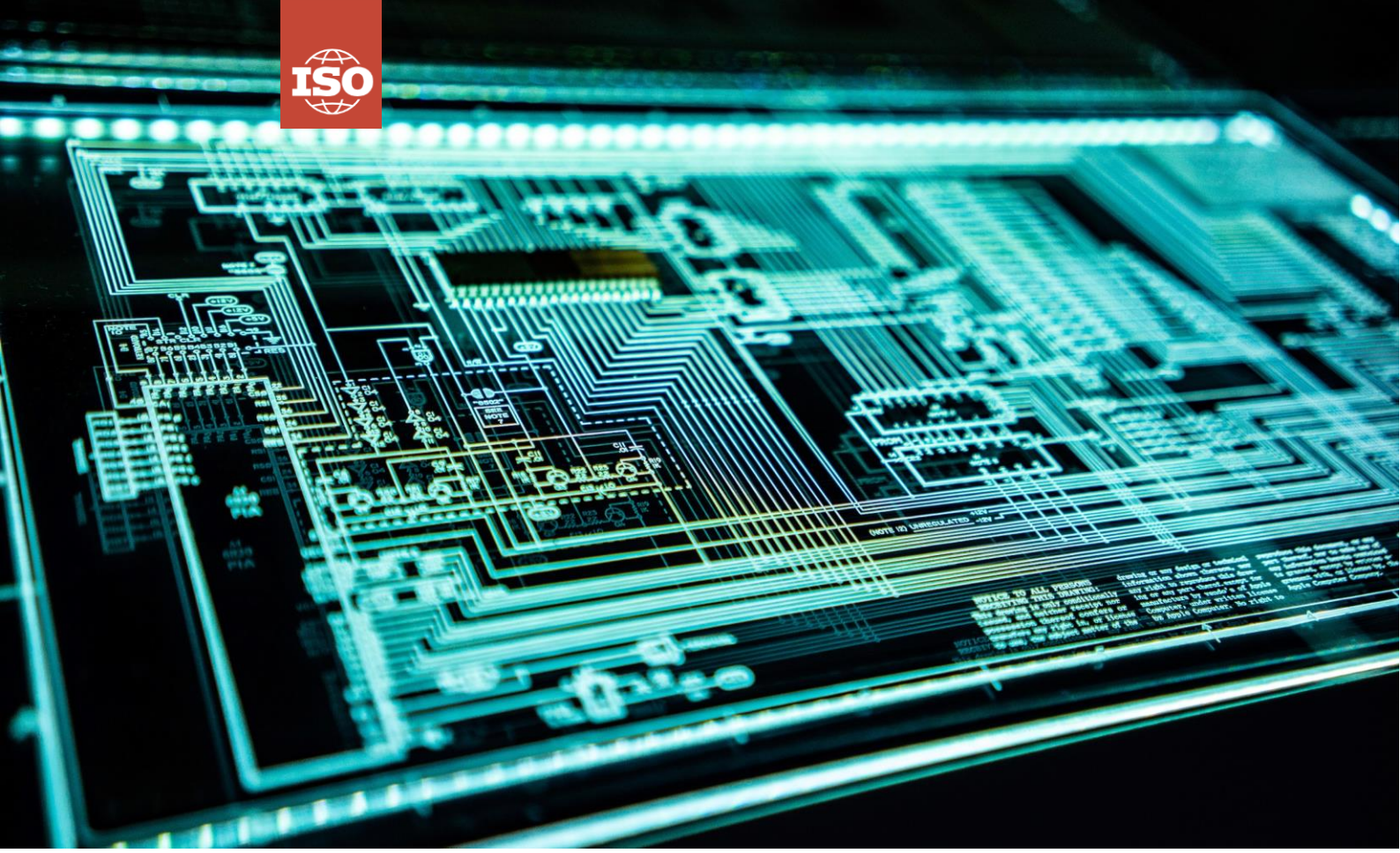
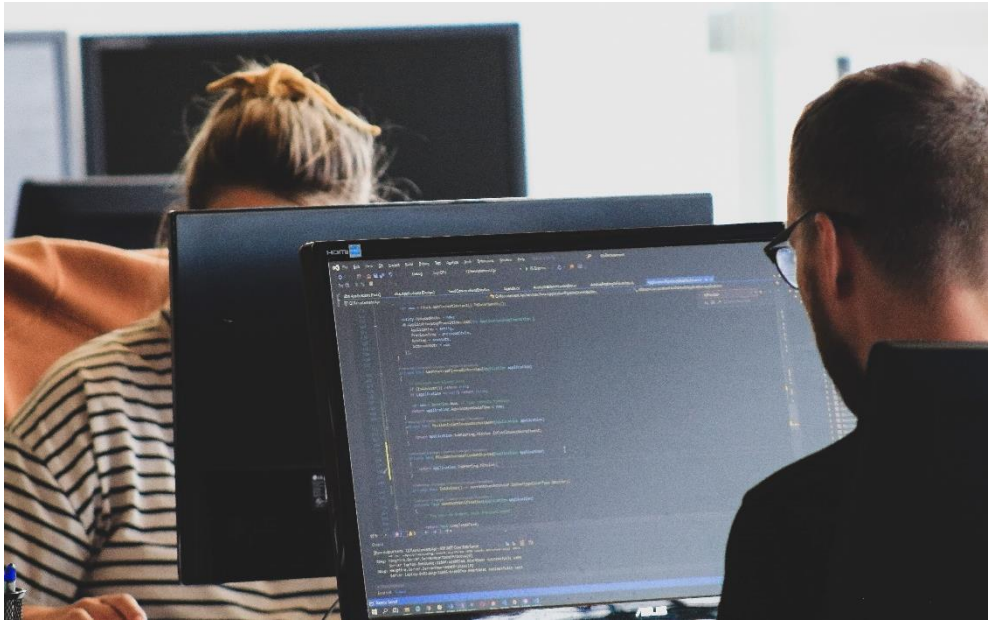


DE CÓMO LOS GIGANTES TECNOLÓGICOS DESARROLLAN LA CIBERRESILIENCIA

La desconfianza nos arrastra a estigmas que nos limitan, pero las Normas Internacionales pueden ayudarnos a ser vulnerables con confianza y resilientes.

