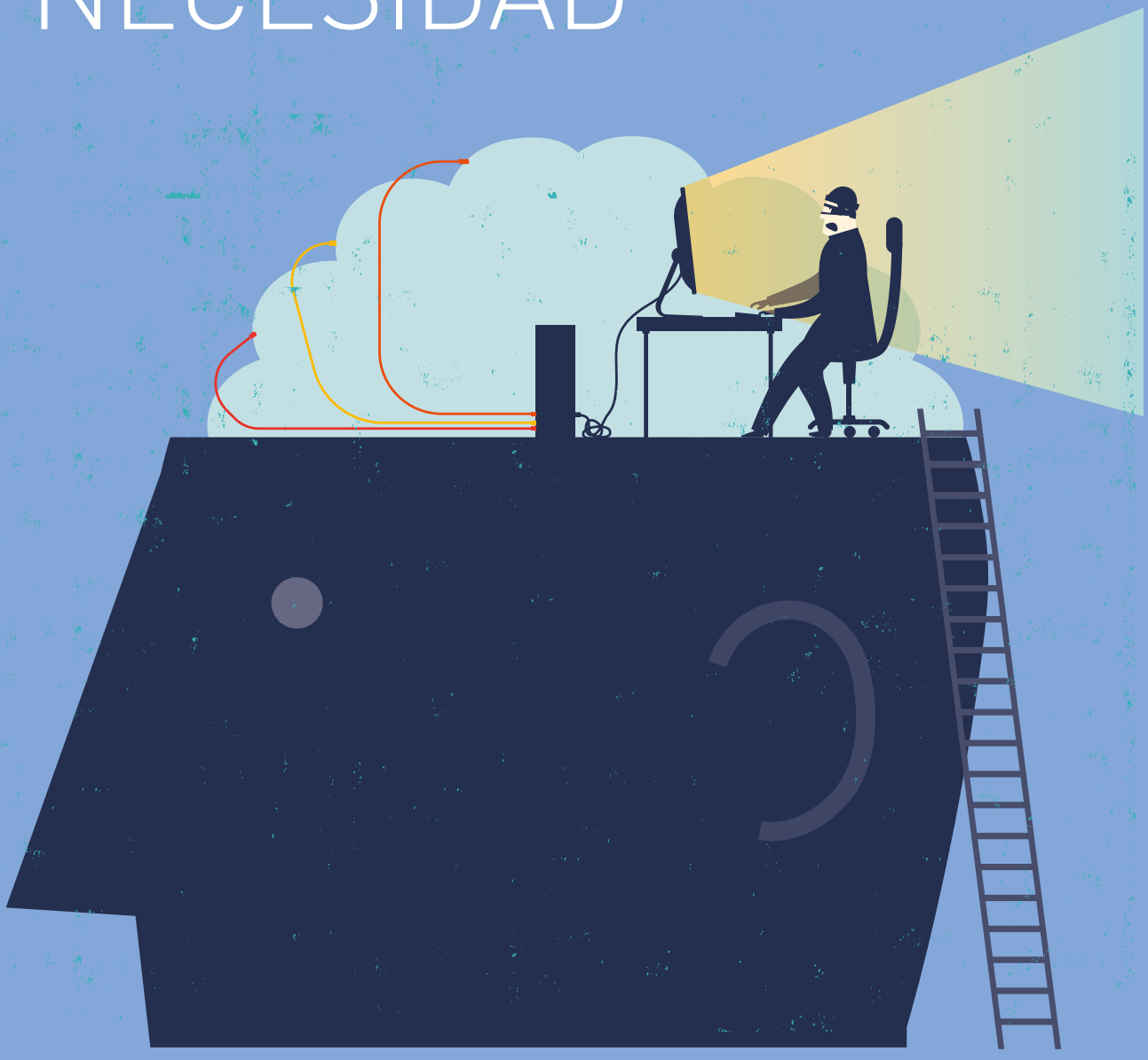
# CIBERSEGURIDAD, MÁS QUE UNA MODA, UNA NECESIDAD



PARA MÁS INFORMACIÓN,
**VISITA www.incibe.es/protege-tu-empresa**

TEXTO **DANIEL LARGACHA** | ILUSTRACIÓN **ISTOCK**

**La transformación digital nos sitúa ante una sociedad totalmente distinta. Las empresas y los ciudadanos tenemos el reto de incorporar la cultura de ciberseguridad como un eje fundamental en este nuevo escenario.**

