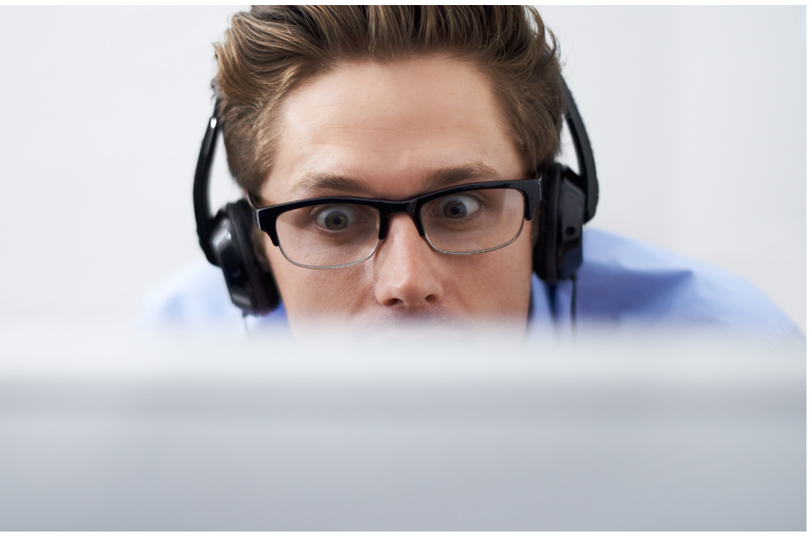
CIBERSEGURIDAD Y COMPLIANCE

José Luis Colom Planas
Asesor del Centro Criptológico Nacional (CCN)

En un mundo cada vez más interconectado e inmerso en la digitalización de la economía, la ciberseguridad ha dejado de ser una elección arbitraria de las organizaciones más cautas, para convertirse en un requisito de protección de los intereses y derechos de terceros, así como de la propia organización.

Los marcos normativos, ya sean jurídicos, como el Esquema Nacional de Seguridad (ENS) regulado por el RD 311/2022, de 3 de mayo, o de adscripción voluntaria, como la norma ISO/IEC 27001:2022 sobre sistemas de gestión de seguridad de la información (SGSI), son un facilitador más para garantizar el cumplimiento de las organizaciones.

En este sentido, el Corporate Compliance Officer (CCO), u Oficial de Cumplimiento como lo designamos en España, debe implicarse en la consideración de la Ciberseguridad por parte de la Organización en la que presta su desempeño profesional.



ALGUNAS DEFINICIONES PARA ACLARAR CONCEPTOS

Podemos considerar el **CIBERESPACIO** como aquel espacio virtual, constituido por medios cibernéticos (TIC), donde se agrupan los diferentes servicios digitales de Internet.

En consecuencia, entenderemos por **CIBERSEGURIDAD** la protección de los Sistemas de Información que se encuentran conectados al ciberespacio de los potenciales ataques procedentes de Internet, preservando así los servicios que prestan y la información que manejan.

Podemos ver la Ciberseguridad como un subconjunto de un concepto más amplio, que es la SEGURIDAD DE LA INFORMACIÓN. A modo de ejemplo aclaratorio, la Ciberseguridad no abarca la protección ante una intrusión física a un Centro de Datos, ni ante la inserción de un pendrive USB infectado con malware en un equipo informático, ataques que sí se contemplan desde el punto de vista más amplio de la seguridad de la información y/o de los servicios.

De la definición de Ciberseguridad surge la necesidad de clarificar que se entiende por un Sistema de Información, a diferencia de un sistema informático. Entendemos por **SISTEMA DE INFORMACIÓN** aquel conjunto de elementos, habitualmente tecnológicos (sistemas informáticos y de comunicaciones) pero que suelen incluir personas, que interactúan para soportar los servicios que dicho sistema presta, tratando la información que éstos manejan. Como vemos, pone el acento en lo material, es decir, personas y tecnología.

Adicionalmente, respecto a un Sistema de Información se pueden implementar **SISTEMAS DE GESTIÓN**, que podemos definir como un conjunto de instrumentos organizativos (Políticas, normas internas, procedimientos, etc.) interrelacionados y orientados a mejorar la eficacia y la eficiencia de lo gestionado. En el caso de un Sistema de Gestión de la Seguridad de la Información (SGSI) se pretende mejorar la eficacia y la eficiencia de la seguridad del Sistema de Información sobre el que se aplica.

Otros Sistemas de Gestión son, por ejemplo, de calidad, que determina la norma ISO 9001:2015, ambiental, basado en la norma ISO 14001:2015, de Compliance, que determina la norma ISO 37301:2021, etc.

