 43		760
Entidad 45		750
Entidad 47		740
Entidad 49		730
Entidad 51		720
Entidad 53		720
Entidad 55		710
Entidad 57		710
Entidad 59		700
Entidad 61		700
Entidad 63		690

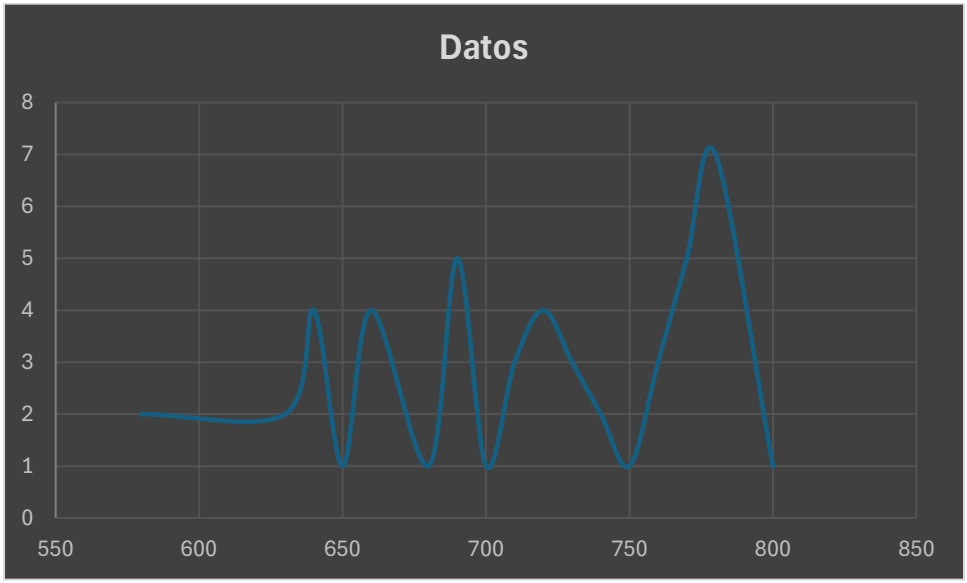
Entidad 26		770
Entidad 28		770
Entidad 30		770
Entidad 32		770
Entidad 34		770
Entidad 36		770
Entidad 38		770
Entidad 40		770
Entidad 42		760
Entidad 44		750
Entidad 46		750
Entidad 48		740
Entidad 50		720
Entidad 52		720
Entidad 54		720
Entidad 56		710
Entidad 58		700
Entidad 60		700
Entidad 62		690
Entidad 64		690

Entidad 65		690
Entidad 67		680
Entidad 69		680
Entidad 71		680
Entidad 73		680
Entidad 75		670
Entidad 77		660
Entidad 79		660
Entidad 81		650
Entidad 83		630

	Trend	Rating
Entidad 66		680
Entidad 68		680
Entidad 70		680
Entidad 72		680
Entidad 74		670
Entidad 76		670
Entidad 78		660
Entidad 80		650
Entidad 82		640

Tal y como se comentaba en líneas anteriores en las columnas de arriba se pueden apreciar los avances de los últimos días, tanto para bien como para mal de cada empresa. Desde un punto más técnico se podría averiguar qué ha ocurrido en cada una de las organizaciones para que esa puntuación haya mejorado o empeorado.

De los datos de cada una de las empresas se pueden sacar unos valores que son más representativos, como la siguiente tabla:



También se saben los siguientes datos:

- Media 738.31
- Mediana 760
- Moda 780
- Rango 220
- Desviación estándar 49.11
- Coeficiente de variación 6.65
- Cuartiles:
    - Q1: 690
    - Q2: 760
    - Q3: 780
- Percentiles:
    - 5%: 652
    - 10%: 670
    - 25%: 690

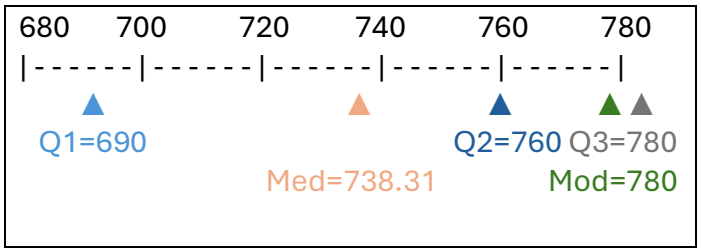
- 50%: 760
- 75%: 780
- 90%: 800
- 95%: 800

De todos estos datos se obtienen las conclusiones muy positivas, con una media de 738.31, se puede apreciar que la desviación no es muy grande, ya que pocos valores están alejados de la media y no hay ningún valor por debajo de 600 puntos. Su mediana es de 760, un valor muy representativo y hace ver la buena seguridad de las empresas del sector.

Se puede apreciar que la moda, el valor que más veces se repite, lo hace 16 veces, queda un poco por encima de la mediana, lo que indica que a pesar de que la media sea inferior, tiene muchos valores agrupados entre 770 y 800 puntos.

Los percentiles indican que el 75% de las empresas monitorizadas dan valores de 780 o superiores, un dato prometedor, aunque no lleva al éxito absoluto. Ya que 10 de las empresas están por debajo de 670, aunque ninguna en valores demasiado bajos.

El 49.11 de la desviación estándar indica una dispersión significativa, hay muchos valores agrupados alrededor del 770, pero con colas bastante grandes, sobre todo hacia la parte más baja.



