Baker McKenzie.

Ciberseguridad e Industria Farmacéutica: Del Secreto Empresarial a la NIS 2

David Molina | Fundación CEFI | 26 de octubre de 2023

David Molina
Asociado Senior
IPTech

+34 685 181 427
david.molina@bakermckenzie.com

Agenda

01 Una panorámica de la ciberseguridad "actual" desde la perspectiva jurídica

02 Pinceladas de la NIS 2

01 Una panorámica de la ciberseguridad "actual" desde la perspectiva jurídica

Ciberseguridad, Ciberincidente y Ciberataque

Ciberseguridad

Conjunto de actuaciones orientadas a asegurar, en la medida de lo posible, las redes y sistemas que constituyen el ciberespacio: (i) detectando y enfrentándose a intrusiones, (ii) detectando, reaccionando y recuperándose de incidentes y (iii) preservando la confidencialidad, disponibilidad e integridad de la información.

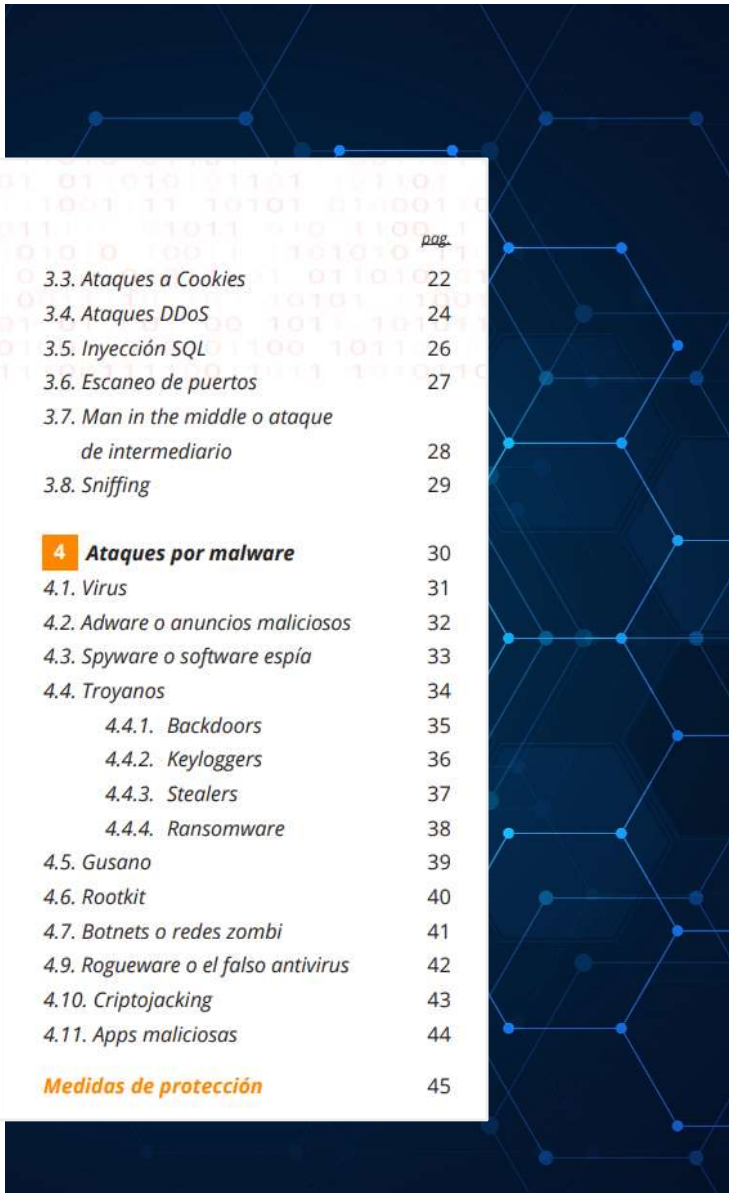
Ciberincidente

Todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información.

Ciberataque

Ataque organizado contra el sistema informático de una entidad o empresa con el objetivo de bloquearlo, dañarlo u obtener información.