Para finalizar este elenco de definiciones, definiremos S**EGURIDAD DE LA INFORMACIÓN**, en sentido amplio, como el conjunto de medidas preventivas (basadas en el riesgo) y reactivas, que permiten proteger en todas las dimensiones establecidas los servicios y la información, junto a los demás activos vinculados, que constituyen un Sistema de Información.

La seguridad es un término abstracto que para ayudar a perfilar habitualmente se descompone en tres dimensiones: la Confidencialidad, la Integridad y la Disponibilidad, aunque el ENS considera adicionalmente la Autenticidad y la Trazabilidad, hasta totalizar cinco dimensiones, según señala el apartado 2 del Anexo I del RD 311/2022, señalando: *"A fin de determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información tratada o de los servicios prestados y, en su consecuencia, establecer la categoría de seguridad del sistema de información en cuestión, se tendrán en cuenta las siguientes dimensiones de la seguridad, que se identificarán por sus correspondientes iniciales en mayúsculas: a) Confidencialidad [C]; b) Integridad [I]; c) Trazabilidad [T]; d) Autenticidad [A]; e) Disponibilidad [D]"*.

Podemos definirlas por la finalidad que pretenden:

- **Confidencialidad:** Garantiza que la información únicamente será accesible a quienes están autorizados a hacerlo.
- **Integridad:** Garantiza que la información únicamente será modificada por quienes tienen autorización para hacerlo.
- **Disponibilidad:** Garantiza que la información y los servicios estén disponibles durante los intervalos establecidos.
- **Autenticidad:** Garantiza que quién accede o proporciona información realmente "sea quién dice ser".
- **Trazabilidad:** Garantiza que en todo momento pueda conocerse "quién hizo qué".

LOS ESLABONES MÁS DÉBILES DE LA CADENA

Si asimilamos una organización a una cadena, los eslabones más débiles desde el punto de vista de la Ciberseguridad suelen ser los **empleados y colaboradores**. Los ciberdelincuentes lo saben y por esta razón intentarán romper primero esos eslabones, previendo que así obtendrán un ahorro en el esfuerzo necesario para comprometer la Organización.

Un ejemplo lo tenemos en los Ciberataques basados en técnicas de ingeniería social como puede ser el phishing, la suplantación de identidad, etc.

Es por dicho motivo que, además de las medidas de seguridad técnicas y organizativas, las acciones directas focalizando en empleados y colaboradores, como lo es la concienciación en Ciberseguridad, se tornan en imprescindibles.

Pero, desde un punto de vista riguroso, ¿Qué diferencia hay entre formación y concienciación? Quienes tengan formación jurídica están en mejores condiciones para comprender la diferencia inicialmente, ya que una distinción doctrinal en la Teoría del Derecho determina que una norma pude descomponerse en reglas y principios.

Las REGLAS indican lo que debe o no debe hacerse, mientras que los PRINCIPIOS son aquel bien superior que justifica las reglas. Ante esta tesitura, podemos entender que mientras la Formación se limita a explicar las reglas a las personas, haciéndolo de la forma más didáctica posible, la Concienciación supone determinadas acciones encaminadas a favorecer que las personas interioricen los principios, de modo que no incumplan las reglas, tanto si se sienten observadas, como si no.

En consecuencia, un equilibrio entre **formación y concienciación** parece la fórmula adecuada. En este sentido, el ENS dispone de dos medias de seguridad específicas en su Anexo II:

De una parte, la medida **[mp.per.3] Concienciación,** que señala *"Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente:*

- *[mp.per.3.1] La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.*
- *[mp.per.3.2] La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.*
- *[mp.per.3.3] El procedimiento para informar sobre incidentes de seguridad, sean reales o falsas alarmas".*

De otra parte, la medida **[mp.per.4] Formación,** que señala:

- *"[mp.per.4.1] Se formará regularmente al personal en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones, en particular en lo relativo a:*
  - *Configuración de sistemas.*
  - *Detección y reacción ante incidentes.*
  - *Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.*
- *Además, se evaluará la eficacia de las acciones formativas llevadas a cabo".*

CONCLUSIONES INFERIDAS OBSERVANDO CIBERATAQUES

Existe una gran variedad de posibles ciberataques, ciberdelitos si se prefiere, con implicaciones directas o indirectas en la Organización que se producen constantemente.

