PRIMERA EDICIÓN

Observatorio
de riesgos de ciberseguridad

- FEBRERO 2024 -

CCN-CERT centro criptológico nacional

Institut Cerdà

ÍNDICE

Índice interactivo.

05.

Los 17 Riesgos del Observatorio | 18

06.

Ciberataque al Hopital Clínic | 54

07.

Bibliografía | 66

Índice interactivo. Pincha en los asteriscos para avanzar a cada uno de los apartados. Con el asterisco siempre podrás volver al índice.

01.

Presentación del Observatorio de Riesgos de Ciberseguridad

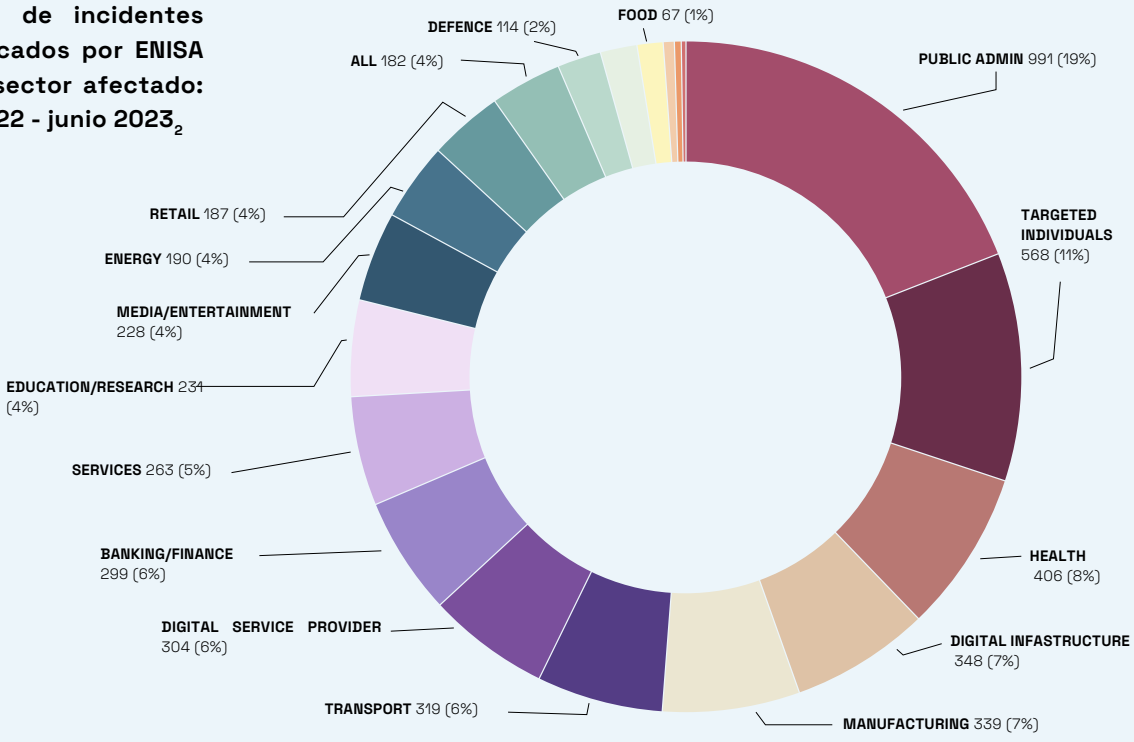
01.1. INTRODUCCIÓN

Aunque los inicios de la ciberseguridad se remontan a más de cincuenta años atrás, la proliferación de ataques con repercusión mediática la han situado, en la actualidad, en el primer plano de interés. La aceleración de la transformación digital, que penetra en todos los ámbitos de la sociedad y de la economía, comporta el incremento exponencial de las interconexiones entre equipos a escala planetaria. Esta ubicuidad propicia amplios y nuevos riesgos para la seguridad de la información y de las instalaciones que operan con medios digitales. Los avances de la inteligencia artificial se suman a la gravedad potencial de las amenazas. Por ese motivo, la ciberseguridad ha alcanzado la notoriedad y la relevancia que muestra hoy.

> **La seguridad en el ciberespacio se ha convertido en un objetivo prioritario en las agendas de los gobiernos con el fin de garantizar su seguridad nacional y de crear una sociedad digital basada en la confianza**[1]

La Agencia Europea de Ciberseguridad (ENISA) ha analizado más de 2.500 ciberataques mayores en el período que transcurre entre julio de 2022 y junio de 2023. En cuanto a los objetivos de estos ciberataques, el 19% se han dirigido contra administraciones públicas, siendo el sector que ha recibido más.

Número de incidentes identificados por ENISA según sector afectado: julio 2022 - junio 2023[2]



Por ese motivo, se ha considerado de interés presentar un Observatorio de Riesgos de la Ciberseguridad que, aun teniendo una perspectiva amplia y general, se oriente fundamentalmente hacia el sector público.

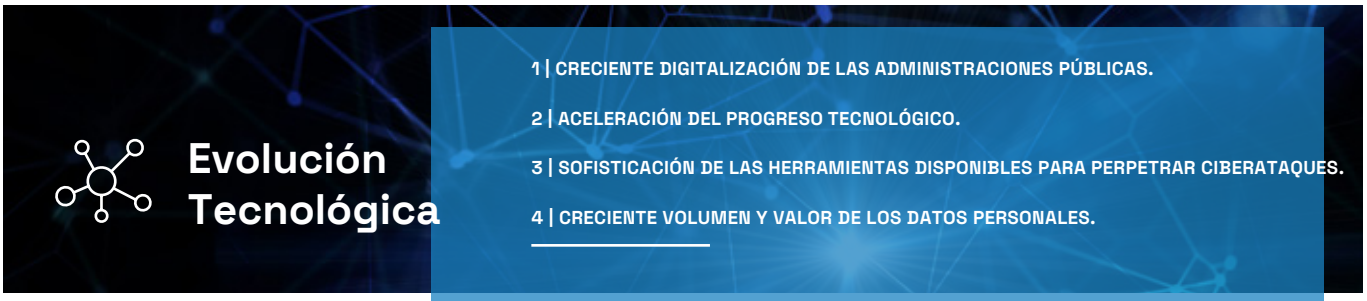
02.

Contenido del informe

02.1. LAS FICHAS DE RIESGOS

El Observatorio de Riesgos de Ciberseguridad ha sido elaborado con la colaboración del Institut Cerdà, que cuenta con la experiencia de realizar anualmente el Observatorio de Riesgos para las Empresas en España. Con una metodología y un rigor análogos, se han identificado 17 riesgos, organizados en 7 ámbitos temáticos.

El resultado es el siguiente:

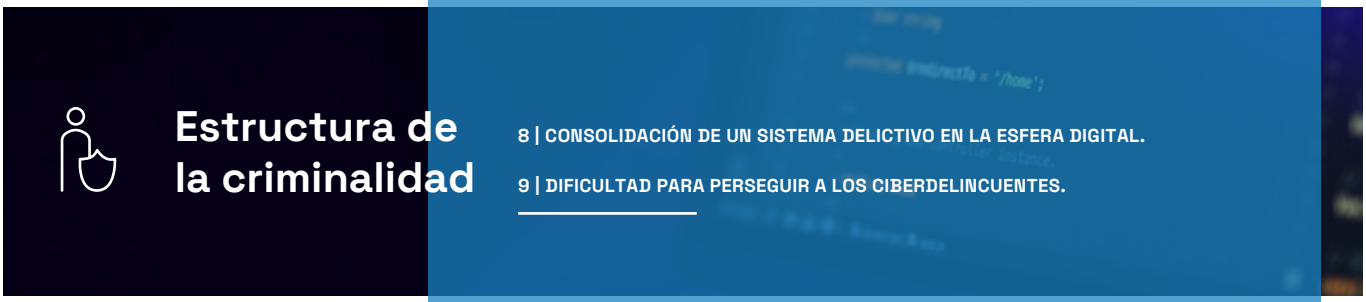


Sociopolíticos

5 | AUMENTO DE LA TENSIÓN GEOPOLÍTICA.

6 | AUMENTO DE LA POLARIZACIÓN SOCIAL.

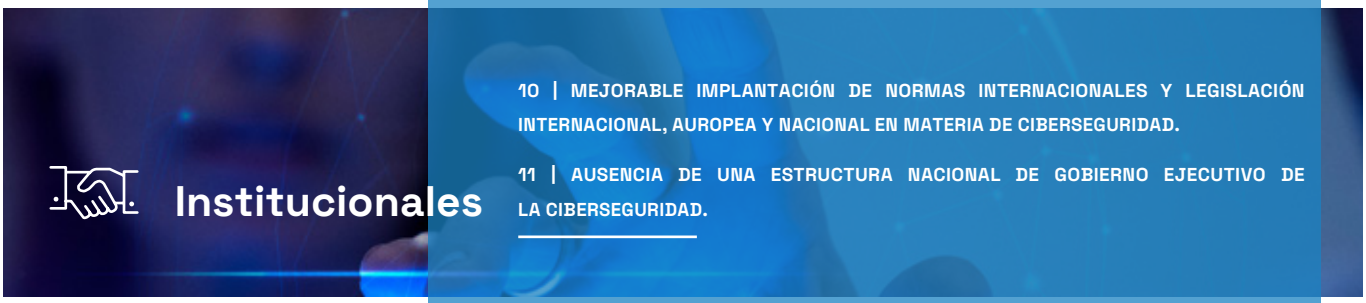
7 | AUMENTO DE LA BRECHA DIGITAL.



Estructura de la criminalidad

8 | CONSOLIDACIÓN DE UN SISTEMA DELICTIVO EN LA ESFERA DIGITAL.

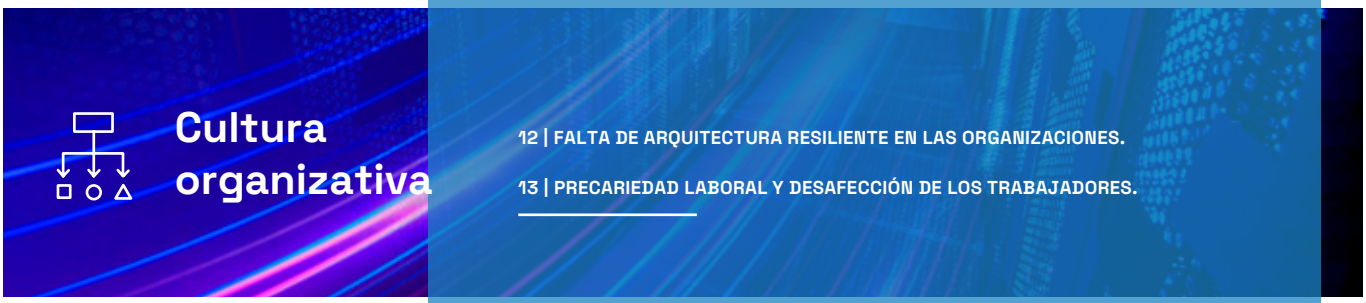
9 | DIFICULTAD PARA PERSEGUIR A LOS CIBERDELINCUENTES.



Institucionales

10 | MEJORABLE IMPLANTACIÓN DE NORMAS INTERNACIONALES Y LEGISLACIÓN INTERNACIONAL, AUROPEA Y NACIONAL EN MATERIA DE CIBERSEGURIDAD.

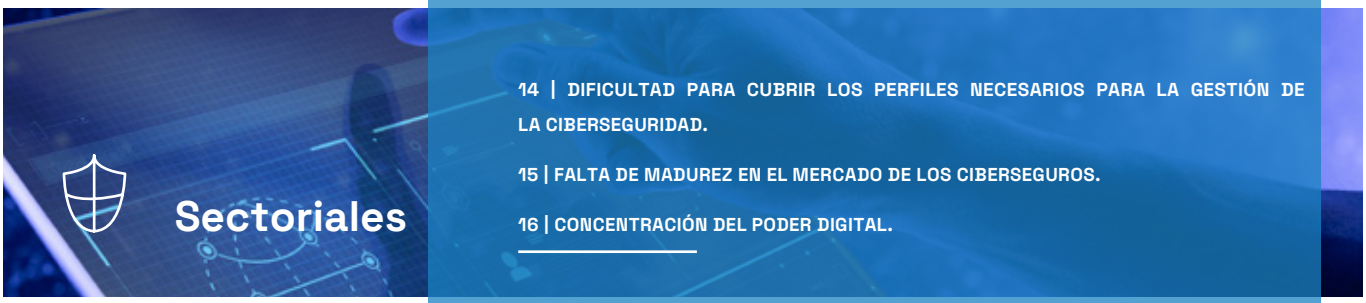
11 | AUSENCIA DE UNA ESTRUCTURA NACIONAL DE GOBIERNO EJECUTIVO DE LA CIBERSEGURIDAD.