La sociedad del siglo XXI está expuesta a una serie de cambios que bien se pueden parecer a los que anticipaban algunos libros y películas futuristas de los años 60. Lo cierto es que nadie conoce con certeza el futuro, ni lo que nos deparará, aunque sí que es posible intuir que la humanidad se encuentra muy cerca de un posible cambio de era para el que debemos estar preparados.

**LA NUEVA ERA DIGITAL NO PODRÁ ENTENDERSE SIN LA CIBERSEGURIDAD,** ENTENDIENDO ESTA COMO UN ELEMENTO NECESARIO QUE **APORTARÁ CONFIANZA Y ESTABILIDAD** A TODO EL ENTORNO DIGITAL Y, EN CONSECUENCIA, **A EMPRESAS, GOBIERNOS Y CIUDADANOS COMO PARTE DE LA SOCIEDAD.**

### ¿Cómo se adaptan las empresas?

Las empresas ya existentes tienen dos hándicaps importantes a la hora de poder adaptarse a este nuevo escenario. Por una parte, tienen que seguir prestando servicio a sus actuales clientes, con medios más tradicionales. Por otra, tienen que incorporar las nuevas tecnologías a sus procesos, que le permitirán relacionarse con el cliente digital de la actualidad y con el del futuro (los nativos digitales).

Este proceso de introducción de nuevas tecnologías en las organizaciones, la famosa transformación digital, ha provocado un mayor apalancamiento tecnológico (o dependencia de las tecnologías) de las empresas, en la medida en que cada vez los procesos internos necesarios para funcionar son más digitales y requieren de la tecnología para funcionar. Según hemos visto anteriormente la transformación digital plantea una serie de ventajas y de retos evidentes a todas las empresas, pero hay otro aspecto que es común a todas las organizaciones que está ligado al apalancamiento tecnológico y que emerge como necesario en este nuevo entorno, este es el de la ciberseguridad como elemento que preserve la tecnología de los riesgos asociadas a ésta.

## El efecto estabilizador de la ciberseguridad

De la misma forma que hoy en día no podríamos entender la sociedad sin la energía eléctrica, la nueva era digital no podrá entenderse sin la ciberseguridad, entendiendo esta como un elemento necesario que aportará confianza y estabilidad a todo el entorno digital y, en consecuencia, a empresas, gobiernos y ciudadanos como parte de la sociedad.

A pesar de que se están realizando grandes esfuerzos, la introducción de la ciberseguridad en el ecosistema tecnológico probablemente no se esté haciendo de una forma gradual. Como ha ocurrido en ocasiones anteriores en la historia de la humanidad, el grado de importancia que tome sufrirá un aumento importante una vez se vean los efectos devastadores de una ausencia o aplicación inadecuada.

La ciberseguridad es una disciplina relativamente joven, que aún es necesario desarrollar y que además siempre tendrá una dependencia directa con la tecnología (que es recíproca). La evolución de la ciberseguridad en los próximos años se pivotará en tres factores principales. El primero es el de la propia tecnología: la ciberseguridad requiere de herramientas tecnológicas que deberán adaptarse a los nuevos entornos digitales. Esta adaptación está llegando aunque a una velocidad inferior a la del resto de la tecnología, por ahora. El segundo factor es el de la regulación. La nueva economía digital no entiende de fronteras ni de aranceles y además es capaz de sortear las leyes de los países para establecerse en ámbitos no regulados que le permiten mayor libertad para operar. El tercer factor y más importante es el de las personas. No solo es importante porque la ciberseguridad va a requerir de profesionales adecuadamente formados (se espera que para el 2020 la demanda de profesionales de seguridad se incremente en un 50%), sino porque la cultura de ciberseguridad va a desempeñar un papel de mayor peso en toda la sociedad. El hecho de que cada uno de nosotros tenga una adecuada formación en ciberseguridad será un aspecto fundamental, sea para nuestro ámbito profesional, cualquiera que sea, o como ciudadanos de esta sociedad actual (como votantes, padres, contribuyentes, consumidores de productos/servicios, etc).

