Vicente Moret Millás
Letrado de las Cortes Generales y 'Of Counsel' de Andersen Tax & Legal

Coronavirus y ciberseguridad

La irrupción de un evento inesperado como la epidemia de COVID-19, un cisne negro, está poniendo de manifiesto muchas perspectivas distintas de abordar un problema sanitario que ya se ha convertido en una crisis de seguridad nacional. Si algo se está poniendo de relieve es la relevancia de que los mecanismos jurídicos y administrativos de actuación de los Estados ante emergencias de este calibre estén preparados y dispuestos con antelación para poder responder con eficacia.

En los Estados actuales el concepto de Seguridad Nacional y el sistema institucional responsable, tienen por objeto implementar políticas públicas que contemplen de forma integral la seguridad en todas sus perspectivas.

Las interconexiones entre los distintos ámbitos que afectan a la seguridad nacional se están poniendo en evidencia en esta crisis del COVID-19, en la cual una crisis de seguridad sanitaria también debe ser abordada por sus consecuencias para la seguridad económica, o para el orden público o para la seguridad alimentaria.

En definitiva, se trata de proteger de forma completa la esfera de derechos y libertades de los ciudadanos españoles en cada uno de los ámbitos de especial interés que se señalan en la Estrategia de Seguridad Nacional.

Uno de los enfoques que merece especial atención en este contexto complejo y convulso es el de la ciberseguridad. Como consecuencia de la declaración de estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 muchas organizaciones y empresas están implantando sistemas de gestión del trabajo utilizando las herramientas digitales que las IT han puesto a nuestro alcance y que eran impensables hasta hace algunos años.

Las que ya utilizaban estas formas de trabajar con asiduidad antes de la crisis sanitaria, probablemente tenían unos sistemas de comunicaciones y de gestión bien diseñados y que contemplan la ciberseguridad como un factor determinante a la hora de implantar esta forma de trabajar. Otras, en cambio, no habían pre-

visto que este modelo de trabajo *online* podría implantarse masivamente de forma repentina, y probablemente la ciberseguridad no forma parte de las preocupaciones centrales a la hora de dar respuesta a la necesidad de seguir con la actividad de gestión.

Por ello, el CCN organismo dependiente del CNI, ha lanzado en los últimos días varias recomendaciones para evitar que este uso masivo de sistemas de trabajo *online* pueda favorecer las intrusiones, la difusión de *malware*, la desinformación o cualquier otro tipo de actividad maliciosa que pueda derivar en ciberincidentes graves.

Este es el momento en el cual debe insistirse en la importancia, a la hora de prevenir riesgos y de mitigar posibles responsabilidades, de que empresas y organizaciones dispongan de normas internas y protocolos que permitan afrontar estos *riesgos cíber* con garantías de que la gestión de los mismos se lleva a cabo con la debida antelación y preparación. Es evidente que para ello las herramientas tecnológicas son fundamentales.

No obstante, estos ataques se basan casi siempre en mecanismos de ingeniería social, y ello supone la necesidad de aumentar la resiliencia de las organizaciones y las personas que son objeto de esos ataques. La política de ciberseguridad de una empresa u organización se debe concretar con la elaboración y establecimiento de normas de uso interno que recojan principios, procedimientos y obligaciones a las que están sujetas todas las personas integradas.

Es momento de insistir en la importancia de contar con normas internas para afrontar los 'riesgos cíber' con garantías

Las herramientas normativas de obligado uso interno con contenido jurídico pueden crear una serie de pautas preventivas y también reactivas contra el fraude en internet. Además, sirven para alinear y unificar criterios, y para atribuir de forma clara responsabilidades y funciones en caso de ciberincidentes.

Si bien existen muchas recomendaciones generales en esta materia comúnmente aceptadas como útiles, es necesario realizar un esfuerzo por adaptar esas recomendaciones a los fines y características de cada organización específicamente. Los principios que deben inspirar la redacción de estas normas internas serían, entre otros, la simplicidad, el compromiso con la seguridad, la responsabilidad, la estandarización de procesos, la formación, o la generación de confianza.

El contenido mínimo de esas normas internas debería consistir en una serie de regulaciones sobre aspectos tales como verificación de identidad; alertas; usos no aceptables; notificaciones de incidentes; uso de dispositivos personales, wifis, o contraseñas, entre otros. Todos estos aspectos deberán ir respaldados por las correspondientes medidas sancionadoras en caso de incumplimiento grave.

En definitiva, una buena regulación interna de los procesos internos en esta materia puede ser un efectivo medio para prevenir y también focalizar a toda la organización de forma homogénea en torno a normas comunes y criterios de actuación compartidos.

Para que estas normas sean efectivas es necesario que toda la organización esté implicada en el cumplimiento de estas normas, desde los máximos niveles de dirección hasta la misma base de la organización.

Estas normas de uso interno pueden ser una poderosa herramienta para aunar esfuerzos de forma coherente y asegurar ese compromiso con la ciberseguridad. Como está demostrando esta crisis del COVID-19, no podemos preocuparnos de las situaciones extraordinarias cuando ya han llegado, sino que hemos de prepararnos para gestionarlas cuando aún no se han producido.