Cultura organizativa

12 | FALTA DE ARQUITECTURA RESILIENTE EN LAS ORGANIZACIONES.

13 | PRECARIEDAD LABORAL Y DESAFECCIÓN DE LOS TRABAJADORES.



Sectoriales

14 | DIFICULTAD PARA CUBRIR LOS PERFILES NECESARIOS PARA LA GESTIÓN DE LA CIBERSEGURIDAD.

15 | FALTA DE MADUREZ EN EL MERCADO DE LOS CIBERSEGUROS.

16 | CONCENTRACIÓN DEL PODER DIGITAL.

Recursos

17 | MULTIPLICIDAD DE AGENTES EN LAS CADENAS DE SUMINISTRO.

En apartados posteriores, cada uno de estos riesgos está descrito con una ficha específica en la que se presentan las informaciones más destacadas sobre los mismos.

Todas las fichas responden a una misma estructura:

- **Clasificación**: indicación de cuál de los siete ámbitos lo engloba.
- **Enunciado del riesgo**.
- **Descripción**: breve explicación sobre qué consiste.
- **Factores clave**: reseña de los 3 o 4 elementos que determinan las causas y el alcance del riesgo.
- **Nivel**: asignación a una de las 3 categorías preestablecidas (crítico, elevado o moderado).
- **Ámbito de afectación**: vinculación al tipo de actividad implicada, mediante la valoración de si su afectación es general o interna y de si tiene una influencia alta o baja. En este sentido, se identifican cuatro ámbitos no excluyentes:
    - Acción (afectación interna e influencia alta).
    - Colaboración (afectación general e influencia alta).
    - Prevención (afectación interna e influencia baja).
    - Monitorización (afectación general e influencia baja).

02.2. EL CASO PRÁCTICO

La presentación y descripción de los riesgos se complementa con un estudio de caso: en concreto, se analiza el ciberataque padecido por el Hospital Clínic de Barcelona en marzo de 2023.

De esta manera, mediante una minuciosa descripción del suceso, se pretende ampliar el conocimiento del lector sobre el desarrollo e impacto de un ciberataque de notable repercusión, poniendo el foco en las lecciones aprendidas y en la relación con los 17 riesgos del Observatorio.

El caso se describe en base a la siguiente estructura:

1. Resumen del incidente
2. Partes involucradas
3. Descripción del suceso
   - 3.1. Desarrollo del ciberataque
   - 3.2. Articulación de la respuesta
   - 3.3. Cronología de la recuperación
4. Relación del incidente con los riesgos del Observatorio
5. Consecuentas
6. Lecciones aprendidas

03.

Metodología

El presente informe ha sido elaborado de acuerdo con el conocimiento y perspectiva del Centro Criptológico Nacional y el Institut Cerdà, junto con el análisis de informes de referencia y la contribución de expertos de diferentes sectores: Administración pública, empresa pública, empresa prestadora de servicios públicos y proveedores IT de la Administración.

En primer lugar,

se han revisado y adaptado al contexto nacional las principales publicaciones en materia de ciberseguridad, a fin de elaborar un listado preliminar de riesgos con afectación en el sector público y categorizarlos.

Posteriormente,

se ha procedido a validar este listado mediante dos sesiones de trabajo con expertos llevadas a cabo en noviembre de 2023. En estas sesiones, se valoró el nivel de criticidad de cada riesgo, se matizaron los riesgos ya identificados y se identificaron nuevos focos de riesgo, dando lugar al listado definitivo de los 17 riesgos del Observatorio.

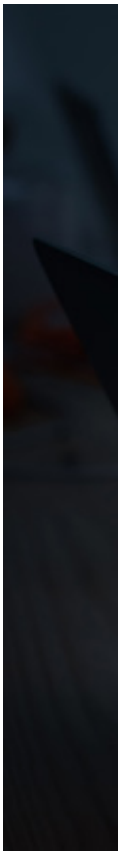
Por último,

se ha elaborado un análisis de cada uno de los riesgos del listado a fin de determinar sus causas y el alcance que tienen, así como su ámbito de afectación.

En cuanto al caso, cabe señalar que se ha elaborado en base la síntesis de la información pública disponible.

04.

Panorama de riesgos del Observatorio



A continuación, se presentan las principales ideas relativas a los citados riesgos agrupadas por cada una de las categorías. En esta exposición, el orden es temático y, por lo tanto, no indica mayor gravedad o prioridad.

Los riesgos vinculados a la evolución tecnológica

La industria digital vive en un estado de continua innovación que supone nuevos retos para la ciberseguridad. Desde este punto de vista, la evolución tecnológica genera riesgos por diversos cauces.

Por un lado, aumentan los objetivos potenciales a medida que se digitalizan las administraciones públicas y las organizaciones con las que se relacionan. Hay, pues, un número creciente de:

- Organismos, equipos y herramientas que se convierten en digitales y, en consecuencia, devienen susceptibles de ciberataques.
- Servicios a usuarios e interacciones con proveedores que se realizan a través de mecanismos digitales y, por lo tanto, pueden verse comprometidos por un ciberataque.
- Datos personales en bases de datos digitales, que pueden tener interés para fines ilícitos.

Por otro lado, los cibercriminales mejoran continuamente su capacidad para superar las protecciones e idear nuevas formas de delinquir. Para evitar las nuevas amenazas, las organizaciones deben afrontar:

- Una constante actualización de sistemas y protocolos.

- Una búsqueda permanente de nuevos puntos de vulnerabilidad.
- Un aumento de los recursos técnicos y económicos disponibles.
- La creación y el mantenimiento de una estructura de gobierno de la ciberseguridad y un marco normativo adecuado.

Finalmente, la evolución tecnológica también exige el desarrollo de nuevos marcos regulatorios, sea para fijar las reglas de la innovación -como en el caso de la inteligencia artificial-, sea para indicar los estándares de ciberprotección que deben acometerse. El retraso o la insuficiencia en la adopción de estos marcos representa, inevitablemente, otro riesgo.

Los riesgos sociopolíticos

Una parte de los ciberataques puede encuadrarse en la delincuencia común puesto que su finalidad es claramente económica (robo, extorsiones...). Otra parte, en cambio, está vinculada a motivaciones sociales o políticas y, por lo tanto, su riesgo está asociado a los vaivenes que se produzcan en estos ámbitos. En este sentido, se pueden distinguir dos grandes motores de este tipo de ataques:

- Las tensiones geopolíticas, que inducen a ciertos estados o grupos a su servicio a cometer ciberataques deliberados contra las administraciones o las infraestructuras de los países rivales.
- El activismo radical, que pretende denunciar o comprometer mediante sus ciberataques a instituciones, entidades o empresas que, según su criterio, atentan contra los valores que los activistas pretenden defender (pacifismo, ecologismo, justicia social...).

En otro orden de cosas, también debe considerarse un riesgo sociopolítico la expansión de la brecha digital por motivos sociales, económicos, territoriales... Su consecuencia es que determinados sectores tienen mayores vulnerabilidades por su dificultad para protegerse adecuadamente.

Los riesgos vinculados a la estructura de la criminalidad

La capacidad tecnológica de los ciberdelincuentes es, lógicamente, un factor crítico del alcance de sus actuaciones. Esta capacidad tecnológica abarca tanto la sofisticación de los ataques para penetrar en los objetivos que se han marcado como la habilidad para dificultar su rastreo y localización.

Aparte de la capacidad tecnológica, la estructura de este tipo de criminalidad añade riesgos que derivan de:

- La aparición de organizaciones criminales centradas en la ciberdelincuencia, incluso con especialización en distintos aspectos del delito. Se ha llegado a establecer el concepto de cibercrimen como servicio (CaaS por su sigla en inglés: Cybercrime-as-a-Service): en este caso, determinados cibercriminales prestan sus habilidades a otros delincuentes.
- Los problemas jurisdiccionales (ataques desde terceros países, protección por determinados estados...) que dificultan la eficacia de los esfuerzos policiales y judiciales en los casos concretos.

Los riesgos institucionales

Se entiende por riesgos institucionales los que derivan de las actuaciones que deben impulsar los organismos públicos, sea a escala internacional sea a escala nacional.

En la primera, la internacional, los riesgos existentes están vinculados con la inexistencia de unas bases suficientemente sólidas sobre unos estándares comunes de ciberprotección, amparados internacionalmente y, en consecuencia, exigibles en todo el mundo (por ejemplo, mediante certificaciones formales). Obviamente, en una sociedad y una economía con redes tan interconectadas, se abren puertas de vulnerabilidad allí donde estándares y exigencias sean menores.

En la segunda, la nacional, pueden originarse riesgos si los distintos organismos con responsabilidades en ciberseguridad -que han surgido respondiendo a la organización territorial de España- no establecen y facilitan espacios y mecanismos de coordinación de sus estrategias y de intercambio de información de sus experiencias.

Los riesgos de la cultura organizativa

La cultura corporativa determina cómo se comportan tanto los equipos directivos como el conjunto del personal de una organización. Emana de los hábitos que se han ido implantando a lo largo del tiempo. En este sentido, la ciberseguridad debe afrontar los riesgos de una cultura corporativa en la que no se dé la importancia necesaria a la protección y, por lo tanto, se mantengan prácticas que aumenten la vulnerabilidad ante los ciberataques.

Deben destacarse como deficiencias de una cultura corporativa apropiada para la ciberseguridad:

- Una falta de conciencia y de implicación generalizadas en toda la organización con respecto a las buenas prácticas de ciberprotección.
- La inexistencia de protocolos aptos para hacer frente a los ciberincidentes y para recuperarse de los mismos.

Estos riesgos se agravan cuando existe una elevada rotación del personal que utiliza la información sensible.

Los riesgos sectoriales

Los primeros riesgos que se han considerado son los propios del sector de la ciberseguridad en la medida que ésta es una actividad con naturaleza propia, que abarca empresas, instituciones y profesionales dedicados a desarrollar equipos y a prestar servicios para prevenir y contrarrestar la criminalidad en este ámbito.

Entre los riesgos específicos del sector, destacan dos déficits:

- La falta de personal cualificado para ocupar las plazas ofrecidas, especialmente en las administraciones y las empresas públicas. En un entorno de crecimiento del sector y, por lo tanto, de mayor demanda de profesionales, el sector público no suele contar con los mecanismos ágiles y flexibles de contratación que serían necesarios para competir adecuadamente con las ofertas del sector privado.
- Las carencias existentes en el mercado de los ciberseguros. Tratándose de un fenómeno aún poco conocido, con escasos datos históricos, surgen dificultades para establecer los perfiles de riesgo y los estándares con que fijar el alcance de las coberturas. En consecuencia, aún existen limitaciones e incertidumbres para protegerse económicamente de los ciberincidentes en general y los ciberataques en particular.

Los riesgos sectoriales

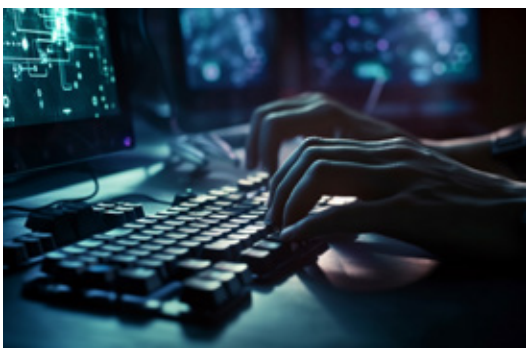
Otro riesgo sectorial es la concentración del poder digital en unos pocos gigantes tecnológicos, una situación que favorece las prácticas oligopólicas. Aunque el fenómeno percola toda la transición digital, debe atenderse también a su incidencia en la ciberseguridad. Estas grandes empresas almacenan un volumen creciente de datos sensibles de administraciones, empresas y particulares y, en consecuencia, se convierten en un objetivo apetecible de la ciberdelincuencia y pueden dejar inermes a las organizaciones que les han confiado sus datos.

Los riesgos vinculados a los recursos

Las operaciones de las administraciones, las empresas y otras entidades dependen de unas cadenas de suministro que pueden llegar a ser muy extensas e, incluso, tener alcance global. En la actualidad, estas cadenas suelen interrelacionarse mediante las redes digitales de manera que se multiplican las vulnerabilidades ante los ciberataques. Por este motivo, las organizaciones no sólo padecen los riesgos causados por los déficits de ciberprotección propios sino también por los que puedan darse en el resto de la cadena si no se establecen las medidas de contención adecuadas.

Por otro lado, aunque una organización disponga de la protección necesaria, puede verse igualmente afectada en su funcionalidad por la falta de suministros si un agente de la cadena ha visto alterada su capacidad de producción o de distribución por culpa del cibercrimen.

Así pues, la ciberseguridad en el ámbito de los recursos utilizados por una organización condiciona tanto su propia ciberseguridad como la garantía de mantener su actividad ordinaria.