Guía sobre Ciberataques de INCIBE y la OSI



Índice

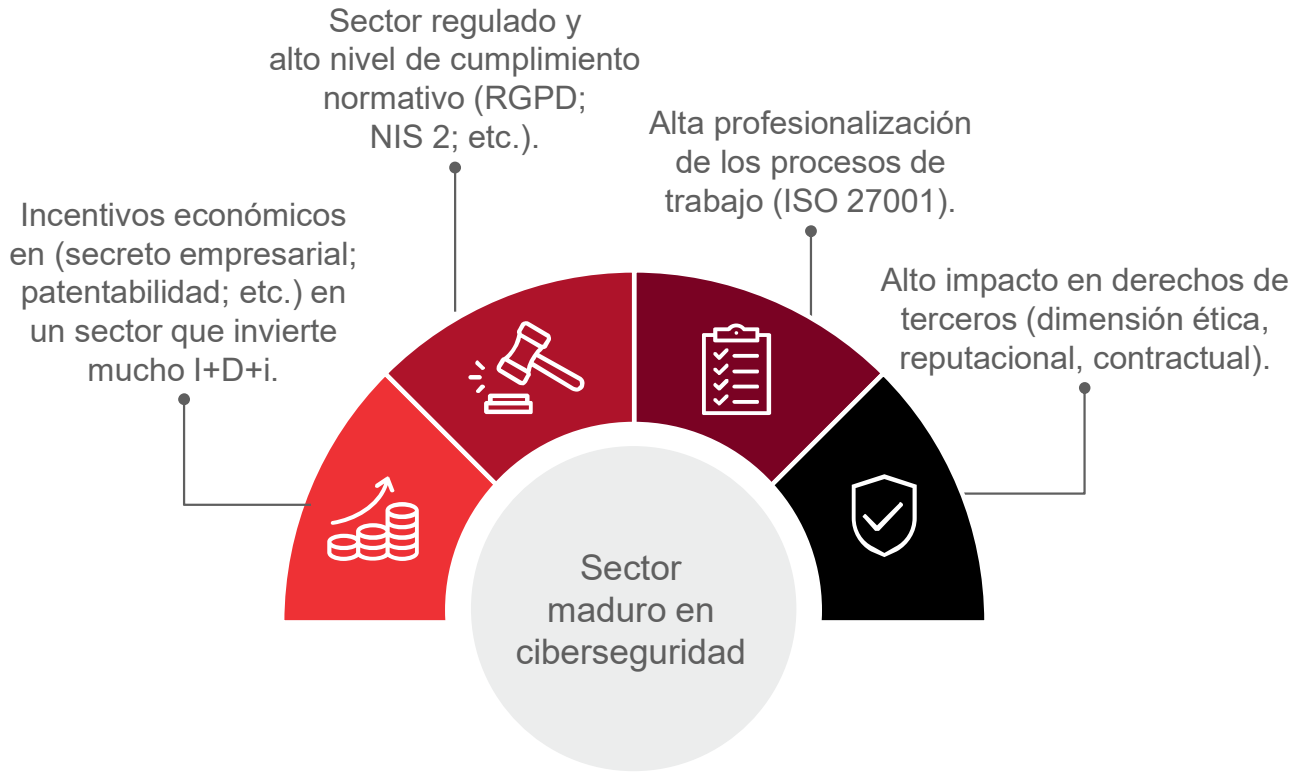
Clásica aproximación no jurídica

Aproximación clásica: (i) gestión empresarial y de procesos y (ii) desde la pura técnica informática.

Por ejemplo, ver el "Procedimiento de gestión de ciberincidentes para el sector privado y la ciudadanía" de INCIBE.

Figura 1. Fases de la gestión de incidentes

¿Qué hace especial el sector farmacéutico respecto a la Ciberseguridad?



Posibles implicaciones legales (para el receptor del ciberataque)

Protección de datos

Secretos empresariales propios y de terceros

¿NIS 1?