Por tanto, la cultura de ciberseguridad es quizá el factor más importante sobre el que se debe construir la nueva economía digital y cuanto antes empecemos a cimentarlo, menor esfuerzo nos costará abordar el cambio en lo que ya hay construido. Cada vez, como sociedad, somos más conscientes aunque ya sabemos que el ser humano tiene cierta tendencia a tropezar primero para después levantarse.

**LA CULTURA DE CIBERSEGURIDAD ES QUIZÁ EL FACTOR MÁS IMPORTANTE SOBRE EL QUE SE DEBE CONSTRUIR LA NUEVA ECONOMÍA DIGITAL** Y CUANTO ANTES EMPECEMOS A CIMENTARLO, MENOR ESFUERZO NOS COSTARÁ ABORDAR EL CAMBIO EN LO QUE YA HAY CONSTRUIDO.

SE ESPERA QUE PARA **2020** LA **DEMANDA DE PROFESIONALES DE SEGURIDAD SE INCREMENTE** EN UN **50%**

EL GRADO DE IMPORTANCIA QUE TOME LA CIBERSEGURIDAD SUFRIRÁ UN AUMENTO IMPORTANTE UNA VEZ SE VEAN LOS **EFECTOS DEVASTADORES DE UNA AUSENCIA O APLICACIÓN INADECUADA**

# DECÁLOGO
## CONCIENCIACIÓN EN CIBERSEGURIDAD EN LA EMPRESA

### 1. **PUESTO** DE TRABAJO
- Mantén la mesa limpia de papeles que contengan información sensible
- Bloquea la sesión de tu equipo cuando abandones tu puesto

### 2. **DISPOSITIVOS**
- No modifiques la configuración de tus dispositivos
- No instales aplicaciones no autorizadas
- No conectes dispositivos USB no confiables
- Establece una clave de acceso y la opción de bloqueo automático en tus dispositivos móviles

### 3. **USO DE EQUIPOS** NO CORPORATIVOS
- No manejes información corporativa en equipos públicos
- Si accedes al correo corporativo desde tu equipo personal no descargues ficheros al equipo

### 4. **FUGAS** DE INFORMACIÓN
- No facilites información sensible si no estás seguro de quién es el receptor de la misma
- Destruye la información sensible en formato papel. No la tires a la papelera

### 5. GESTIÓN DE **CREDENCIALES**
- No compartas tus credenciales de acceso (usuario y contraseña)
- No utilices tus credenciales de acceso corporativas en aplicaciones de uso personal
- No apuntes tus credenciales en lugares visibles

### 6. **NAVEGACIÓN**
- Evita acceder a páginas web no confiables
- No pinches en enlaces sospechosos. Procura escribir la dirección en la barra del navegador

### 7. **CORREO** ELECTRÓNICO
- Elimina todo correo sospechoso que recibas
- Evita los correos en cadena (reenvío de correos que van dirigidos a un gran número de personas)

### 8. PROTECCIÓN DE LA **INFORMACIÓN**
- Realiza copias de seguridad de aquella información sensible que solo esté alojada en tus dispositivos

### 9. **VIAJE** SEGURO
- Procura no trasportar información sensible en dispositivos extraíbles. Si lo haces, cifra la información
- No manejes información sensible en redes WIFI no confiables

### 10. **ERES SEGURIDAD**
- Si detectas cualquier actividad sospechosa o un funcionamiento anómalo de tu equipo, avisa al departamento de seguridad

Fuente: INCIBE, Instituto Nacional de Ciberseguridad (España)