Entre todos ellos, cabe citar: Código dañino (malware) en general; Ransomware, en particular, con exfiltración previa de datos sensibles para asegurar la extorsión, junto a cifrado masivo la información; ataques basados en ingeniería social, como lo son:

- El phishing, ya sea masivo o dirigido;
- La suplantación de identidad haciéndose pasar, por ejemplo, por un proveedor que desea cambiar la cuenta bancaria donde recibir las transferencias;

- El fraude del CEO, haciéndose pasar el ciberdelincuente por el CEO de la organización para ordenar un pago de forma urgente, necesario para cerrar un 'negocio' sin tiempo a verificarlo por el personal administrativo;

- Ataques de denegación de servicio, impidiendo los accesos legítimos a determinado portal web;

- Espionaje e intrusiones a los servidores de una Organización para acceder a información sensible, alterarla o suprimirla;

- Hacktivismo para causar daños a la Organización atacada, tal vez a su imagen; etc.

Desgraciadamente, podemos llegar a afirmar que todas las organizaciones, ya sean del sector público o privado, deben considerar que **no se trata de "si se producirá" un ciberataque, sino de "cuándo se producirá" y si cuando eso ocurra, la organización estará preparada.** Por lo tanto, todas las organizaciones deben revisar, actualizar y reforzar continuamente la ciberseguridad.

Un ciberataque puede tener consecuencias muy graves, tanto en términos de posible interrupción de las operaciones, como por el daño reputacional y/o económico que pueda causarse a empleados, clientes, etc.

Al final, puede llegar a afirmarse que la seguridad de la información en la 'era digital' es una de las aristas de la **sostenibilidad,** ya que 'nadie usa aquello en lo que no confía'.

EL CONCEPTO DE COMPLIANCE Y SU RELACIÓN CON LA CIBERSEGURIDAD

Según la norma ISO 37301:2021, *"Compliance es un proceso continuo y el resultado de que una organización cumpla con sus obligaciones"*.

En esta definición de amplio recorrido cabe todo. Es por ello que cobra valor una buena definición del 'alcance', es decir, de los límites que determinan el ámbito que abarcará el Sistema de Gestión de Compliance (SGC) que se defina e implante en la Organización.

En consecuencia, podemos hablar de Compliance en general; de Compliance legal, si lo circunscribimos al cumplimiento de las obligaciones legales que marca el ordenamiento jurídico de la(s) jurisdicción(es) donde opera la Organización; de Compliance Penal, si pretendemos llegar a impedir que se cometan delitos en nombre o por cuenta de la Organización y en su beneficio, pudiendo, consecuentemente, quedar exonerada de responsabilidad penal la persona jurídica que implante eficazmente, por ejemplo, en España, un SGC basado en la norma UNE 19601:2017; y, por último, de Compliance respecto a las obligaciones como sujeto obligado que determina la Ley 10/2010 de PBCyFT. Y así podríamos continuar determinando otras parcelas de cumplimiento.

Podemos analizar las implicaciones en Compliance, es decir, en el cumplimiento o incumplimiento de las obligaciones por parte de una Organización, partiendo de las consecuencias del ciberataque que, en muchas ocasiones, impedirán cumplir:

- **Exfiltración de información:** incumplimiento de cláusulas contractuales y/o acuerdos de confidencialidad.

- **Violaciones de datos personales:** incumplimiento de la responsabilidad de custodiar datos personales de empleados, clientes (ciudadanos en el sector público) y proveedores. Violación según la determina el art. 33 RGPD.

- **Pérdida de continuidad del negocio:** incumplimiento contractual debido a la pérdida de disponibilidad en los servicios, derivando en reclamaciones de clientes. Incumplimiento de preceptos legales debido, por ejemplo, a la incapacidad de atender al ejercicio de derechos de Protección de Datos.

- **Daño reputacional:** A la organización que ha sufrido el ciberataque y/o al honor y a la propia imagen de terceros.

- **Daños a terceros:** Ordenadores zombis que han sido hackeados para obedecer a un puesto de mando y control y lanzar desde él ataques a terceros, por ejemplo, de denegación de servicio (DoS o DDoS).

- **Pasarela para acceder a un tercero:** Hackeo de una Organización para, desde ella, entrar y comprometer a sus clientes.

- **Etc.**

La responsabilidad de la Persona Jurídica (PJ) puede ser de diferente naturaleza, como penal o civil.

La PJ autora del ciberataque puede incurrir en:

- **Responsabilidad penal derivada de la comisión de dos posibles delitos:** el primero, de daños informáticos (art. 264 CP), y el segundo, de descubrimiento de secretos o vulneración de la intimidad (art. 197 al 200 CP).

- **Responsabilidad civil subsidiaria,** tipificada en el art. 120.4 CP.

