

INCIBE – INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 5 de diciembre de 2019.- El Instituto Nacional de Ciberseguridad (INCIBE) es un organismo dependiente del Ministerio de Economía y Empresa a través de la Secretaría de Estado para el Avance Digital, consolidado como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos y empresas. Además, es un instrumento para la transformación social y oportunidad para la innovación, fomentando la I+D+i y el talento.

INCIBE centra sus esfuerzos en la prestación de servicios públicos de prevención, concienciación, detección y respuesta ante incidentes de seguridad, adaptándose a cada público específico (menores, ciudadanos y empresas), así como al desarrollo de tecnología y herramientas que permiten identificar, catalogar y analizar dichos incidentes.

Navegación segura y privada para ti y tu empresa. Parte II

La semana pasada, INCIBE, desde Protege tu Empresa, publicó un artículo que proporcionaba pautas a las empresas para configurar correctamente las actualizaciones automáticas, las ventanas emergentes y el almacenamiento de contraseñas.

Esta semana, en la segunda parte, se tratan los riesgos asociados a la utilización incorrecta de *Javascript*, *Flash* y las *cookies*. ¿Cómo se definen estos conceptos? ¿Cómo se deben configurar para que una empresa pueda usarlos de forma segura?

Más información en: <https://www.incibe.es/protege-tu-empresa/blog>.

¿Sabías que los ataques de ingeniería social suponen un 93% de las brechas de seguridad?

La ingeniería social es una técnica usada por los ciberdelincuentes que consiste en engañar o manipular a las personas para conseguir información personal, como contraseñas y datos bancarios, o para obtener acceso a equipos con el fin de instalar *software* malicioso o *malware* de forma inadvertida.

De esta forma, INCIBE, a través de la Oficina de Seguridad del Internauta (OSI), proporciona recomendaciones a los usuarios para evitar ser víctimas de este tipo de engaños, como desconfiar de los chantajes o extorsiones.

Más información en: <https://www.osi.es/es/actualidad/blog>.



Protección del puesto de trabajo. Escenarios de riesgo

En multitud de ocasiones, tendemos a relacionar la ciberseguridad de una empresa con grandes inversiones en la implantación de medidas tecnológicas orientadas a la protección de la información: sistemas de detección de intrusos, controles de acceso a las instalaciones, salas de servidores, *firewalls*, etc.

Sin embargo, hay que tener en cuenta que, cuando hablamos de ciberseguridad, la pieza fundamental es el usuario. Por ello, es de vital importancia invertir en la formación y concienciación del personal de una empresa.

Más información en: <https://www.incibe.es/protege-tu-empresa/blog>.



Línea de ayuda

EN CIBERSEGURIDAD



INSTITUTO NACIONAL DE CIBERSEGURIDAD

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

Esta información puede ser usada en parte o en su integridad citando la fuente.