La criticidad de los riesgos

Como se ha apuntado anteriormente, se ha asignado un determinado nivel de gravedad para cada uno de los riesgos. Lógicamente, los riesgos más relevantes son los que han recibido la categorización de críticos. Por su mayor importancia y porque, por esa razón, requieren más atención por parte de las organizaciones para gestionarlos, se considera de utilidad citarlos a continuación. Así pues, los riesgos detectados y calificados como críticos son los 6 siguientes:

- Dificultad para cubrir los perfiles necesarios para la gestión de la ciberseguridad.
- Concentración del poder digital.
- Escasa implementación de estándares internacionales en cuanto a ciberseguridad.
- Ausencia de una estructura nacional de gobierno ejecutivo de la ciberseguridad.
- Falta de arquitectura resiliente en las organizaciones.
- Dificultad para perseguir a los ciberdelincuentes.

Como puede constatarse, los riesgos críticos abarcan múltiples aspectos, relacionados con las capacidades de las organizaciones (cubrir los perfiles necesarios, disponer de una arquitectura resiliente), con las políticas de ciberseguridad (tener una gobernanza adecuada, implantar estándares internacionales, perseguir la delincuencia) y con la estructura económica (concentración del poder digital).

05.

Los 17 riesgos del Observatorio

CONTENIDO DEL APARTADO

A continuación, se presenta el análisis correspondiente a cada uno de los riesgos identificados por parte del Observatorio.

Tal como se indicó en la introducción, se desgranan 17 riesgos agrupados en 7 ámbitos temáticos:

- Los riesgos vinculados a la **evolución tecnológica**.
- Los riesgos **sociopolíticos**.
- Los riesgos vinculados a la **estructura de la criminalidad**.
- Los riesgos **institucionales**.
- Los riesgos de la **cultura organizativa**.
- Los riesgos **sectoriales**.
- Los riesgos vinculados a los **recursos**.

Evolución Tecnológica

1 | CRECIENTE DIGITALIZACIÓN DE LAS ADMINISTRACIONES PÚBLICAS.

2 | ACELERACIÓN DEL PROGRESO TECNOLÓGICO.

3 | SOFISTICACIÓN DE LAS HERRAMIENTAS DISPONIBLES PARA PERPETRAR CIBERATAQUES.

4 | CRECIENTE VOLUMEN Y VALOR DE LOS DATOS PERSONALES.

Sociopolíticos

5 | AUMENTO DE LA TENSIÓN GEOPOLÍTICA.

6 | AUMENTO DE LA POLARIZACIÓN SOCIAL.

7 | AUMENTO DE LA BRECHA DIGITAL.

Estructura de la criminalidad

8 | CONSOLIDACIÓN DE UN SISTEMA DELICTIVO EN LA ESFERA DIGITAL.

9 | DIFICULTAD PARA PERSEGUIR A LOS CIBERDELINCUENTES.

Institucionales

10 | MEJORABLE IMPLANTACIÓN DE NORMAS INTERNACIONALES Y LEGISLACIÓN INTERNACIONAL, AUROPEA Y NACIONAL EN MATERIA DE CIBERSEGURIDAD.

11 | AUSENCIA DE UNA ESTRUCTURA NACIONAL DE GOBIERNO EJECUTIVO DE LA CIBERSEGURIDAD.

Cultura organizativa

12 | FALTA DE ARQUITECTURA RESILIENTE EN LAS ORGANIZACIONES.

13 | PRECARIEDAD LABORAL Y DESAFECCIÓN DE LOS TRABAJADORES.

Sectoriales

14 | DIFICULTAD PARA CUBRIR LOS PERFILES NECESARIOS PARA LA GESTIÓN DE LA CIBERSEGURIDAD.

15 | FALTA DE MADUREZ EN EL MERCADO DE LOS CIBERSEGUROS.

16 | CONCENTRACIÓN DEL PODER DIGITAL.

Recursos

17 | MULTIPLICIDAD DE AGENTES EN LAS CADENAS DE SUMINISTRO.

Pincha en los números de los apartados para avanzar a cada uno de los riesgos del Observatorio que quieras ver.

Evolución Tecnológica

Creciente digitalización de las administraciones públicas

DESCRIPCIÓN

La transformación digital, liderada por órganos como la Secretaria General de Administración Digital, se ha consolidado como uno de los principales pilares en cuanto a la gestión y prestación de servicios por parte de Administraciones. Si bien esta digitalización ha permitido mejorar la eficiencia y el nivel de servicio, también ha multiplicado los puntos de entrada de ciberataques y la dependencia respecto a los sistemas y herramientas digitales.

1

22,6%

Del PIB español corresponde a la economía digitalizada (toda actividad económica basada en bienes y servicios digitales)[1]

68%

Población internauta española que realizó gestiones y trámites de la Administración pública de manera telemática en 2021[2]

97%

Organizaciones españolas que utilizan herramientas y entornos cloud[3]

FACTORES CLAVE

Entre los diversos elementos que condicionan la creciente digitalización de la economía, destacan los siguientes:

1 | Mayor riesgo de paralizar la actividad debido a ciberataques en activos clave de las organizaciones

La digitalización recae sobre activos (físicos y digitales) que se tornan imprescindibles para el funcionamiento interno y la prestación de un creciente número de servicios. De esta manera, se abre la posibilidad a la generación de vulnerabilidades digitales que, explotadas en ciberataques, pueden distorsionar la actividad de las organizaciones y la provisión de servicios públicos esenciales.

2 | Mayor número de equipos informáticos, entornos cloud y sistemas IoT susceptibles de ser atacados

El crecimiento en el número de sistemas TI interconectados es un factor de riesgo con doble afectación. Por un lado, supone un incremento en los posibles puntos de entrada de ciberataques. Por otro, aumenta el nivel de complejidad de los sistemas informáticos, incrementando los recursos necesarios para garantizar su protección.

3 | Mayor dependencia de herramientas digitales para la prestación de servicios, propias o de proveedores

La creciente digitalización de la economía no solo incide en la vulnerabilidad frente a ciberataques. La interrupción en el servicio de proveedores TI clave o fallas en los programas informáticos esenciales empleados por la Administración pone de manifiesto la importancia de gestionar la ciberseguridad a lo largo de toda la cadena de proveedores y clientes.

NIVEL DE RIESGO
Crítico
Elevado
Moderado

PINCHA AQUÍ PARA VOLVER AL APARTADO 05.

Evolución Tecnológica

Aceleración del proceso tecnológico

DESCRIPCIÓN

El progreso tecnológico supone una oportunidad para mejorar la operativa y servicios ofrecidos por todas las administraciones, sin embargo, a su vez, comporta nuevas vulnerabilidades y la necesidad de actualizar y reforzar la ciberseguridad (sistemas, protocolos, normativa, etc.) en torno tanto de la gestión de datos como de la de activos públicos críticos para la población. En este sentido, cabe incidir en la mayor exposición de aquellas administraciones con menores recursos.

2

>3 años

Tiempo transcurrido desde la presentación de la Ley de Inteligencia Artificial de la U.E (EU AI Act) en abril de 2021, sin que se haya aprobado formalmente

11ª posición

De España en el índice europeo de madurez digital del sector público, situándose por encima de la media [1]

8 horas

Tiempo que podría tardar un ordenador cuántico en descifrar los sistemas de encriptación más comunes en la actualidad [2]

FACTORES CLAVE

Entre los diversos elementos que cabe tener en cuenta de la aceleración del progreso tecnológico, destacan los siguientes:

1 | Necesidad de actualización permanente de sistemas y protocolos

Una de las principales vías de acceso ilícito en ciberataques es la explotación de vulnerabilidades de software en los activos tecnológicos a disposición de la Administración. Por ello, la constante incorporación e integración de nuevos productos, servicios y tecnologías comporta la necesidad de actualizar regularmente sus sistemas y protocolos de seguridad.

2 | Surgimiento de nuevos puntos de vulnerabilidad y amenazas como, por ej., la IA

El surgimiento de nuevas tecnologías pone a disposición de los cibercriminales nuevas herramientas para comprometer la seguridad de las organizaciones. A modo de ejemplo, destaca el potencial de la IA para la suplantación de identidades y la redacción de correos de phishing.

3 | Desequilibrio entre la adaptación de la normativa y la aceleración tecnológica

El marco regulatorio no tiene la capacidad de seguir el ritmo del progreso tecnológico, existiendo un retraso entre la aparición y desarrollo de nuevas tecnologías y la implementación de las normativas requeridas para minimizar los riesgos existentes.

NIVEL DE RIESGO

Crítico

Elevado

Moderado

PINCHA AQUÍ PARA VOLVER AL APARTADO 05.

Evolución Tecnológica

Sofisticación de las herramientas disponibles para perpetrar ciberataques

DESCRIPCIÓN

El incremento de las capacidades tecnológicas es empleado por parte de las ciberamenazas para incrementar el número y complejidad de los ciberataques, comprometiendo la seguridad de las organizaciones y, en especial, aquellas con sistemas y estrategias menos actualizados.

3

x2

Aumento de la velocidad de las Unidades Centrales de Procesamiento (CPU) entre 2010 y 2022 [1]

81%

De los directivos considera insostenible el coste en ciberseguridad para mantenerse por delante de los cibercriminales [2]

+135%

Crecimiento de los ataques que emplean técnicas de ingeniería social desde finales de 2022 [3]

FACTORES CLAVE

Entre los diversos elementos que condicionan los potenciales efectos derivados de la sofisticación de las herramientas disponibles para perpetrar ciberataques, destacan los siguientes:

1 | Necesidades de inversión y partidas específicas para ciberseguridad

Entidades como el Consejo Europeo alertan que el cibercrimen es cada año más sofisticado y complejo. En este escenario, por las tecnologías de ciberseguridad se han posicionado, con el 70%, como la principal prioridad de inversión parte de los CIO (Chief Information Officer) de las organizaciones europeas (ENISA, 20234), destacando además que ninguna organización prevé disminuir su gasto en ciberseguridad.

2 | Mayor facilidad para realizar ataques de "ingeniería social"

Las crecientes capacidades de las herramientas digitales son empleadas para incrementar el número y la sofisticación de los ataques de "ingeniería social", es decir, aquellas actividades que, mediante la manipulación y el engaño, intentan provocar un error humano o explotar comportamientos para conseguir acceder a información secreta o sensible, y cuyos ejemplos más representativos son el phishing o el baiting.

3 | Personalización sofisticada de las herramientas para perpetrar ciberataques

El acceso a un creciente volumen de información, junto con las herramientas disponibles, permite incrementar el grado de personalización en el diseño de los ciberataques, aumentando su probabilidad de éxito al adaptarse a las características de cada persona u organización.

NIVEL DE RIESGO

Crítico

Elevado

Moderado

PINCHA AQUÍ PARA VOLVER AL APARTADO 05.

Evolución Tecnológica

Creciente volumen y valor de los datos personales

DESCRIPCIÓN

Los sistemas TI de empresas y Administraciones almacenan datos personales sensibles como contraseñas, información sanitaria o datos fiscales. El creciente valor de estos datos ha posicionado a individuos y organizaciones como objetivos prioritarios para las ciberamenazas, que venden los datos robados o amenazan con publicarlos abiertamente como medida de extorsión. En paralelo a la preocupación que suscita esta amenaza se ha aprobado nueva normativa para la protección de datos (como el Reglamento General de Protección de Datos de la UE, traspuesto en España con la LOPDGDD 3/2018, que dedica su Disposición adicional primera a la aplicación del ENS).

4

425 millones

Personas afectadas por filtraciones de datos en 2022 [1]

+95%

Crecimiento de los ciberataques a Administraciones públicas y entidades gubernamentales en 2022 [2]

65%

De la población mundial tendrá sus datos personales protegidos bajo regulaciones de privacidad de reciente creación [3]

FACTORES CLAVE

Entre los diversos elementos que condicionan el creciente volumen y valor de los datos personales, destacan los siguientes:

1 | Creciente interés por atacar a las entidades que almacenan o gestionan datos personales

El sector público y su red de proveedores almacenan información sensible como, por ejemplo, datos fiscales y sanitarios, siendo por ello los principales afectados por ciberataques con diversos objetivos, desde el cibercrimen al ciberespionaje. Así, entre 2022 y 2023 el 27% de los ciberincidentes analizados por la Agencia de la Unión Europea para la Ciberseguridad (ENISA[4]) se concentraron en la Administración pública y el sector sanitario.

2 | Foco en el espionaje a personal de las organizaciones

El espionaje y ciberataque a nivel individual supone una vía alternativa que los actores de ciberamenaza emplean para comprometer a las organizaciones, ya sea a través de la exposición de información sensible o mediante el robo de credenciales. Cabe destacar que, dado que las Administraciones y entidades públicas emplean a más de 2,7 millones de personas en España, los ciberataques a individuos son un extenso vector de exposición.

