



## INCIBE – INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 21 de diciembre de 2018.- [El Instituto Nacional de Ciberseguridad \(INCIBE\)](#) tiene como misión reforzar la ciberseguridad, la confianza y la protección de la privacidad en los servicios de la Sociedad de la Información, aportando valor a ciudadanos, empresas, Administración, al sector de las tecnologías de la información y las comunicaciones y sectores estratégicos en general. INCIBE elabora para los medios informativos un boletín semanal, con el fin de colaborar conjuntamente en la difusión de la seguridad de la información.

### Menores de edad y la publicidad en Internet

La publicidad forma parte de nuestro día a día, también en Internet. Tanto es así que en ocasiones resulta difícil distinguir si un contenido es o no un anuncio. Dado que los menores son más vulnerables a los riesgos relacionados con los contenidos comerciales, hemos de ayudarles a reducir su exposición a los mismos en línea, así como a saber identificar los anuncios y analizarlos críticamente.

Algunas de las recomendaciones para mantener una exposición equilibrada y saludable ante la publicidad pasan por fomentar la capacidad crítica de los menores y hacerles conscientes de las estrategias publicitarias, utilizar bloqueadores de anuncios, decantarse por espacios en Internet libres de publicidad o publicidad menos abusiva, evitar la publicidad personalizada, fomentar el consumo responsable en el hogar y limitar los tiempos de uso de pantallas.

### Primeros pasos para mejorar la seguridad de nuestros datos

Las formas de ataque que pueden utilizar los ciberdelincuentes son muy variadas. En muchas ocasiones se aprovechan de nuestro desconocimiento para perpetrar sus ataques a nuestros dispositivos sirviéndose de técnicas de ingeniería social. Es por ello que debemos estar siempre atentos mientras navegamos o utilizamos dispositivos o servicios en Internet.

A pesar de esto, no hay que preocuparse en exceso ni dejar de utilizar Internet, siempre que utilicemos nuestro sentido común y tengamos en mente una serie de pautas y buenas prácticas en materia de ciberseguridad: analizar las descargas y dispositivos que conectemos a nuestro equipos con un antivirus, comprobar las páginas y los correos antes de dar información confidencial, mejorar la seguridad de nuestras

Esta información no puede ser usada en parte o en su integridad sin necesidad de citar fuentes.





contraseñas, actualizar nuestros dispositivos, tener cuidado con las modas y mantenerse al día con las noticias de ciberseguridad.

### Que un desastre no te detenga, elabora un plan de continuidad de negocio

Incendios, cortes en el suministro eléctrico, actos vandálicos, ataques informáticos o fugas de información. Diariamente una empresa puede verse afectada por multitud de escenarios que hagan peligrar la continuidad del negocio. Para evitar que uno de los sucesos anteriores, u otro cualquiera, reduzca la actividad empresarial o incluso llegue a detenerla, será de suma importancia elaborar un plan de continuidad de negocio.

Existen varios aspectos a tener en cuenta a la hora de elaborar este plan: determinar su alcance, definir responsables, realizar un análisis de impacto en el negocio, política de comunicación y aviso a entidades externas, definir la estrategia de continuidad, desarrollar actividades de entrenamiento y verificación y establecer la caducidad del plan.

### Sigue estas recomendaciones para almacenar tu información en la nube

La nube se ha convertido en una de las herramientas más utilizadas por organizaciones de cualquier tamaño y sector. Uno de los diferentes usos que se le puede dar a esta, es como medio de almacenamiento de información, bien sea como sistema de almacenamiento de copias de seguridad o como sistema de almacenamiento de información. Las ventajas de utilizar este tipo de servicios son diversas como la descentralización, el acceso desde cualquier ubicación con acceso a Internet o el ahorro de recursos. El mayor inconveniente de estos servicios es que la información deja de estar almacenada internamente y se guarda en el servicio contratado. Antes de comenzar a utilizar un servicio cloud es recomendable elaborar una política de almacenamiento en la nube siguiendo las recomendaciones que ofrece INCIBE.

### Cifrado seguro de correo electrónico con PGP

Hoy en día, el correo electrónico se ha convertido en una herramienta imprescindible en la vida personal y profesional. Así mismo, cada vez es más habitual que la información que se desea intercambiar sea confidencial y requiera, por tanto, de un medio seguro de comunicación entre las partes.

Una forma sencilla de conseguir esto es mediante el cifrado del mensaje. Para ello se puede utilizar alguna de las herramientas disponibles, como

Esta información no puede ser usada en parte o en su integridad sin necesidad de citar fuentes.





por ejemplo PGP, cuyo objetivo es mantener la confidencialidad, integridad y autenticidad en las comunicaciones que se realicen a través del correo electrónico, protegiendo la información mediante el uso de criptografía de clave pública.



Para más información en materia de Ciberseguridad visite INCIBE [www.incibe.es](http://www.incibe.es), Protege tu Empresa <https://www.incibe.es/protege-tu-empresa>, OSI [www.osi.es](http://www.osi.es) e IS4K [www.is4k.es](http://www.is4k.es).

Esta información no puede ser usada en parte o en su integridad sin necesidad de citar fuentes.

[comunicacion@incibe.es](mailto:comunicacion@incibe.es)

[www.incibe.es](http://www.incibe.es)



Av. José Aguado 41 / 24005 León  
T. (+34) 987 877 189 / F. (+34) 987 261 016