Disciplina laboral

Responsabilidad civil
(tanto respecto a obligaciones contractuales como a daños)

Dimensión penal

Ciberseguro

¿Ámbito regulatorio?

26 de enero de 2023, ejemplo aclaratorio de la dimensión regulatoria

La AEMPS informa de varios fallos de software relacionados con las bombas de insulina […]

"

- La Agencia Española de Medicamentos y Productos Sanitarios (AEMPS) **ha tenido conocimiento, a través del fabricante** […], de cuatro posibles fallos en el software de las bombas de insulina […]. Estos fallos **afectan a la administración de la dosis correcta de insulina**, lo que puede resultar en una hipoglucemia o hiperglucemia.
- […] Si ocurre este cuarto fallo, podría provocar hipoglucemia o hiperglucemia. En casos graves de hipoglucemia o hiperglucemia, el usuario puede requerir hospitalización o intervención de un médico.
- **La empresa está enviando una nota de aviso a los centros sanitarios y a los pacientes que disponen de las bombas de insulina** […] incluidas en el apartado de "Productos afectados", para informarles del problema identificado y de las acciones a seguir.
- […] ha desarrollado una actualización de software para la bomba de insulina […] que **mitiga los posibles problemas descritos anteriormente**. Esta actualización se denomina […]"

Secretos empresariales VS información confidencial-reservada, etc.

Ley 1/2019, de 20 de febrero, de Secretos Empresariales

Artículo 1. Objeto.

1. El objeto de la presente ley es la protección de los secretos empresariales.

A efectos de esta ley, se considera secreto empresarial cualquier información o conocimiento, incluido el tecnológico, científico, industrial, comercial, organizativo o financiero, que reúna las siguientes condiciones:

a) Ser secreto, en el sentido de que, en su conjunto o en la configuración y reunión precisas de sus componentes, no es generalmente conocido por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información o conocimiento en cuestión, ni fácilmente accesible para ellas;

b) tener un valor empresarial, ya sea real o potencial, precisamente por ser secreto, y

c) haber sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto.

2. La protección se dispensa al titular de un secreto empresarial, que es cualquier persona física o jurídica que legítimamente ejerza el control sobre el mismo, y se extiende frente a cualquier modalidad de obtención, utilización o revelación de la información constitutiva de aquél que resulte ilícita o tenga un origen ilícito con arreglo a lo previsto en esta ley.

3. La protección de los secretos empresariales no afectará a la autonomía de los interlocutores sociales o a su derecho a la negociación colectiva. Tampoco podrá restringir la movilidad de los trabajadores; en particular, no podrá servir de base para justificar limitaciones del uso por parte de estos de experiencia y competencias adquiridas honestamente durante el normal transcurso de su carrera profesional o de información que no reúna todos los requisitos del secreto empresarial, ni para imponer en los contratos de trabajo restricciones no previstas legalmente.