3 | Dificultad de adaptación a la regulación en materia de protección de datos

El cumplimiento de la regulación en materia de protección de datos requiere recursos y conocimientos con los que no cuentan todas las organizaciones. De esta manera, el riesgo de incumplimiento de normativas como la Ley Orgánica de Protección de Datos Personales (LOPD) puede conllevar el descrédito de las organizaciones infractoras y multas de hasta 20 millones de €.

NIVEL DE RIESGO

Crítico

Elevado

Moderado

PINCHA AQUÍ PARA VOLVER AL APARTADO 05.

Sociopolíticos

Aumento de la tensión geopolítica

DESCRIPCIÓN

La tensión geopolítica incide de forma directa sobre las cadenas de suministro del sector tecnológico y en la implementación de distintas formas de ciberamenaza como instrumentos al servicio de Estados y actores no-estatales con intereses geopolíticos. Así, las organizaciones que desempeñan funciones críticas ven incrementada la incidencia de los ciberataques promovidos desde estados enfrentados.

5

+140%

Crecimiento de ciberataques contra infraestructuras industriales críticas en 2022 [1]

+300%

Crecieron los ciberataques a países de la OTAN desde el comienzo de la guerra de Ucrania [2]

80%

De los ciberataques perpetrados por estados nación tienen como objetivo agencias gubernamentales, think tanks y ONG [3]

FACTORES CLAVE

Entre los diversos elementos que condicionan el aumento de la tensión geopolítica, destacan los siguientes:

1 | Promoción de actores avanzados de ciberamenaza por parte de Estados y organizaciones terroristas

Algunos Estados y actores adversarios no-estatales promueven de forma directa la actividad de ciberamenazas en el desarrollo de ciberataques contra países en escenarios geopolíticos de interés para esos Estados promotores. Las infraestructuras críticas, las empresas estratégicas y las Administraciones Públicas se posicionan como un objetivo preferente para estas ciberamenazas. Así, ENISA estima que entre 2022 y 2023 el 25% de los ciberincidentes tuvieron motivaciones geopolíticas, siendo los ataques de denegación de servicio (DDoS) la principal herramienta empleada.

2 | Afectación de los conflictos políticos a las cadenas de suministro

Los conflictos geopolíticos influyen en aspectos como el precio de las materias primas, el comercio internacional y las rutas de transporte, generando distorsiones en las cadenas de suministro de tecnologías clave para garantizar la ciberseguridad. A título de ejemplo, destaca la incidencia de las tensiones entre China y EE.UU sobre el mercado de los semiconductores y telecomunicaciones.

NIVEL DE RIESGO

Crítico

Elevado

Moderado

PINCHA AQUÍ PARA VOLVER AL APARTADO 05.

Sociopolíticos

Aumento de la polarización social

DESCRIPCIÓN

La polarización social incide y, al mismo tiempo, se ve acrecentada por las campañas de desinformación, una táctica de desestabilización que tiene por objetivo Administraciones, empresas e individuos particulares. En este contexto, la injerencia de los gobiernos extranjeros y de un "hacktivismo híbrido" al servicio de esos gobiernos, tanto mediante operaciones de desinformación como de desestabilización, se posicionan como un riesgo para la reputación y ciberseguridad de las organizaciones.

6

86%

Personas con acceso a internet de todo el mundo han estado expuestas a fake news [1]

3.º

Puesto de España en un ranking que mide el incremento de la polarización social en 40 países entre 2011 y 2021 [2]

82%

De los españoles considera la desinformación un problema de gran envergadura para el país y la democracia [3]

FACTORES CLAVE

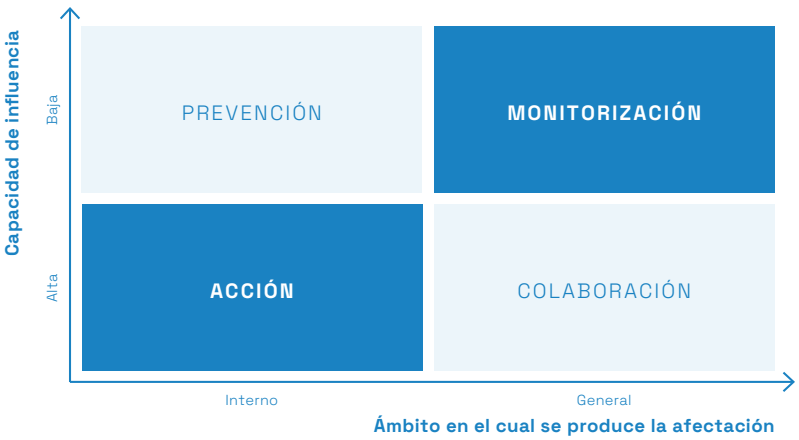
Entre los diversos elementos que condicionan el aumento de la polarización social, destacan los siguientes:

1 | Potencial lesivo de las campañas de desinformación, acrecentadas por el crecimiento de la IA y la injerencia extranjera

Las noticias falsas se difunden hasta 6 veces más rápido que las reales (MIT4), lo que confiere a las campañas de desinformación de contenidos y por medios digitales la capacidad de perjudicar la reputación de las organizaciones y causar ciberincidentes en un corto periodo de tiempo. En este sentido, destaca el potencial de la IA para generar contenido cada vez más verosímil, así como el peso de la injerencia extranjera en las campañas de desinformación.

2 | Incremento del "hacktivismo híbrido" debido al servicio de intereses geopolíticos

ENISA estima que en torno al 4% de los ciberincidentes tienen detrás una motivación ideológica5. Así, la transcendencia social de empresas y Administraciones se posiciona como un elemento que incide en la vulnerabilidad frente a ciberataques por parte de actores de ciberamenaza que actúan con una máscara de motivación ideológica de falso hacktivismo (hacktivismo híbrido) que, en realidad, oculta el servicio a intereses geopolíticos Estatales. En 2023 el 66% de los ataques por denegación de servicio (DoS por sus siglas en inglés) se reivindicaron bajo narrativas que pretendían motivaciones políticas y activistas.



NIVEL DE RIESGO
Crítico
Elevado
Moderado

PINCHA AQUÍ PARA VOLVER AL APARTADO 05.

Sociopolíticos

Aumento de la brecha digital

DESCRIPCIÓN

La existencia de brechas digitales merma los recursos disponibles, tanto económicos como de recursos humanos, de algunas organizaciones y condiciona la gestión del personal. A nivel territorial, la desigualdad en el acceso a los recursos TI se manifiesta mediante diferencias en aspectos como las infraestructuras y el talento disponible en el medio rural y el urbano. A nivel social, esta brecha se aprecia en el nivel de competencias digitales y acceso a la tecnología de determinados colectivos.

7

36%

De la población española no cuenta con competencias digitales básicas [1]

20%

De diferencia en la adquisición de competencias digitales básicas entre las personas de 16-24 y las de más de 45 años [2]

72%

Cobertura de la fibra óptica en los hogares rurales en junio de 2022 [3]

FACTORES CLAVE

Entre los diversos elementos que condicionan el aumento de la brecha digital, destacan los siguientes:

1 | Existencia de segmentos poblacionales con dificultades para aplicar las medidas básicas de ciberseguridad

Segmentos poblacionales, como las personas en edad avanzada o en situación de vulnerabilidad socioeconómica, presentan menores niveles de competencias digitales. De esta manera, una parte de la fuerza laboral y de los usuarios de los servicios públicos no disponen de las competencias digitales básicas para implementar buenas prácticas en materia de ciberseguridad.

2 | Desigual disponibilidad de recursos TI en el medio rural y urbano

Las Administraciones y servicios públicos ubicados en el medio rural se encuentran en una situación de desigualdad respecto a las zonas urbanas en cuanto la disponibilidad de los recursos necesarios para garantizar la ciberseguridad. Por un lado, se enfrentan a mayores retos para atraer talento digital desde los núcleos urbanos. Por otro, a nivel de infraestructuras, existen brechas de hasta el 25% en aspectos como la cobertura de banda ancha ultrarrápida (MINECO, 2022[4]).

NIVEL DE RIESGO

Crítico

Elevado

Moderado

PINCHA AQUÍ PARA VOLVER AL APARTADO 05.

Estructura criminalidad

Consolidación de un sistema delictivo en la esfera digital

DESCRIPCIÓN

El cibercrimen se ha consolidado como un negocio en expansión. La sofisticación de la estructura de estas organizaciones criminales y los métodos que emplean han reforzado su influencia y capacidades, pudiendo poner en riesgo a organizaciones que, anteriormente, estaban fuera de su alcance.

8

8 Billones de $

Coste anual del cibercrimen en todo el mundo, que ascenderá hasta los 10,5 billones de dólares en 2025 [1]

38%

Incremento del "Cybercrime-as-a-service" dirigido a emails corporativos entre 2019 y 2022 [2]

1,6 Billones de $

Valor económico del sector del "Cybercrime-as-a-Service" en todo el mundo en 2020 [3]

FACTORES CLAVE

Entre los diversos elementos que condicionan la consolidación de un sistema delictivo en la esfera digital, destacan los siguientes:

1 | Aumento en el número y profesionalización de las organizaciones cibercriminales

Los ciberdelincuentes emplean redes de lavado de dinero cada vez más complejas, herramientas de phishing más verosímiles y softwares con mayor capacidad para penetrar en los sistemas de las víctimas (EUROPOL, 20214). En este contexto, las empresas y Administraciones que no han incrementado su nivel de protección al ritmo de evolución del cibercrimen presentan mayores niveles de vulnerabilidad.

2 | Incremento del "Cybercrime-as-a-Service"

El afianzamiento del cibercrimen como servicio posibilita que actores sin conocimientos en este ámbito puedan realizar ciberataques a través del uso de software de terceros y la contratación externa de grupos especializados. Así, entidades como el MIT[5] señalan que la facilidad de contratar estos servicios elimina barreras que anteriormente marcaban un freno a la expansión del cibercrimen.

Igualmente, diversos estudios recogidos por ENISA entre 2022 y 2023 destacan que en la dark web pueden adquirirse paquetes para ejecutar ataques de phishing por tan solo 40 euros[6].

NIVEL DE RIESGO

Crítico

Elevado

Moderado

PINCHA AQUÍ PARA VOLVER AL APARTADO 05.

Estructura criminalidad

Dificultad para perseguir a los ciberdelincuentes

DESCRIPCIÓN

El cibercrimen se lleva a cabo de manera anónima y deslocalizada, lo que dificulta rastrear a los perpetradores e iniciar causas judiciales. A este factor, cabe sumar el hecho de que no todas las jurisdicciones colaboran para la persecución de cibercriminales y, en algunos casos, estos son amparados por los estados desde donde operan.

9

0,3%

Denuncias por delitos de cibercrimen son procesadas y se aplican a los ciberatacantes [1]

15%

Denuncias por cibercrimen esclarecidas en España en 2022 (aquellas en las que se identifica al autor o se determina que no hay una infracción) [2]

54,5%

De los ciberataques detectados en la U.E fueron perpetrados por autores desconocidos [3]

FACTORES CLAVE

Entre los diversos elementos que condicionan la dificultad para perseguir a los ciberdelincuentes, destacan los siguientes:

1 | Protección de grupos cibercriminales por parte de determinados estados

Algunos estados, como Rusia o China, han sido acusados por el gobierno de EE.UU de proteger a los cibercriminales que actúan sobre terceros países. De este modo, se obstaculiza llevar a cabo acciones judiciales contra determinados grupos criminales, favoreciendo que operen sin limitaciones.

2 | Existencia de conflictos jurisdiccionales

El limitado alcance de las jurisdicciones nacionales dificulta aplicar la ley a aquellos criminales que realizan ciberataques desde terceros países. Si bien existen tratados de cooperación internacional como el Convenio de Budapest, este ha sido adoptado por 69 países, quedando fuera la mayor parte de países de Asia y África.

3 | Anonimato y dificultad de rastreo de los ciberdelincuentes

Los cibercriminales emplean herramientas como el cifrado de datos, las redes privadas virtuales (VPN) o direcciones IP dinámicas para operar de forma anónima. La dificultad para salvar estas barreras por parte de los instrumentos de persecución penal actúa como un mecanismo de protección que permite a los criminales ejercer su actividad al margen de la ley.

NIVEL DE RIESGO

Crítico

Elevado

Moderado

PINCHA AQUÍ PARA VOLVER AL APARTADO 05.

Institucionales

Mejorable implantación de normas internacionales y legislación internacional, europea y nacional en materia de ciberseguridad

DESCRIPCIÓN

Los avances en el ámbito digital no se han visto correspondidos por la materialización de acuerdos internacionales que unifiquen criterios y recomendaciones bajo un marco regulatorio común a escala global. Iniciativas como el ENS suelen basarse en un enfoque nacional. Ante esta falta de homogeneidad normativa e interoperabilidad, es habitual encontrar distorsiones que dificultan operar con garantías en ciberseguridad.