La PJ atacada puede sufrir consecuencias tanto en vía administrativa como en la civil, si carece de las pertinentes medidas de seguridad:

- La responsabilidad contractual (art. 1101 CC y siguientes) y extracontractual por obligaciones que nacen de la culpa o negligencia (art. 1902 y 1089 CC), encuentran su justificación en el deber general de no dañar a terceros, adoptando las medidas de seguridad necesarias y actuando con la debida diligencia.

- No obstante, la Organización puede quedar exonerada de responder de aquellos daños que no hayan podido preverse, o cuando no quede demostrado el nexo de causalidad (art. 1.105 y 1.107 CC).

La Organización es responsable de los daños o perjuicios que el ciberataque haya podido causar a sus clientes. Por ello, es recomendable que, en el momento en que se sufra este tipo de ciberataques, se ponga en contacto tanto con los clientes que han podido verse afectados, para advertirles y que procedan a la modificación de sus credenciales, como con aquellos clientes que todavía no han sufrido, o no han notado, sus consecuencias, para prevenirles.

No debe olvidarse la legislación vigente en materia de Protección de Datos. El art. 32 RGPD señala respecto a la seguridad del tratamiento: *"Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo"*.

Se puede finalizar este apartado recordando que las organizaciones pueden llegar a ser responsables por su actuación u omisión, antes, durante y tras el ciberataque, ante la falta grave del deber de cuidado.

Concretando más, pueden serlo por el incumplimiento injustificado de la normativa vigente de Protección de Datos, ya sea antes del Ciberincidente (art. 32 RGPD, reproducido en el párrafo anterior) o después del mismo (art. 34 RGPD), que dispone: *"1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida"*, sin perjuicio de su comunicación a la autoridad de control, como puede ser en España la AEPD o, para el sector público, las agencias o autoridades autonómicas de protección de datos, de existir, según determina el art. 33 RGPD: *"En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas"*.

NORMATIVA JURÍDICA RELACIONADA CON LA CIBERSEGURIDAD

Es evidente que, en función del sector de actividad de la Organización, o de sus potestades o competencias públicas, de tenerlas, podrá estar obligada por diferente normativa, además de, por ejemplo, el Esquema Nacional de Seguridad si pertenece al sector público, o le aporta soluciones o presta servicios.

A modo de ejemplo, podemos citar la reciente Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, en lo que respecta a sectores de alta criticidad (Anexo I) u otros sectores críticos (Anexo II) conocida como NIS2, que sustituye a la NIS1 traspuesta al ordenamiento jurídico español mediante el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, desarrollado mediante el Real Decreto 43/2021, de 26 de enero.

Por otro lado, la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, obliga a los sectores estratégicos Nacionales relacionados en su Anexo, estando desarrollada mediante el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas en España.

Otro ejemplo es la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, que comprende, entre otros, la instalación y explotación de las redes de comunicaciones electrónicas, así como la prestación de los servicios de comunicaciones electrónicas, incluyendo aspectos como son el secreto de las comunicaciones (Art. 58), Protección de Datos de carácter personal (Art. 60), Cifrado (Art. 62), e Integridad y seguridad (Art. 63).

Y así podríamos ir enumerando normas jurídicas vinculadas con la Ciberseguridad y/o la Seguridad de la Información, en función del tipo de Organización.

Para facilitar la labor de los Oficiales de Cumplimiento en este ámbito de la Ciberseguridad, el Boletín Oficial del Estado (BOE), edita los que se han dado en llamar Códigos electrónicos, conteniendo un compendio temático y actualizado de normativa vigente, que además admite suscripción gratuita al servicio de avisos sobre actualizaciones. Los dos códigos más relevantes, en materia de Ciberseguridad, son los siguientes:

- **Código de Derecho de la Ciberseguridad:** Incluye normativa de Seguridad Nacional; Infraestructuras críticas; normativa de seguridad; Equipo de respuesta a incidentes de seguridad; telecomunicaciones y usuarios; Ciberdelincuencia, Protección de Datos; y relaciones con la Administración.

- **Ámbitos de la seguridad Nacional - Ciberseguridad:** Incluye normativa sobre Protección de Datos; ciberamenazas y seguridad en el Ciberespacio - cooperación en materia de seguridad; Infraestructuras Críticas en España; y uso eficiente de las Tecnologías de la Información.

RESUMEN FINAL

Como resumen, podemos llegar a afirmar que la Ciberseguridad ya no es una disciplina ajena al **cumplimiento normativo,** sino que, para muchas organizaciones, es un requisito específico de cumplimiento, **de forma directa,** y un facilitador de otras obligaciones normativas, **de forma indirecta.**