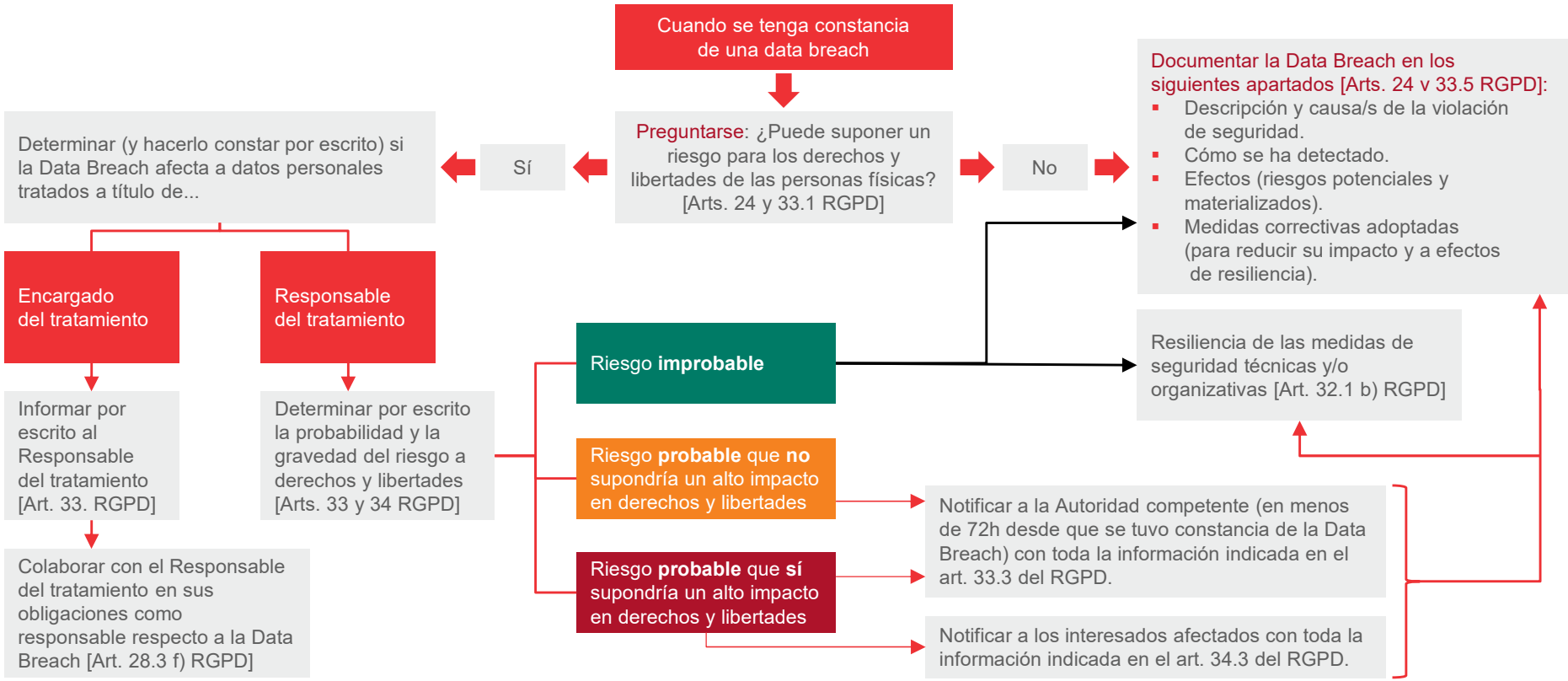
Asimismo, lo dispuesto en esta ley se entenderá sin perjuicio de lo previsto en el Título IV de la Ley 24/2015, de 24 de julio, de Patentes.

Definición de brechas de seguridad y obligación de notificar a la autoridad competente

Art. 4. 12 RGPD:

12) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

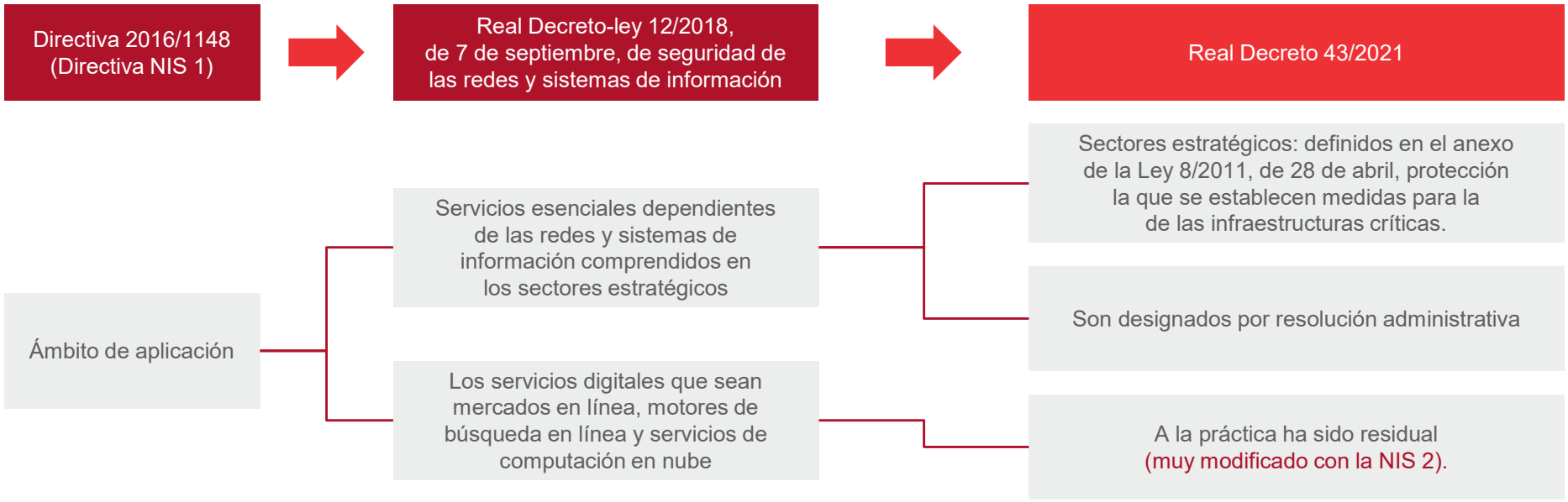
Brechas de seguridad (RGPD)



Medidas de seguridad en protección de datos: obligación de medios con constante necesidad de actualización (ejemplo de IA)

02 Pinceladas de la NIS 2

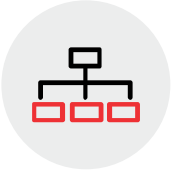
Normativa actualmente vigente en materia de Ciberseguridad: difícilmente aplicable al sector farmacéutico (a diferencia de la NIS 2)



Ideas clave

Debería estar transpuesta al ordenamiento estatal como muy tarde el 17 de octubre de 2024 (y el día siguiente ya debería ser aplicable).

Sanciones de hasta 7 o 10 millones de Euros (según el tipo de entidad) o hasta 1,4% o 2% de la facturación mundial anual.



Responsabilidad directa del Órgano de Dirección (ciertas inhabilitaciones a directivos como persona física; a la espera de su transposición).

Modificación substancial del ámbito de aplicación, (art. 2.1 de la Directiva y su remisión al Anexo I si son como mínimo medianas empresas de dicho sectores) + otros casos en que se pueden añadir a más entidades.

Mediana empresa según la referencia normativa (50 empleados o más o volumen de negocios anual o cuyo balance general anual supere los 10 millones de euros).

Anexo I de la NIS 2 (sectores de alta criticidad)

Sector sanitario		—Prestadores de asistencia sanitaria, tal como se definen en el artículo 3, letra g), de la Directiva 2011/24/UE del Parlamento Europeo y del Consejo ([18]) —Laboratorios de referencia de la UE, tal como se definen en el artículo 15, del Reglamento (UE) .../...del Parlamento Europeo y del Consejo ([19]) —Entidades que realizan actividades de investigación y desarrollo de medicamentos, tal como se definen en el artículo 1, punto 2, de la Directiva 2001/83/CE del Parlamento Europeo y del Consejo ([20]) —Entidades que fabrican productos farmacéuticos de base y especialidades farmacéuticas a que se refiere la sección C, división 21, de la NACE Rev. 2 —Entidades que fabrican productos sanitarios que se consideran esenciales en situaciones de emergencia de salud pública («lista de productos sanitarios esenciales durante la emergencia de salud pública») en el sentido del artículo 22 del Reglamento (UE) 2022/123 del Parlamento Europeo y del Consejo ([21])

Reglamento (UE) 2022/2371 del Parlamento Europeo y del Consejo, de 23 de noviembre de 2022, sobre las amenazas transfronterizas graves para la salud y por el que se deroga la Decisión n.o 1082/2013/UE (DO L 314 de 6.12.2022, p. 26).