10

28%

De las entidades certificadas en el Esquema Nacional de Seguridad son organismos del sector público [1]

54%

Empresas de dispositivos médicos consideran que no cumplen con las regulaciones y estándares de ciberseguridad [2]

66%

De las empresas prevén que su gasto en ciberseguridad estará impulsado por mandatos legales [3]

FACTORES CLAVE

Entre los diversos elementos que condicionan la escasa implementación de estándares internacionales en cuanto a ciberseguridad, destacan los siguientes:

1 | Proliferación de legislación y normativa sin una base común a escala global

El sector digital se caracteriza por su dimensión global, sin embargo, la legislación que se ocupa de la ciberseguridad suele tener una base nacional o europea, produciendo disparidades entre países. En consecuencia, dificulta garantizar la seguridad en entornos internacionales, siendo necesario llevar a cabo un sobreesfuerzo para operar bajo legislaciones extranjeras y en las relaciones con proveedores de terceros países. La normativa europea, como las recientes directivas NIS 2 o la Cyber Resilience Act, supone uno de los pocos ejemplos de gobernanza regional en materia de ciberseguridad.

2 | Ausencia de cooperación internacional para supervisar estándares y facilitar su interoperabilidad

Los estándares de ciberseguridad no cuentan con instituciones internacionales que supervisen su cumplimiento y encaje con las normativas nacionales y regionales. Así, obstaculiza su implementación e interoperabilidad y, por tanto, su uso armonizado.

3 | Falta de un marco público-privado que fomente la adhesión a normas técnicas comunes

Más allá de la ISO 27000, no existe un marco centralizado global que se encargue de la gestión de la ciberseguridad. Además, la adhesión a normas técnicas comunes es principalmente voluntaria e individual, sin un plan agregado que aporte beneficios por su incorporación, por ejemplo, en los contratos públicos, dificultando así su generalización tanto en el sector público como el privado.

NIVEL DE RIESGO

Crítico

Elevado

Moderado

PINCHA AQUÍ PARA VOLVER AL APARTADO 05.

Institucionales

Ausencia de una estructura nacional de gobierno ejecutivo de la ciberseguridad

DESCRIPCIÓN

Si bien a nivel nacional se dispone de órganos consultivos como el Consejo Nacional de Seguridad, no existe una agencia central de ciberseguridad con funciones ejecutivas que englobe todos los ámbitos de la ciberseguridad. Así, el país carece de un organismo que vele por la armonización de estrategias y normativas.

11

>10

Agencias públicas de ciberseguridad operando en España

2022

Puesta en marcha de la primera Red Nacional de Centros de Operaciones de Ciberseguridad

100%

Principales economías de la UE (a excepción de España) que disponen de una agencia horizontal de ciberseguridad con funciones ejecutivas [1]

FACTORES CLAVE

Entre los diversos elementos que condicionan la ausencia de una política nacional de gobernanza de la ciberseguridad, destacan los siguientes:

1 | Heterogeneidad sectorial y territorial de los servicios públicos

La heterogeneidad de sectores, alcance territorial y tamaño de las Administraciones y entidades públicas, ya sean de ámbito estatal, autonómico o local, deriva en un amplio abanico de necesidades específicas. A título de ejemplo, servicios públicos, como la salud, la educación o el transporte, requieren aproximaciones y políticas adaptadas a sus requerimientos. Igualmente, las características poblacionales, topográficas o económicas de las administraciones locales no tan solo afectan al tipo de ataque que pueden recibir sino también a los recursos técnicos y humanos disponibles.

2 | Distribución de las competencias en materia de ciberseguridad en diversas autoridades

En España existen más de 10 agencias y organizaciones públicas que se ocupan de la ciberseguridad, repartidas entre los 3 niveles territoriales de la administración. En un contexto en el que no existe una agencia central de ciberseguridad, esta fragmentación dificulta establecer mecanismos sólidos de coordinación e intercambio de información entre los distintos organismos.

NIVEL DE RIESGO

Crítico

Elevado

Moderado

PINCHA AQUÍ PARA VOLVER AL APARTADO 05.

Cultura organizativa

Falta de arquitectura resiliente en las organizaciones

DESCRIPCIÓN

Una estructura organizativa resiliente frente a las ciberamenazas no solo requiere de herramientas, recursos y personal cualificado, también necesita establecer estrategias eficaces de prevención, detección y recuperación. La falta de arquitectura resiliente en las organizaciones puede derivar en un mayor riesgo de sufrir ciberataques, desde la prevención a la respuesta, pasando por la fase crítica de detección.

12

86%

Organizaciones españolas que carecían de una cultura de ciberseguridad entre los empleados en 2021 [1]

27%

Trabajadores públicos de un municipio de más de 200.000 habitantes facilitaron sus claves en un simulacro de phishing en 2022 [2]

96%

De los CISOs afirman necesitar mejores soluciones para que sus organizaciones sean más ciberresilientes [3]

FACTORES CLAVE

Entre los diversos elementos que condicionan la falta de una arquitectura resiliente en las organizaciones, destacan los siguientes:

1 | Vulnerabilidad potencial de activos críticos a través de ciberataques

Las Administraciones públicas y las empresas estratégicas o que gestionan activos críticos actúan tanto mediante infraestructuras físicas como con sistemas digitales, con lo que las estrategias de resiliencia integran activos críticos con interrelaciones complejas. En este contexto, cabe tener presente que la dispersión territorial, tanto de infraestructuras críticas como de servicios públicos, añade dificultad y, por tanto, una dimensión de vulnerabilidad a la implantación de estrategias armonizadas de resiliencia.

2 | Falta de concienciación y conocimientos en materia de ciberseguridad

La difusión interna de una cultura de la ciberseguridad, la interiorización de buenas prácticas digitales y una formación básica son tres dimensiones indispensables para la confección de una estructura resiliente frente a los ciberincidentes. Sin embargo, no todas las organizaciones cuentan con la concienciación y conocimientos suficientes en todas sus capas, creando eslabones internos y externos "vulnerables" que comprometen la ciberseguridad.

3 | Falta de medidas y protocolos necesarios para prevenir, detectar y recuperarse de un ciberincidente

Si bien la prevención es fundamental, también es imprescindible que las organizaciones dispongan de protocolos para detectar y responder frente a ciberincidentes, no solo desde el punto de vista TI sino también a nivel de operaciones (como Disaster Recovery Plans o planes de continuidad de negocio) y comunicación. Asimismo, la falta de mecanismos consolidados para compartir lecciones aprendidas puede mermar su resiliencia.

NIVEL DE RIESGO

Crítico

Elevado

Moderado

PINCHA AQUÍ PARA VOLVER AL APARTADO 05.

Cultura organizativa

Precariedad laboral y desafección de los trabajadores

DESCRIPCIÓN

La desafección de los trabajadores, condicionada por la precariedad y la rotación laboral, es un elemento que merma la configuración estable de plantillas formadas, clave para reforzar la experiencia, el conocimiento, la cultura y el aprendizaje en torno a la ciberseguridad. Más si se tiene en cuenta que las organizaciones no son elementos aislados, sino que forman parte de ecosistemas complejos que abarcan proveedores, clientes o la ciudadanía, entre otros.

13

93%

Organizaciones de todo el mundo admiten que les resulta difícil ejecutar tareas esenciales de ciberseguridad [1]

29%

Empresas españolas con una rotación de personal superior al 20% en los equipos de ciberseguridad, según Observaciber [2]

30%

Tasa de temporalidad en el sector público durante el tercer trimestre de 2023 [3]

FACTORES CLAVE

Entre los diversos elementos que condicionan la precariedad laboral y desafección de los trabajadores, destacan los siguientes:

1 | Implicación de los trabajadores a la hora de aplicar buenas prácticas

El Foro Económico Mundial estima que el 95% de los ciberincidentes son causados por el error humano4. En este contexto, contar con una plantilla comprometida facilita implementar medidas de seguridad y evitar que existan eslabones "débiles" que puedan comprometer a la organización. No obstante, factores como la precariedad laboral y la desafección de los trabajadores respecto a sus organizaciones merma este compromiso.

2 | Elevada rotación de trabajadores que manejan información sensible y sistemas críticos

El Observaciber (formado por el INCIBE y el ONTSI) indica que el 50% de las empresas tiene una rotación laboral superior al 10% en los equipos de ciberseguridad5, dificultando garantizar la estabilidad de perfiles que manejan información sensible y sistemas críticos. Si bien en el sector público el personal funcionario es de carácter estable, cabe tener en cuenta que el personal laboral y la plantilla de las empresas que le prestan servicio puede verse afectada por este nivel de rotación.

NIVEL DE RIESGO

Crítico

Elevado

Moderado

PINCHA AQUÍ PARA VOLVER AL APARTADO 05.

Sectoriales

Dificultad para cubrir los perfiles necesarios para la gestión de la ciberseguridad

DESCRIPCIÓN

Contar con personal cualificado es imprescindible para garantizar la ciberseguridad. Sin embargo, las administraciones y empresas públicas se enfrentan a dificultades para atraer y retener expertos en ciberseguridad, mermando, por tanto, su capacidad de prevención, detección y respuesta frente a ciberamenazas.

14

30.000

Vacantes en ciberseguridad sin cubrir en España [1]

93%

Empresas sin un plan de promoción específico para el talento en ciberseguridad [2]

17%

Organizaciones españolas con un especialista TIC en plantilla [3]

FACTORES CLAVE

Entre los diversos elementos que condicionan la provisión de los perfiles necesarios para garantizar la ciberseguridad, destacan los siguientes:

1 | Ventaja competitiva de las multinacionales para atraer y retener talento en un mercado globalizado

La naturaleza deslocalizada del sector digital permite a los expertos en ciberseguridad trabajar de forma remota para cualquier compañía, independientemente de su localización. En un sector caracterizado por el cambio constante, la atracción y retención de talento resulta más sencilla para las empresas multinacionales debido a su capacidad para pagar mayores salarios y la capacidad de atracción que ejercen por su rol en la evolución del sector.

2 | Rigidez de la Administración a la hora de remunerar y ofrecer planes de carrera atractivos

En lo que a personal funcionario se refiere, el sistema de contratación, remuneración y promoción en la Administración se rige por el Estatuto Básico del Empleado Público. Este sistema articula las necesidades de perfiles profesionales tecnológicos para la base funcionarial de la Administración a largo plazo, pero es poco ágil para responder a la movilidad, diversidad y la naturaleza rápidamente cambiante del sector de la ciberseguridad, que requiere de un marco profesional más dinámico que deja a las Administraciones en desventaja en el mercado laboral de la ciberseguridad.

3 | Divergencia entre las demandas de las organizaciones y la oferta del sistema formativo

El Instituto Nacional de Ciberseguridad (INCIBE) señala que el sistema formativo no cuenta con la capacidad de proporcionar el volumen de profesionales de ciberseguridad demandado por las organizaciones4. Además, cabe señalar que el sistema formativo también se enfrenta a desafíos a la hora de adaptarse al acelerado ritmo de cambio tecnológico, redundando en un menor número de profesionales con conocimientos actualizados.

NIVEL DE RIESGO

Crítico

Elevado

Moderado

PINCHA AQUÍ PARA VOLVER AL APARTADO 05.

Sectoriales

Falta de madurez en el mercado de los ciberseguros

DESCRIPCIÓN

El mercado de los ciberseguros se encuentra en vías de consolidación, presentando carencias en materia de estandarización, coberturas y asignación de pólizas. En consecuencia, empresas y Administraciones se encuentran ante dificultades para disponer de las herramientas necesarias para cubrirse frente a los ciberincidentes.

15

58%

Directivos de organizaciones de todo el mundo que consideran que merece la pena pagar un ciberseguro [1]

30%

Ciberseguros contratados que cubren riesgos graves (como ransomware) [2]

25%

Empresas en todo el mundo que tienen contratada una póliza específica de ciberseguro [3]

FACTORES CLAVE

Entre los diversos elementos que condicionan la falta de madurez en el mercado de los ciberseguros, destacan los siguientes:

1 | Dificultad para ajustar las pólizas debido a la falta de información y la constante evolución del cibercrimen

En el mercado de los seguros, las pólizas se han fijado tradicionalmente en base datos retrospectivos. Sin embargo, en el caso particular de los ciberseguros, la falta de información estadística y la constante evolución del cibercrimen dificultan determinar las pólizas, dando lugar a una estructura de precios que obstaculiza el acceso a esta clase de seguro por parte de las organizaciones.

2 | Dificultad para determinar el perfil de riesgo de las organizaciones aseguradas

La incertidumbre a la hora de evaluar las medidas de seguridad de las organizaciones, los posibles vectores de ataque y las consecuencias de un incidente dificultan establecer el perfil de riesgo de las entidades aseguradas. En este contexto, las aseguradoras optan por exigir certificaciones, incrementar el importe de las pólizas y reducir coberturas, mermando la protección recibida e incrementando el coste de los seguros.

