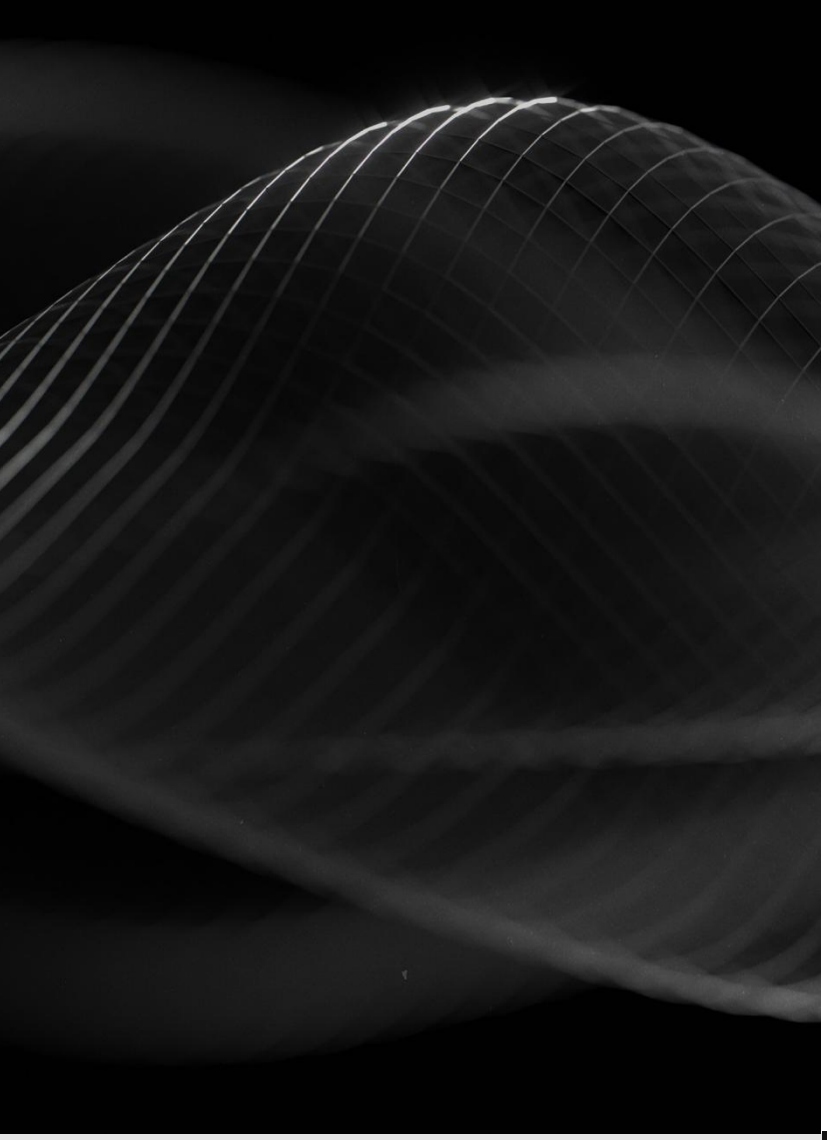

ECIJA

NOTA INFORMATIVA

El apagón y la resiliencia de estructuras críticas

Un problema en el sistema eléctrico general español, ocasionado en la infraestructura de Red Eléctrica, deja a oscuras toda la península Ibérica y el sur de Francia, haciendo colapsar por horas los sistemas y redes de gran parte de las entidades del tejido institucional y empresarial del país.

A la hora de extraer lecciones aprendidas, una conclusión es clara; en la sociedad digital actual, adoptar medidas que aseguren un elevado nivel de resiliencia digital desde la óptica de la ciberseguridad se antoja crucial.

Uso público

Las conclusiones en un vistazo,

- La caída generalizada del sistema eléctrico sufrida era imprevisible, si bien, sus consecuencias a nivel de resiliencia operativa podían **mitigarse**.

- Contar con redes, sistemas de información y sistemas industriales **resilientes** ante este tipo de escenarios de riesgo es esencial para salvaguardar la información en las entidades, tanto públicas, como privadas.

- Las medidas de protección en materia de ciberseguridad deben contemplar, también, **medidas de protección física y ambientales**, como planes de contingencia que contemplen escenarios de pérdida de la fuente de alimentación, la redundancia de los sistemas o la gestión de copias de respaldo y recuperación.

- En la UE, contamos con distintos **marcos jurídicos** a nivel de ciberseguridad cuyo cumplimiento asegura un alto nivel de protección.