Directiva 2001/83/CE del Parlamento Europeo y del Consejo, de 6 de noviembre de 2001, por la que se establece un código comunitario sobre medicamentos para uso humano (DO L 311 de 28.11.2001, p. 67).

Reglamento (UE) 2022/123 del Parlamento Europeo y del Consejo, de 25 de enero de 2022, relativo al papel reforzado de la Agencia Europea de Medicamentos en la preparación y gestión de crisis con respecto a los medicamentos y los productos sanitarios (DO L 20 de 31.1.2022, p. 1).

Notificación de incidente significativo al CSIRT/CERT o a la autoridad

Notificación por etapas. A más plazo, más nivel de detalle.

Plazos de 24 horas, de 72 horas **y** 1 mes.

Incidente

"Todo hecho que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los **datos** almacenados, transmitidos o tratados, **o los servicios** ofrecidos por sistemas de redes y de información o accesibles a través de ellos".

Significativo

O (a) ha causado o puede causar "**graves perturbaciones operativas** de los servicios **o pérdidas económicas**" **o** (b) ya ha afectado o puede llegar a afectar a "otras personas físicas o jurídicas al causar **perjuicios materiales o inmateriales considerables**".

Ideas clave de las medidas de seguridad a adoptar basadas en un análisis de riesgos

"Medidas técnicas, operativas y de organización adecuadas y proporcionadas para gestionar los **riesgos** […] en sus operaciones o en la prestación de sus servicios y **prevenir o minimizar** las repercusiones de los incidentes en los destinatarios de sus servicios y en otros servicios.

Factores que influyen en las medidas a establecer (**expresamente previstos**): (1) el propio análisis de riesgos (deben ofrecer un nivel de seguridad adecuado a dicho análisis), (2) el coste de su aplicación, (3) el grado de exposición a los riesgos, (4) el tamaño de la entidad, (5) la probabilidad que se den incidentes y (6) la posible gravedad de las consecuencias.

Hay unas medidas mínimas a adoptar y la UE desarrollará cómo se aterrizan estas medidas mínimas (como muy tarde el 17 de octubre de 2024).

Medidas mínimas obligatorias

- a) Las políticas de seguridad de los sistemas de información y análisis de riesgos;
- b) La gestión de incidentes;
- c) La continuidad de las actividades, como la gestión de copias de seguridad y la recuperación en caso de catástrofe, y la gestión de crisis;
- d) La seguridad de la cadena de suministro, incluidos los aspectos de seguridad relativos a las relaciones entre cada entidad y sus proveedores o prestadores de servicios directos;
- e) La seguridad en la adquisición, el desarrollo y el mantenimiento de sistemas de redes y de información: incluida la gestión y divulgación de las vulnerabilidades;
- f) Las políticas y los procedimientos para evaluar la eficacia de las medidas para la gestión de riesgos de ciberseguridad;
- g) Las prácticas básicas de ciberhigiene y formación en ciberseguridad;
- h) Las políticas y procedimientos relativos a la utilización de criptografía y, en su caso, de cifrado;
- i) La seguridad de los recursos humanos, las políticas de control de acceso y la gestión de activos;
- j) El uso de soluciones de autenticación multifactorial o de autenticación continua, comunicaciones de voz: video y texto seguras y sistemas seguros de comunicaciones de emergencia en la entidad, cuando proceda.

Preguntas

Baker McKenzie ofrece soluciones integradas para desafíos complejos.

Los desafíos empresariales complejos requieren una respuesta integrada que abarque diferentes mercados, sectores y áreas del derecho. Nuestras soluciones proporcionan a nuestros clientes un asesoramiento sin fisuras, respaldado por un profunda experiencia legal y sectorial, así como un conocimiento de primer nivel de los retos a los que se enfrentan las empresas en cada mercado local. Presentes en más de 70 oficinas en todo el mundo, Baker McKenzie trabaja junto a nuestros clientes para ofrecer soluciones para un mundo conectado.

bakermckenzie.com