3 | Falta de estandarización a la hora de definir el alcance de las coberturas

La falta de consolidación del mercado de los ciberseguros y la constante evolución del sector digital dificultan estandarizar y definir el alcance de las coberturas, quedando aspectos sin cubrir. En el caso del sector público, la especial protección que requieren las infraestructuras críticas con respecto a las ciberamenazas avanzadas, conlleva que una deficiente definición del alcance de una póliza pueda comprometer su cobertura y exponer a las infraestructuras a mermas de recursos disponibles para responder a las consecuencias de los ciberataques.

NIVEL DE RIESGO
Crítico
Elevado
Moderado

PINCHA AQUÍ PARA VOLVER AL APARTADO 05.

Sectoriales

Concentración del poder digital

DESCRIPCIÓN

La cuota de mercado y capilaridad de los gigantes tecnológicos les otorgan un poder de mercado que comporta riesgos para las organizaciones. Por un lado, la concentración del poder digital favorece el surgimiento de prácticas monopolísticas. Por otro, el volumen de datos que gestionan y su amplia presencia en los sistemas IT de empresas y Administraciones incentiva a los cibercriminales a atacarlas, poniendo en riesgo la seguridad de todas las organizaciones que utilizan sus servicios.

16

70%

De los ingresos de la publicidad digital en España se dividieron entre 2 compañías: Alphabet y Meta [1]

66%

Del mercado global de servicios de almacenamiento en la nube se concentra en Amazon, Alphabet y Microsoft [2]

70%

De los ciberataques globales tienen como objetivo vulnerabilidades del ecosistema Office de Microsoft [3]

FACTORES CLAVE

Entre los diversos elementos que condicionan la concentración digital, destacan los siguientes:

1 | Potencial oligopólico y anticompetitivo en empresas con mayor cuota de mercado

Los productos y servicios digitales de los gigantes tecnológicos son indispensables para toda clase de organizaciones. Esta relación de dependencia conlleva la implantación de dinámicas de poder que podrían derivar, si no se regulan, gestionan y compensan, en la conformación de prácticas anticompetitivas que añadan vulnerabilidad a las infraestructuras tecnológicas.

2 | Incremento en el interés por perpetrar ataques a organizaciones que almacenan un creciente volumen de datos

Los gigantes tecnológicos gestionan un creciente volumen de datos e información sensible procedente de empresas y Administraciones, situándose como un objetivo prioritario para los ciberdelincuentes. Así, una vulnerabilidad en un proveedor clave puede suponer una filtración masiva de datos.

3 | Mayor exposición a interrupciones de servicio y vulnerabilidades en productos y servicios clave

La dependencia frente a un reducido grupo de proveedores IT sitúa a las organizaciones en una posición de vulnerabilidad frente a interrupciones de servicio o ataques a funciones clave. Este hecho se ve agravado por la falta de alternativas extendidas y eficaces a los servicios ofrecidos.

NIVEL DE RIESGO

Crítico

Elevado

Moderado

PINCHA AQUÍ PARA VOLVER AL APARTADO 05.

Recursos

Multiplicidad de agentes en las cadenas de suministro

DESCRIPCIÓN

La multiplicidad de agentes en las cadenas de suministro implica que las organizaciones dependan de extensas redes de proveedores para la prestación de sus servicios y la gestión de la ciberseguridad. En este escenario, un ciberincidente en un proveedor clave puede provocar disrupciones en el funcionamiento de la Administración e, incluso, penetrar los sistemas propios mediante los conocidos como “ataques a la cadena de suministro”.

17

56%

De las empresas manufactureras de todo el mundo sufrieron ciberataques de ransomware en los 3 primeros meses de 2023 [1]

x2

Ataques sobre la cadena de suministro de software en 2023 respecto a los tres años anteriores combinados [2]

40%

De todos los ciberincidentes se desarrollan de forma indirecta a través de la cadena de suministro [3]

FACTORES CLAVE

Entre los diversos elementos que condicionan la multiplicidad de agentes en las cadenas de suministro, destacan los siguientes:

1 | Incremento de las incidencias e interrupciones de servicio relacionadas con proveedores

La multiplicidad de agentes en la cadena de suministro puede conducir a que un ciberataque o incidencia en un proveedor clave paralice la actividad de la Administración o la provisión servicios. De esta manera, las organizaciones no solo están expuestas a ciberincidentes en sus sistemas, también a través de vulnerabilidades de terceros.

2 | Mayor vulnerabilidad frente a ciberataques a la cadena de suministro

La dependencia respecto a una red extensa de proveedores incrementa la exposición frente a los ciberataques a la cadena de suministro, es decir, aquellos que penetran en los sistemas de una organización a través de un proveedor. Según las estimaciones de Gartner, para 2025 la incidencia de esta clase de ataques se habrá triplicado respecto al año 2021[4].

NIVEL DE RIESGO

Crítico

Elevado

Moderado

PINCHA AQUÍ PARA VOLVER AL APARTADO 05.

06.

Ciberataque al Hospital Clínic

06.1. RESUMEN DEL INCIDENTE

En marzo de 2023, el Hospital Clínic de Barcelona sufrió un **ciberataque de tipo ransomware** que dejó inoperativo su sistema informático, obligando a ralentizar parte de la actividad rutinaria del hospital. Si bien este ataque no logró paralizar la totalidad de la actividad del hospital, sí **provocó la interrupción de servicios básicos** como urgencias, consultas externas o el laboratorio de análisis clínicos. Más allá del impacto en la operativa diaria, cabe señalar que el incidente también supuso la **filtración de datos personales sensibles**, con los que los ciberatacantes intentaron extorsionar al Hospital Clínic.

06.2. PARTES INVOLUCRADAS

Agentes de respuesta

HOSPITAL CLÍNIC BARCELONA

Hospital universitario que forma parte del Servei Català de Salut (SCS). Desde hace décadas es uno de los hospitales de referencia a nivel nacional, siendo puntero en campos como la innovación quirúrgica, los trasplantes y la producción científica. Actualmente el Hospital Clínic se estructura como un consorcio público participado por la Generalitat de Catalunya y la Universidad de Barcelona.

Otras partes de interés

RANSOMHOUSE

Grupo criminal especializado en el diseño y uso de ransomware que empezó su actividad en diciembre de 2021. Ha llevado a cabo ciberataques en todo el mundo, tanto a Administraciones y agencias públicas como a empresas privadas como, por ejemplo, AMD. Su motivación es el lucro económico y no se conoce ni el lugar desde el que opera ni la identidad de sus miembros.

Agentes de respuesta

AGENCIA DE CIBERSEGURIDAD DE CATALUNYA

Órgano adscrito a la Generalitat de Catalunya, encargado de prevenir, detectar y responder a incidentes en las redes de comunicaciones electrónicas y sistemas de información públicos. También se encarga de gestionar, coordinar y supervisar la ciberseguridad en Catalunya.

Otras partes de interés

AUTORIDAD CATALANA DE PROTECCIÓN DE DATOS

Organismo dependiente del Parlament de Catalunya, encargado de velar por el cumplimiento de la legislación sobre protección de datos personales. Está dotado de potestad sancionadora y tiene la capacidad de inmovilizar los datos que atenten contra los derechos recogidos en la Constitución Española.

06.3. DESCRIPCIÓN DEL SUCESO

06.3.1. DESARROLLO DEL CIBERATAQUE

Tras haber experimentado un intento de ciberataque dos días antes, el domingo 5 de marzo de 2023, hacia las 11:17 horas, el Hospital Clínic de Barcelona sufrió un **ciberataque que provocó la encriptación de una parte importante de sus sistemas informáticos**, aunque no afectó directamente al sistema core del hospital, el gestor hospitalario. Este ataque afectó tanto a las 3 sedes del hospital como al IDIBAPS (el Instituto de Investigaciones Biomédicas August Pi i Sunyer, centro de investigación vinculado al Clínic) y a 3 Centros de Atención Primaria de la ciudad.

El autor del ciberataque fue el grupo criminal RansomHouse, el cual llevó a cabo un ataque de tipo ransomware a fin de obtener un rescate económico mediante un sistema de doble extorsión: por un lado, introdujo un malware que bloqueó el sistema y, por otro, robó datos que amenazó con filtrar en caso de que el Hospital Clínic no pagase el rescate. El vector de ataque fue la **explotación de la debilidad de una contraseña en las credenciales de autenticación de un trabajador** para los sistemas informáticos del hospital. Sobre la contraseña débil, los ciberatacantes realizaron un "ataque de diccionario", un método de fuerza bruta consistente en probar palabras hasta dar con la combinación de la contraseña. Una vez se hicieron con la contraseña y lograron entrar, alcanzaron a comprometer otros ordenadores y servidores del sistema informático interconectados del hospital.

El grupo logró extraer 4,5 Terabytes de datos personales, por los cuáles pedía 4,2 millones de euros para no publicarlos en la Dark Web. Tanto desde la dirección del hospital como desde la ACC y la Generalitat de Catalunya **no quisieron negociar en ningún momento con los responsables del ciberataque** ni acceder a realizar el pago para liberar el sistema y recuperar los datos sustraídos.

Los datos robados incluían información personal de pacientes, profesionales, entidades colaboradoras y proveedores. Estos datos incluían datos sanitarios, resultados identificativos, resultados de ensayos clínicos, DNIs, números de cuentas bancarias, números de teléfono y hasta firmas escaneadas. Además de datos personales, RansomHouse se hizo con documentación médica de investigaciones y ensayos sobre el cáncer o enfermedades autoinmunes, campos en los que la institución es puntera. Aun así, los atacantes no tuvieron acceso ni a los historiales clínicos de los pacientes ni a los datos del sistema asistencial, de recursos humanos o económicos. Pese a la encriptación y robo, **el ciberataque no supuso pérdida de datos ya que el Clínic contaba con backups** no conectados a la red y, por lo tanto, fuera del alcance de los ciberatacantes.

Desde el principio se mantuvo toda la actividad de internamiento hospitalario (que incluía a unos 800 pacientes), al igual que las hospitalizaciones domiciliarias, los hospitales de día, las pruebas endoscópicas, las exploraciones radiológicas, los servicios de diálisis y la farmacia ambulatoria. Por ello, **no se llegó a producir una paralización total de la actividad**. Sin embargo, intervenciones quirúrgicas no urgentes, las extracciones, el servicio de laboratorio o las sesiones de radioterapia oncológica (que afectaron a 25 pacientes) se tuvieron que aplazar. Los primeros días posteriores al ciberataque, el Hospital Clínic fue recuperando parte de sus servicios y funcionalidad. Así, a los 10 días se lograron recuperar la mayor parte de los sistemas afectados, aunque **la recuperación total no se alcanzó hasta un mes después** del inicio del ciberataque.