¿Qué se puede hacer para mejorar el rating o la seguridad en general de una compañía? Dos pasos clave, nombrar un jefe de seguridad dentro de la empresa, es el primer paso y algo muy importante que debe suceder cuanto antes, el segundo será el de contar con alguien experto, en caso de que aquella persona que hemos nombrado no lo sea, se debería pedir ayuda fuera.

Cuando se hace referencia a mejorar el rating se habla de que la calidad de la ciberseguridad mejore con acciones que se puedan dar. Para ello, en Cybasque contamos con muchas empresas preparadas para acompañar a las entidades que necesiten mejorar sus niveles de ciberseguridad.

En Euskadi hay muchas compañías dedicadas a la ciberseguridad, muchas de ellas centradas en PYMEs, quienes tienen mucha experiencia para acompañar a quien necesitan ayuda. También hay muchas compañías en todo el territorio nacional y más por Europa. Los acuerdos de colaboración de Cybasque tanto con CyberLur, la Asociación Nacional de Empresas de Ciberseguridad, como con ECSO, la Organización Europea de Ciberseguridad, hace que el acceso a este amplio abanico de empresas especializadas está plenamente garantizado.

Las regulaciones que vienen por delante van a ser de obligatorio cumplimiento y habrá que ser conscientes de que sin implementar las exigencias que requieren, hay empresas que van a perder clientes importantes. Lo mismo que sucedía con el Esquema Nacional de Seguridad para trabajar con administraciones públicas, ahora va a ocurrir con muchas otras compañías por motivo de la NIS2.

Sabemos de sobra que el sector sanitario es siempre uno de los primeros en ser regulado y uno de los más vigilados en muchos aspectos. Es, además, un sector crítico y por lo tanto señalado en la Directiva NIS2 para cumplir con sus requisitos.

A su vez, muchos de los socios de BHC son compañías que suministran productos o servicios a entidades del sector sanitario, lo que significa que a pesar de no ser directamente de un sector crítico, sí que deberán cumplir muchos criterios de la NIS2. La cadena de suministro es uno de los puntos clave dentro de la directiva y va a ser el valor diferenciador para poder seguir con los clientes de este y otros sectores críticos.

La CRA va a obligar a quienes vendan producto electrónico a cumplir otra serie de requisitos importantes para poder tener el sello CE.

No sólo en la ciberseguridad va a haber certificaciones, en otros campos como en la IA, los datos u otras tecnologías emergentes también implementarán normativas y habrá que cumplirlas.

El informe que aquí hemos presentado es sólo una herramienta para evaluar dónde está cada empresa y hacia donde debe ir, también puede dar datos de cómo está el sector, cómo están los competidores y si cada cual debe invertir más o no en seguridad.

Conclusiones

En el sector sanitario la seguridad siempre ha sido un pilar clave, como se ve en la alta puntuación de este informe. Pero como muchos otros puntos de la tecnología, la ciberseguridad nunca está completa, nunca se puede estar ciberseguro al 100% por lo que se podría dar un paso más allá para prevenir algún ataque o imprevisto.

Desde el Gobierno Vasco, se publicó una regulación en torno a los planes de continuidad de las compañías, en materia de ciberseguridad. La ley de Autoprotección, la cual involucraba a muchos sectores que no estaban tan preparados o acostumbrados a lidiar con la ciberseguridad.

Esta ley obliga a dichas empresas a tener un plan concreto para cuando suceda un incidente y, como se comentaba en líneas más arriba, el primer paso es contar con un equipo preparado y un líder de ciberseguridad.

El siguiente punto importante para este sector será la NIS2, lo que afectará de manera directa a las empresas del clúster por ser parte de un sector crítico o con motivo de la obligatoriedad de tener controlada a la cadena de suministro. Aspecto clave en esta directiva y que hará que el espectro de la NIS2 sea más extenso que únicamente los sectores que menciona.

Por último, el sector sanitario debe cumplir con algunos valores éticos, ya que los datos que se tratan son datos muy sensibles de personas concretas, por lo que filtraciones de datos de este tipo de entidades puede afectar a toda la población y de forma directa. No sólo eso, sino que deben de tener en cuenta que su trabajo no debe poder pararse por ningún concepto, ni por ataques ni por problemas externos.

Es por ello que las entidades de este sector y sus proveedores deben tener planes de continuidad muy estructurados, deben saber qué hacer en cada situación y cuales son los protocolos a seguir para que el funcionamiento de las entidades no cese.

Para ello es clave tener una buena gestión del riesgo, a través, por ejemplo, de un SGSI (Sistema de Gestión de los Sistemas de Información), es una práctica pensada para la ISO27001 pero muy útil para otras certificaciones o normativas.

Al igual que la directiva NIS2, el ENS también exige tener una gestión controlada de los proveedores, con un inventariado completo, análisis de criticidad o planes de salida. No se trata sólo de una norma de IT, también trata de hacer test periódicos de seguridad y continuidad y en entidades críticas habría que hacer pruebas de penetración.

También se menciona, al igual que en la NIS2, la obligatoriedad de notificar los incidentes en plazos determinados, diferenciando los incidentes TIC de los de ciberseguridad.

Esta normativa es de obligado cumplimiento desde abril de 2026, a pesar de que la transposición no haya llegado por el momento.

Este tipo de informes podrán ser presentados a través de futuras colaboraciones entre BHC y Cybasque a modo de jornadas o webinars, donde poder explicar más en concreto y de la mano de expertos los requisitos que habría que cumplir para las exigencias del sector.

Este informe trata de reflejar la situación actual en Euskadi, en este caso centrándose en el sector sanitario. Pero con el claro mensaje de que para construir un entorno más seguro, es necesario la colaboración y cooperación entre todos los agentes de Euskadi.