¿Qué tienen en común Microsoft, Apple, Google, Intel e IBM? Además de ser empresas Fortune 500, todos estos gigantes

tecnológicos aplican la norma ISO/IEC 27001. Con una aceptación global cada vez mayor y con su presencia en miles de emplazamientos de todo el mundo, ISO/IEC 27001 se ha convertido en la norma de facto para los sistemas de gestión de la seguridad de la información.



A la hora de proteger sus activos de datos críticos frente a las amenazas y vulnerabilidades digitales, las organizaciones deben adoptar una mentalidad ciberresiliente. La ciberresiliencia debe ser un componente integrante no solo de los sistemas técnicos, sino también de los equipos humanos, la cultura de la organización y las operaciones diarias. De hecho, los líderes empresariales son hoy mucho más conscientes de las ciberamenazas que el año precedente. Como reflejan las Perspectivas de la seguridad mundial 2023 del Foro Económico Mundial (FEM), el 91 % de los encuestados consideró que un acontecimiento cibernético catastrófico y de amplio alcance es «al menos algo probable durante los próximos dos años».

Empresas de todo el mundo responden a estas presiones implementando ISO/IEC[1] 27001, la norma más conocida del mundo referida a los sistemas de gestión de la seguridad de la información (SGSI). Se trata de un conjunto documentado de políticas, procedimientos, procesos y sistemas que gestiona los riesgos de pérdida de datos por ciberataques, intrusiones, fugas de datos o sustracciones.

> Las organizaciones deben adoptar una mentalidad ciberresiliente.

¿En qué consiste la ciberresiliencia?

La ciberresiliencia es la capacidad de una organización para operar frente a un ciberataque u otro incidente cibernético. Supone implementar las medidas técnicas y organizativas necesarias para detectar, responder y recuperarse de este tipo de incidentes, junto con la capacidad para adaptarse y aprender de ellos para mejorar la capacidad de recuperación en el futuro.

«La ciberresiliencia es la que toma el control cuando las medidas de prevención de la seguridad flaquean», afirma Andreas Wolf, que encabeza el grupo de expertos responsables de las normas de seguridad de TI de ISO/IEC. «En esta economía digital, la capacidad de trascender las disrupciones cibernéticas es lo que diferencia a los campeones del mercado. Las organizaciones capaces de

---

[1] ISO/IEC 27001 se publica conjuntamente con la Comisión Electrotécnica Internacional (IEC).

convertir la vulnerabilidad en fortaleza podrán asumir con confianza un nivel de riesgo saludable».

Para Wolf, la seguridad no es un tema nuevo. Él y su equipo son los responsables de la nueva y mejorada versión de ISO/IEC 27001, publicada en octubre del año pasado para abordar los desafíos mundiales de la seguridad informática e impulsar la confianza digital. Beneficia a las organizaciones al animarlas a proteger todas las formas de información, desarrollar un marco administrado centralmente, reducir el gasto en tecnología de defensa ineficaz y proteger la integridad, la confidencialidad y la disponibilidad de sus datos.

Sin embargo, la resiliencia no solo se refiere al funcionamiento interno de las organizaciones: debe aplicarse en todas las alianzas con terceros y a toda la cadena de suministro. Afortunadamente, el libro blanco Índice de ciberresiliencia (CRI): impulso a la ciberresiliencia organizativa, también publicado por el FEM, pretende servir como marco de referencia para brindar visibilidad y transparencia acerca de las prácticas de ciberresiliencia en todas las industrias, los pares y la cadena de suministro.

El CRI proporciona a los líderes cibernéticos de los sectores público y privado un marco común de buenas prácticas para una genuina ciberresiliencia, un mecanismo para medir el desempeño de la organización y un lenguaje claro para comunicar su valor. Siguiendo los principios del CRI, las prácticas y subprácticas consiguientes para una ciberresiliencia saludable organizativa supone el uso de marcos de seguridad reconocidos y normas industriales tales como ISO/IEC 27001.

La vulnerabilidad como pilar de la resiliencia

Ser transparentes acerca de las prácticas internas y compartir información con competidores y legisladores puede hacer que las organizaciones se sientan vulnerables, pero es justo esta vulnerabilidad la que conducirá a una genuina colaboración y al progreso.

> En la era digital, no podemos permitirnos poner en riesgo la ciberresiliencia.

En la era digital, no podemos permitirnos poner en riesgo una ciberresiliencia que, además, se fundamenta en claras razones empresariales. Las organizaciones que apuestan por la ciberresiliencia a través de una vulnerabilidad de confianza emergen rápidamente como líderes de sus respectivas industrias y marcan la pauta en sus ecosistemas. El planteamiento holístico de la norma ISO/IEC 27001 significa que toda la organización está cubierta y no solo la TI. Aporta beneficios en todos los ámbitos: personas, tecnología y procesos.