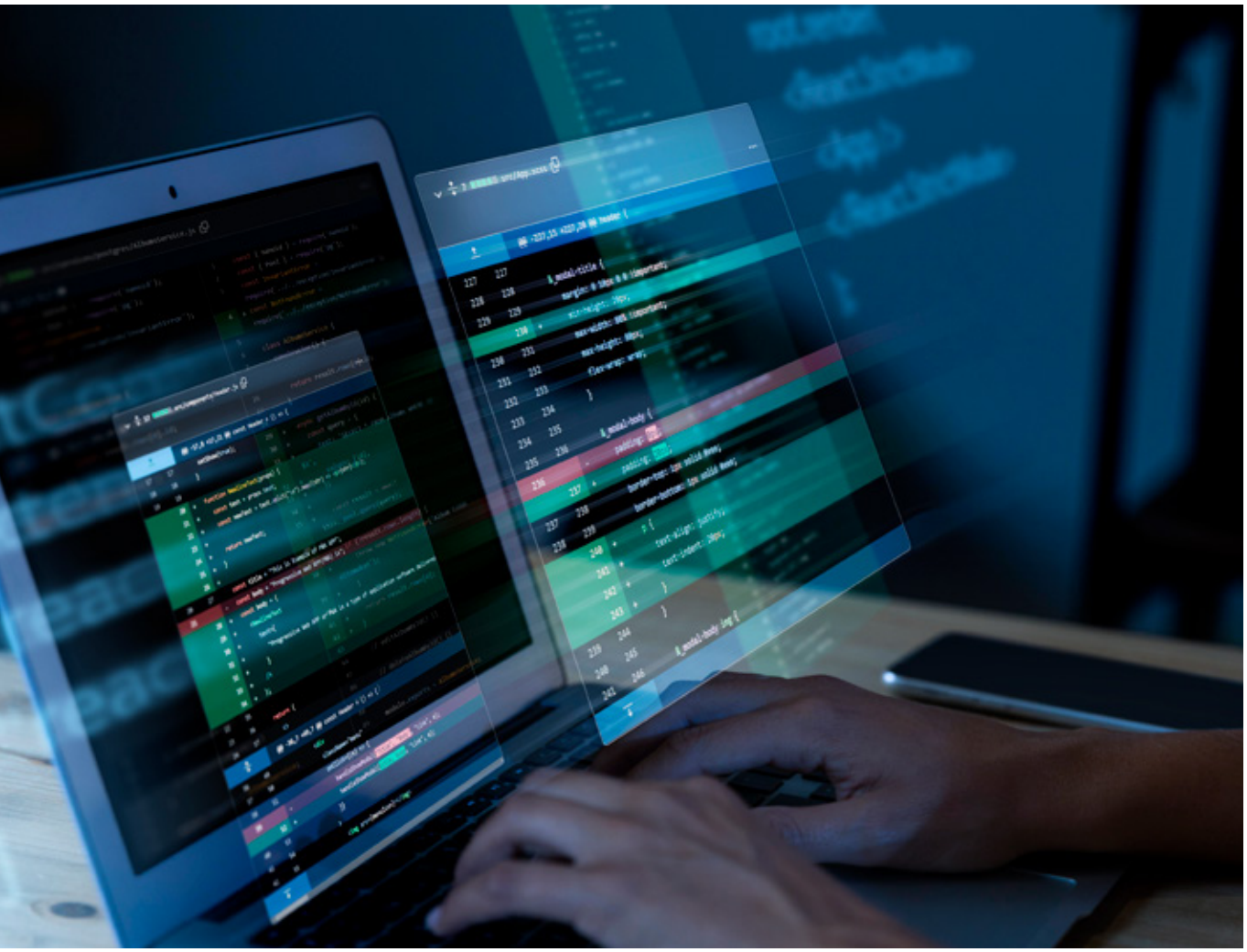
06.3.2. ARTICULACIÓN DE LA RESPUESTA

Primeras decisiones adoptadas. Establecimiento de una estrategia de respuesta

El Hospital Clínic respondió de manera rápida, alertando desde su Dirección de Sistemas de Información (DSI) a la Agencia de Ciberseguridad de Catalunya (ACC) y al Cuerpo de Mossos de Esquadra (a su unidad de Cibercrimen) de que habían sido víctimas de un ciberataque. Más adelante, identificado el actor responsable del ciberataque, la ACC y los Mossos de Esquadra también trabajaron en colaboración con la Interpol. El Hospital informó el mismo día del ciberataque de la creación de comisiones y comités de trabajo específicos.

Además, el Departamento de Salud se coordinó con otros CUAPS (Centro de Urgencias de Atención Primaria) de la ciudad para que estos recibieran los transportes sanitarios de emergencia, especialmente de casos de infartos o ictus. En sintonía con esta medida, **el Clínic pidió públicamente a la población que no acudiese al hospital a no ser que fuese necesario o urgente**.

El equipo técnico de la DSI y la ACC se focalizaron **en implementar las acciones necesarias para restablecer los servicios** y realizar el proceso para la restauración de los datos. Se planificó una recuperación por fases graduales, velando por la contención del impacto y centrándose en la capacidad de restauración.



Aplicación de medidas de contención

Las medidas de contención adoptadas se desarrollaron en base a las siguientes líneas de acción:

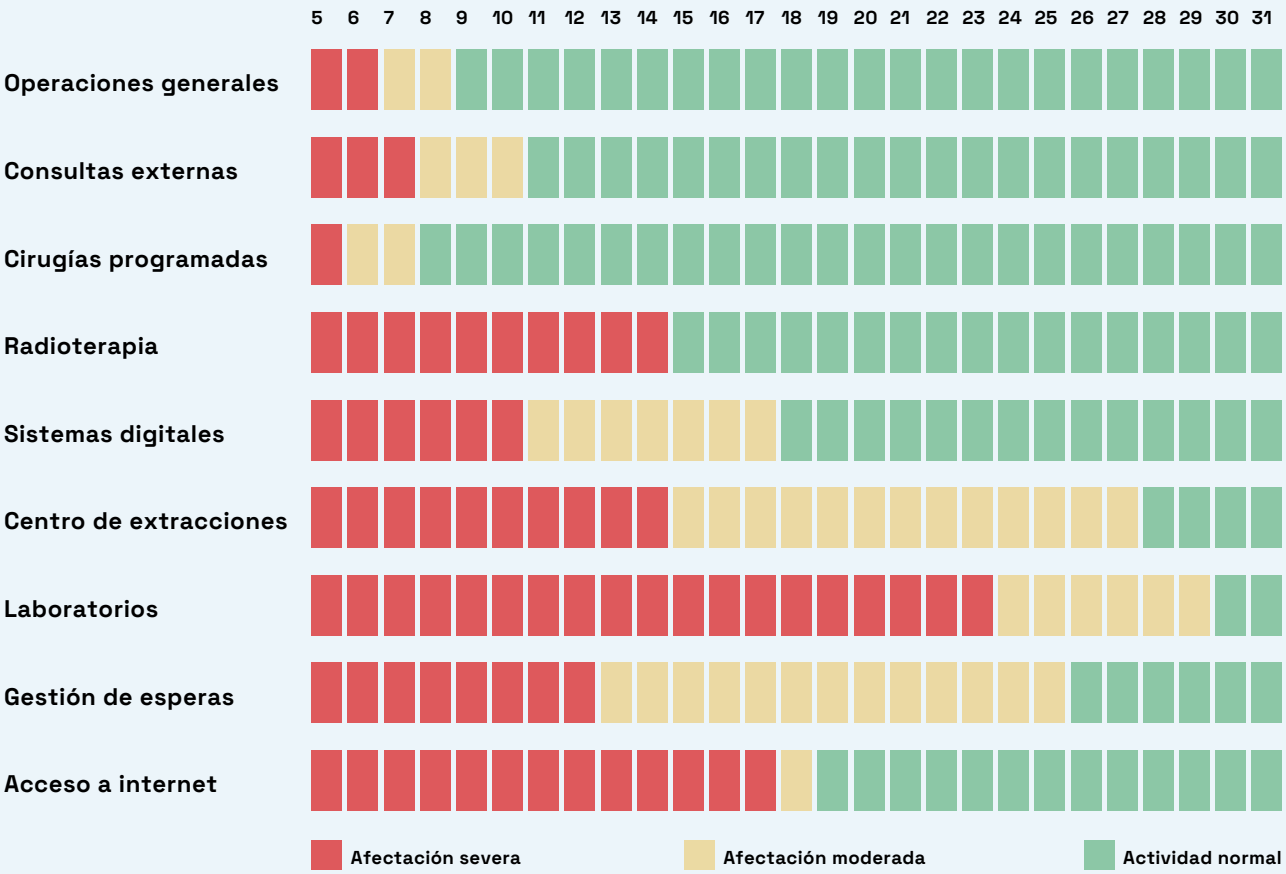
- Medidas técnicas para detener la afectación del ciberataque y erradicar la capacidad de los ciberatacantes.
- Análisis forense del impacto y alcance del ciberataque.
- Proceso de restauración de la información.
- Puesta en servicio de los sistemas de información para reemprender la actividad hospitalaria.
- Cambio masivo de contraseñas.
- Metodologías de trabajo de contingencia tanto internas como externas, para identificar el detalle de las categorías y tipologías de datos comprometidos.

Pese a la activación de los sistemas de contingencia y de la recuperación progresiva de los servicios del hospital, las actividades que se pudieron mantener no se restablecieron con plena capacidad al depender en parte de servicios digitalizados. Esto se plasmó principalmente en **demoras en el ritmo de atención a los pacientes**. Así, la mayor parte de la actividad que mantuvo el Clínic tuvo que **realizarse de forma manual** ante el no funcionamiento de los procesos automatizados, trabajando con **expedientes en papel y rellenando informes y formularios con bolígrafo**. Pese a que el ciberataque se produjo un domingo, buena parte de la plantilla que no tenía que trabajar se acercó al Clínic para colaborar en la recuperación. Esta solidaridad se mantuvo durante los primeros días, aportando recursos humanos que permitieron operar con más eficiencia, pese a tener que trabajar con metodologías manuales.

Habilitación de medidas de recuperación

En el proceso de recuperación **participaron entre 150 y 200 personas cada día**, que trabajaban en estrecha coordinación con los comités de respuesta. Durante los primeros días posteriores al ciberataque, **se desplegaron alrededor de 210 equipos informáticos suplementarios de apoyo** para poder recuperar la normalidad, con los que se consiguió cubrir buena parte de los sistemas afectados hasta que estos se fueron recuperando progresivamente. Por ejemplo, se utilizaron parte de los equipos de apoyo para poder actualizar el censo de pacientes de urgencias y posteriormente actualizar el censo global del hospital, con lo que el Clínic volvía a tener una imagen clara y actualizada de los pacientes ingresados.

06.3.3. CRONOLOGÍA DE LA RECUPERACIÓN: MARZO DE 2023



06.4. RELACIÓN DEL INCIDENTE CON LOS 17 RIESGOS DEL OBSERVATORIO

Incidencia tangencial

Incidencia directa

Evolución Tecnológica

1 | CRECIENTE DIGITALIZACIÓN DE LAS ADMINISTRACIONES PÚBLICAS.

2 | ACELERACIÓN DEL PROGRESO TECNOLÓGICO.

3 | SOFISTICACIÓN DE LAS HERRAMIENTAS DISPONIBLES PARA PERPETRAR CIBERATAQUES.

4 | CRECIENTE VOLUMEN Y VALOR DE LOS DATOS PERSONALES.

Sociopolíticos

5 | AUMENTO DE LA TENCIÓN GEOPOLÍTICA.

6 | AUMENTO DE LA POLARIZACIÓN SOCIAL.

7 | AUMENTO DE LA BRECHA DIGITAL.

Estructura de la criminalidad

8 | CONSOLIDACIÓN DE UN SISTEMA DELICTIVO EN LA ESFERA DIGITAL.

9 | DIFICULTAD PARA PERSEGUIR A LOS CIBERDELINCUENTES.

Institucionales

10 | MEJORABLE IMPLANTACIÓN DE NORMAS INTERNACIONALES Y LEGISLACIÓN INTERNACIONAL, EUROPEA Y NACIONAL EN MATERIA DE CIBERSEGURIDAD.

11 | AUSENCIA DE UNA ESTRUCTURA NACIONAL DE GOBIERNO EJECUTIVO DE LA CIBERSEGURIDAD.

Cultura organizativa

12 | FALTA DE ARQUITECTURA RESILIENTE EN LAS ORGANIZACIONES.

13 | PRECARIEDAD LABORAL Y DESAFECCIÓN DE LOS TRABAJADORES.

Sectoriales

14 | DIFICULTAD PARA CUBRIR LOS PERFILES NECESARIOS PARA LA GESTIÓN DE LA CIBERSEGURIDAD.

15 | FALTA DE MADUREZ EN EL MERCADO DE LOS CIBERSEGUROS.

16 | CONCENTRACIÓN DEL PODER DIGITAL.

Recursos

17 | MULTIPLICIDAD DE AGENTES EN LAS CADENAS DE SUMINISTRO.

06.5. CONSECUENCIAS

Impacto en la actividad

En los momentos inmediatamente posteriores al ataque, la actividad del hospital se llevó a cabo de forma manual, **ralentizando la totalidad de procesos.**

En adición a esta ralentización, hubo algunas actividades que se cancelaron: **11.000 consultas externas, 4.000 analíticas y 300 intervenciones quirúrgicas.**

Apertura de un expediente informativo

A finales de julio, l**a Autoridad Catalana de Protección de Datos (APDCAT) abrió al Hospital Clínic un expediente informativo** para evaluar si, previamente a la filtración de miles de datos personales de los usuarios del servicio de salud, se habían adoptado medidas que garantizasen la protección de datos personales especialmente sensibles.

De detectar un incumplimiento de la LOPD, **se abriría un expediente sancionador.** A día de hoy, no se ha cerrado la evaluación de la APDCAT.