Un problema como el sufrido el pasado día 28 de abril en la red eléctrica española que dejó sin luz a la península Ibérica y sur de Francia era imprevisible, si bien, a nivel de resiliencia operativa, podían haberse mitigado sus consecuencias.

Es crucial, por ello, entender la **ciberseguridad como un eje integral en las entidades**, tanto públicas como privadas, cuya función es la de dotar de herramientas adecuadas que aseguren que sus redes y sistemas, así como la información que se maneja en ellos, se encuentren protegidos, no solo frente a ataques cibernéticos, sino también ante amenazas de carácter físico y ambiental, como es en este el corte del suministro eléctrico. Es común concebir la ciberseguridad como algo centrado en la esfera digital. Sin embargo, hablar de ciberseguridad, en la Sociedad Digital actual, supone incluir en la ecuación, también, la protección de los centros de datos, dispositivos, servidores y demás activos de carácter tangible que soportan toda la infraestructura digital. En definitiva, es esencial garantizar la adopción de medidas de protección físicas **para asegurar la continuidad operativa y la integridad de los sistemas digitales ante escenarios de potencial riesgo que aseguren en última instancia la protección del activo más importante de las entidades, tanto públicas, como privadas; la información**.

Términos como los planes de contingencia, la redundancia de los sistemas o la gestión de copias de seguridad y recuperación no son ajenos a la ciberseguridad, y diferentes normativas a nivel europeo ya los emplean dentro del catálogo de obligaciones y medidas tendentes al fortalecimiento de la resiliencia digital de las entidades incluidas en sus ámbitos de aplicación.

Estos controles deben formar parte de un enfoque integral de gestión de riesgos, garantizando la resiliencia operativa **frente a amenazas físicas** que puedan comprometer la disponibilidad, integridad, autenticidad o confidencialidad de la información manejada.

A día de hoy, existen en la Unión Europea ("**UE**") diferentes marcos jurídicos que configuran un nivel de ciberseguridad sólido en distintos sectores de la economía. Entre ellos, destacan:

- **Directiva (UE) 2022/2555, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (o "NIS 2") :** presenta un conjunto de sectores considerados como "críticos", y ofrece requisitos estrictos en gestión de riesgos tecnológicos, notificación de incidentes y gobernanza interna que deberán reunir las entidades de los mismos, todo ello fortalecido por una mejora en la cooperación entre Estados miembros mediante mecanismos de coordinación y supervisión más eficaces. Su ámbito de aplicación se extiende a sectores esenciales como pueden ser el de la energía, transporte, infraestructuras digitales, salud, agua potable y gestión de residuos, entre otros. Proteger estos sectores es crucial porque sustentan el funcionamiento de la sociedad y la economía, y una interrupción o ciberataque contra ellos podría tener efectos devastadores sobre la seguridad, el orden público o la salud de la población.

- **Reglamento (UE) 2022/2554, sobre la resiliencia operativa digital del sector financiero (o "DORA):** centrado en la regulación de la ciberseguridad en un sector altamente expuesto a la dependencia de la digitalización, como es el sector financiero, en el cual los sistemas de pagos digitales han desplazado al tradicional metálico. Sus disposiciones ofrecen una serie de medidas que sitúan a las redes y los sistemas del entramado financiero entre los más altamente resilientes, permitiendo dotar a las entidades del sector de una alta resistencia frente a eventuales amenazas. Al integrar estos elementos dentro de los planes de continuidad, resiliencia y pruebas (como las pruebas de penetración basadas en amenazas "**TLPT**"), DORA obliga a proteger también el componente físico frente a sabotajes, desastres naturales o accesos no autorizados, lo que refuerza la seguridad integral del ecosistema financiero.

- **Directiva (UE) 2022/2557, relativa a la resiliencia de las entidades críticas (o "CER"):** obliga a los Estados miembros a identificar entidades críticas en sectores clave e infraestructuras esenciales. Estas entidades deben implementar medidas para prevenir, resistir, responder y recuperarse de incidentes que afecten su operativa. También deben realizar evaluaciones de riesgos físicos y operativos, incluyendo amenazas naturales, humanas o tecnológicas. Además, impone obligaciones de notificación de incidentes y cooperación con autoridades nacionales.

Teniendo en cuenta este contexto, el desarrollo de un sistema de gestión de ciberseguridad en entidades relevantes (y en cualquier otra) se hace totalmente necesario en la sociedad actual. Las previsiones normativas y las referencias a estándares internacionales hacen, sin duda que las empresas sean mas resilientes y seguras.

Área de Protección de Datos y ciberseguridad de ECIJA

info@ecija.com

Telf: + 34 91.781.61.60