Filtración de datos

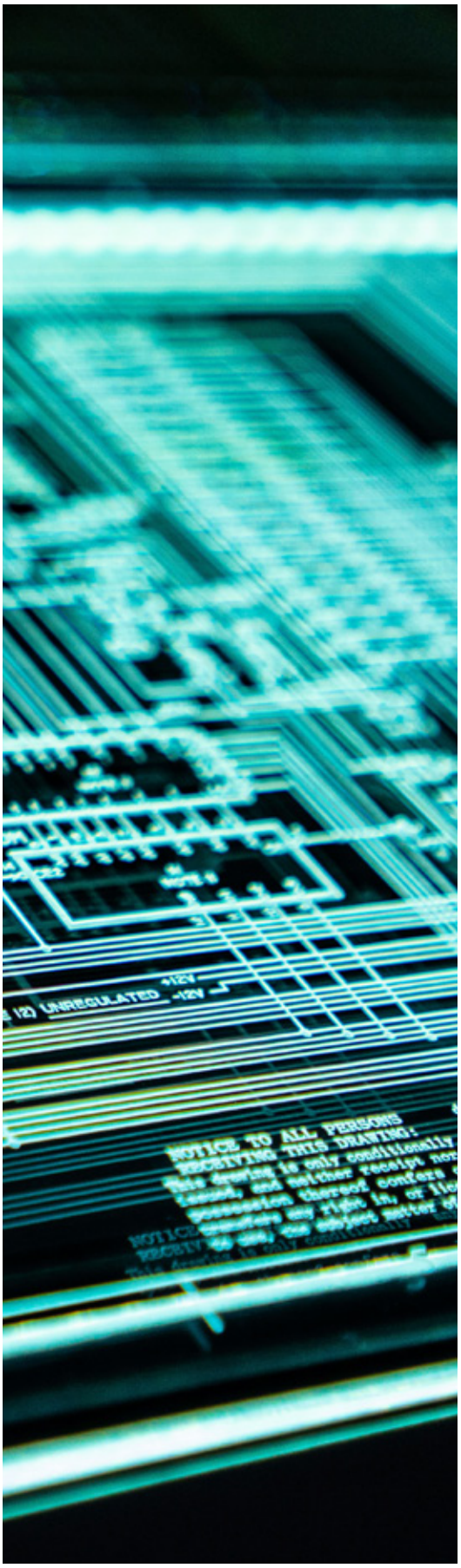
La unidad de cibercrimen de los Mossos d'Esquadra logró tumbar momentáneamente la página web de RansomHouse y dificultar el acceso a los datos robados.

Sin embargo, finalmente, **el grupo pudo distribuir datos personales** mediante 2 filtraciones parciales (de unos 5Gb cada una) en marzo y abril y otra masiva en julio.

Creación de un plan de intervención para el sistema sanitario

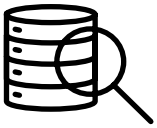
Aunque la Agencia Catalana de Ciberseguridad ya creó en septiembre de 2021 un plan de protección específico para el sistema sanitario, **el Clínic no estaba bajo el amparo de su modelo de protección** en el momento de sufrir el ciberataque. Esto se debe, según la actual secretaría de Telecomunicaciones de la Generalitat, a que el extinto Departamento de Políticas Digitales (responsable del anterior ejecutivo autonómico) marcó una hoja de ruta demasiado lenta. A raíz de este y otros ciberataques sobre hospitales y centros de salud, **se ha acelerado la adopción del plan de intervención en ciberseguridad que integre a todo el sistema sanitario de Catalunya**.

Igualmente, existen otros planes dirigidos a mejorar la ciberseguridad del sistema sanitario, como el CIBERAP, un Plan del Ministerio de Salud de refuerzo de la ciberseguridad en la Atención Primaria financiado con 40 millones de euros a lo largo de 3 años. En este programa participan 13 comunidades autónomas, entre las que se encuentra Catalunya.



Gestión de contraseñas

Pese a que la contraseña atacada en primer momento contenía un número mínimo de caracteres, incluyendo letras mayúsculas, minúsculas y números, los expertos consideraron que era **débil por contener una palabra ligada al hospital**. Como resultado de esta vulnerabilidad, se ha incrementado la robustez de la política de contraseñas de los trabajadores, que incorporarán algún carácter especial, excluirán algunas palabras y el código deberá cambiarse trimestralmente. Adicionalmente, **se ha establecido un sistema de doble autentificación** para fortalecer la seguridad del sistema.



Uso de copias de seguridad

Contar **con back-ups y otras copias de toda la información en varios lugares** (incluyendo al menos un soporte offline) y, por tanto, inaccesibles a los atacantes, demostró ser una estrategia especialmente útil, pues, aunque los atacantes lograron obtener acceso a gran cantidad de datos personales, **no se produjo una pérdida de datos**, que podría haber sido catastrófica. Gracias a esto, el Hospital Clínic no se vio obligado a volver a reunir la información desde cero, si no que pudo reintroducirla en los sistemas digitales una vez volvieron a ser seguros.

Estrategia de comunicación operacional

Si bien la campaña de información general logró un amplio y rápido alcance, el hospital no pudo contactar directamente con los usuarios en los primeros momentos debido a la caída de los sistemas. Por ello, al principio **no se contaba con los medios** para informar individualmente a los pacientes para hacerles saber a qué centro alternativo debían desplazarse o cuál era el estado de sus tratamientos y procesos médicos. No contar con los medios informativos propios supuso añadir una capa al caos informativo general, **aunque la estrategia de comunicación tenía un buen planteamiento desde el primer momento y fue eficaz** para gestionar las medidas que adoptó el hospital.

Política de comunicación pública

Internamente el Hospital pudo coordinarse y hacer saber a todos sus trabajadores cuál era la estrategia de recuperación y cuáles eran las medidas de respuesta que se derivaban. La relevancia pública que adquirió el incidente desde la primera mañana consiguió difundir de forma masiva los comunicados y recomendaciones que adoptó el Hospital Clínic, también gracias a la rápida colaboración con la Generalitat, los Mossos de Esquadra y la Agencia de Ciberseguridad de Catalunya. Así, pasados los primeros momentos de incertidumbre, **el Clínic consiguió imponer una política comunicativa propia** eficaz que facilitó la implementación de las decisiones tomadas.

Notificación y resilencia

Ante la Comisión de Asuntos Institucionales del Parlament de Catalunya, la Autoridad Catalana de Protección de Datos manifestó que el hospital **comunicó la violación de la seguridad dentro del plazo previsto por la normativa y actuó con diligencia** al conocer el incidente, dando aviso a las autoridades competentes de forma ágil y proactiva. La APDCAT también confirmó que **el Clínic estaba implementando nuevas medidas** para fortalecer la seguridad de los sistemas.

07.

Bibliografía

INTRODUCCIÓN

[1] **Estrategia nacional de ciberseguridad 2019**. (2019). Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad, Gobierno de España.

[2] **ENISA Threat Landscape 2023.** (2023). European Union Agency for Cybersecurity.

FICHAS DE RIESGOS

Riesgo 1

[1] **Economía Digital en España.** (2023). Asociación Española de Economía Digital y Boston Consoulting Group.

[2] **6º Estudio sobre la digitalización de la Administración pública.** (2021). Observatorio Nacional de Tecnología y Sociedad.

[3] **El estado de la ciberseguridad en España.** (2022). Deloitte.

Riesgo 2

[1] **eGovernment Benchmark 2022.** (2022). European Commission.

[2] **How a quantum computer could break 2048-bit RSA encryption in 8 hours.** (2019). MIT Technology Review.

Riesgo 3

[1] **How Processor Speeds Have Increased Over the Decades.** (2023). PCSite.

[2] **State of Cyber Resilience.** (2021). Accenture.

[3] **Darktrace Cyber AI Analyst.** (2023). Darktrace.

[4] **NIS Investments Report.** (2023). European Union Agency for Cybersecurity.

Riesgo 4

[1] **Q3 2023 Data Breach Report.** (2023). Identity Theft Resource Center.

[2] **Unprecedented Increase in Cyber Attacks Targeting Government Entities in 2022.** (2022). CloudSEK.

[3] **Future of Privacy.** (2020). Gartner.

[4] **ENISA Threat Landscape 2023.** (2023). European Union Agency for Cybersecurity.

Riesgo 5

[1] **2023 Threat Report – OT Cyberattacks With Physical Consequences.** (2023). Waterfall Security.

[2] **Fog of war: how the Ukraine conflict transformed the cyber threat landscape.** (2023). Google TAG y Mandiant and Trust & Safety.

[3] **Microsoft Digital Defense Report.** (2021). Microsoft.

[4] **ENISA Threat Landscape 2023.** (2023). European Union Agency for Cybersecurity.

Riesgo 6

[1] **2019 CIGI-Ipsos Global Survey on Internet Security and Trust.** (2019). IPSOS.

[2] **Democracy Report 2022.** (2022). V-Dem Institute.

[3] **Standard Eurobarometer 96 - Winter 2021-2022.** (2022). Comisión Europea.

[4] **The spread of true and false news online.** (2018). Massachusetts Institute of Technology.

[5] **ENISA Threat Landscape for Dos Attacks.** (2023). European Union Agency for Cybersecurity.

Riesgo 7

[1] **Colección Monográficos España Digital 2023.** (2023). Observatorio Nacional de Tecnología y Seguridad.

[2] **Colección Monográficos España Digital 2023.** (2023). Observatorio Nacional de Tecnología y Seguridad.

[3] **Cobertura de banca ancha en España en el año 2022.** (2023). Ministerio de Asuntos Económicos y Transformación Digital.

[4] **Cobertura de banca ancha en España en el año 2022.** (2023). Ministerio de Asuntos Económicos y Transformación Digital.

Riesgo 8

[1] **Cybersecurity Ventures Data. (2023).** Cybersecurity Ventures.

[2] **Microsoft Threat Intelligence: Cyber Signals May 2023.** (2023). Microsoft.

[3] **Atlas VPN Data. (2020).** Atlas VPN Research.

[4] **Internet Organised Crime Threat Assessmen**t. (2021). EUROPOL.

[5] **Cybercrime-as-a-Service: Identifying Control Points to Disrupt.** (2017). Massachusetts Institute of Technology.

[6] **ENISA Threat Landscape 2023.** (2023). European Union Agency for Cybersecurity.

Riesgo 9

[1] **To catch a hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors.** (2018). Third Way think tank.

[2] **Informe sobre la cibercriminalidad en España. (2022).** Dirección General de Coordinación y Estudios, Secretaría de Estado de Seguridad.

[3] **ENISA Threat Landscape 2023.** (2023). European Union Agency for Cybersecurity.

Riesgo 10

[1] **Ya son 1.000 las entidades certificadas en el Esquema Nacional de Seguridad.** (2023). Centro Criptológico Nacional.

[2] **Medical Device Cybersecurity: Trends and Predictions 2022 Survey Report.** (2022). Cybellum.

[3] **Cybersecurity statistics, trends, and facts.** (2021). CSO Online.

Riesgo 11

Elaboración propia.

Riesgo 12

[1] **Informe del estado de cultura de ciberseguridad en el entorno empresarial.** (2021). PricewaterhouseCoopers.

[2] **600 trabajadores públicos de Granada 'pican' en un simulacro de estafa por 'phishing'.** (2022). Granada Hoy.

[3] **The Mind of the CISO.** (2023). Trellix.

Riesgo 13

[1] **El estado de la ciberseguridad 2023: el impacto empresarial de los ciberataques en los equipos de seguridad.** (2023). Sophos.

[2] **Análisis y diagnóstico del talento de ciberseguridad en España.** (2022). ObservaCIBER.

[3] **La temporalidad en el sector público se mantiene en el 30 por ciento, el doble que en el privado.** (2023). Central Sindical Independiente y de Funcionarios.

[4] **The Global Risks Report.** (2022). Foro Económico Mundial.

[5] **Análisis y diagnóstico del talento de ciberseguridad en España.** (2022). ObservaCIBER.

Riesgo 14

[1] **Análisis y diagnóstico del talento de ciberseguridad en España.** (2022). ObservaCIBER.

[2] **Análisis y diagnóstico del talento de ciberseguridad en España.** (2022). ObservaCIBER.

[3] **La Sociedad Digital en España 2022.** (2022). Fundación Telefónica.

[4] **Análisis y diagnóstico del talento de ciberseguridad en España.** (2022). ObservaCIBER.

Riesgo 15

[1] **Global cyber risk survey.** (2022). Microsoft y Marsh.

[2] **Cyber Insurance – If you get it, be ready to use it.** (2022). Delinea.

[3] **Informe de Ciberpreparación de Hiscox 2023.** (2023). Hiscox.

Riesgo 16

[1] **Estudio sobre las condiciones de competencia en el sector de la publicidad online en España.** (2021). Comisión Nacional de los Mercados y la Competencia.

[2] **Enterprise spending on cloud infrastructure services.** (2022). Synergy Research Group.

[3] **Security Analyst Summit.** (2019). Kaspersky.

Riesgo 17

[1] **The State of Ransomware in Manufacturing and Production 2023.** (2023). Sophos.

[2] **9th Annual State of the Software Supply Chain Report.** (2023). Sonatype.

[3] **Most common cyberattack patterns from 2022.** (2022). Security Intelligence.

[4] **How Software Engineering Leaders Can Mitigate Software Supply Chain Security Risks.** (2021). Gartner.

Observatorio
de riesgos de ciberseguridad

CCN-CERT
centro criptológico nacional

Institut Cerdà