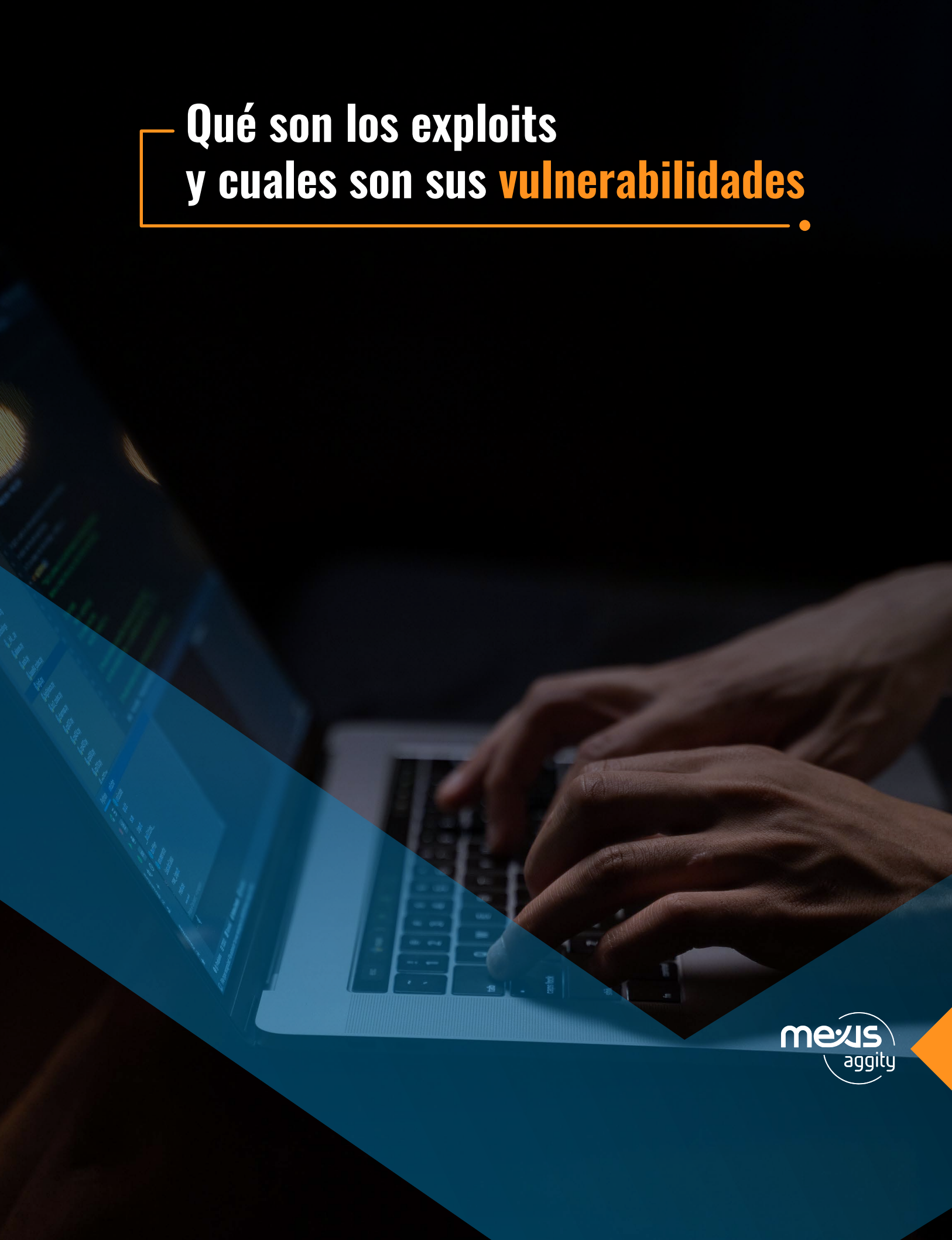
Qué son los exploits y cuales son sus vulnerabilidades



nexus aggity

Los exploits son riesgo permanente y uno de los retos presentes en la agenda de trabajo de los analistas de seguridad informática. La responsabilidad asumida para garantizar la eficacia de la seguridad de la información en una empresa queda comprometida por estos elementos, programables o no, de naturaleza diversa.

Surgen como aplicaciones informáticas, fragmentos de código o secuencias de comandos o procedimientos de ingeniería social aplicados a explotar una vulnerabilidad. A partir de ella es posible un uso no previsto o criminal del sistema sobre el que actúan.

Los exploits, en sus distintos tipos, están determinados por el software al que van dirigidos. Es decir, son específicos para una versión determinada de un sistema operativo o programa. Un malware se crea con una o varias secuencias de código de este tipo. Busca obtener un objetivo no contemplado por los diseñadores de la aplicación atacada.
Un código malicioso vence si logra la capacidad de alcanzar privilegios que rompan los controles de acceso a información reservada o confidencial. Siempre es el resultado de un conocimiento detallado de las características técnicas del sistema atacado, los sistemas de protección y control, y la forma habitual de operar del personal encargado. Es decir, descubren un punto débil explotable para acciones desautorizadas o ajenas a los fines de la organización.
Las acciones de naturaleza delictiva en la red se han profesionalizado mucho. Están al nivel de contar con recursos para combinar varias vulnerabilidades en un solo ataque. Así, forman verdaderos kits de fragmentos de código que hacen un examen minucioso de las posibles puertas abiertas para poner en riesgo servicios estratégicos o de información.

Cómo luchar contra las vulnerabilidades de un sistema

Las siguientes medidas son básicas para defender a un sistema informático de ataques.

1. Documentación completa y actualizada de las características técnicas del sistema, procesos aplicados y de los roles de las personas con permisos para acceder, editar información o hacer cambios definitivos en la infraestructura.

2. Usar siempre versiones actualizadas de software y mantener un contacto fluido con los responsables internos o externos de su desarrollo. Las actualizaciones de seguridad cumplen la función de prevenir un acceso no autorizado, la disposición fraudulenta de datos y el mantenimiento de la eficacia de los servicios de información.

3. Estar al corriente de alertas en sistemas parecidos al propio con la obligación de custodiar.

4. Establecer protocolos de actuación que describan de forma precisa las medidas emprendidas para la defensa de los recursos de la empresa hasta la vuelta a la normalidad.

El papel de las copias de seguridad en la nube para empresas
Las pérdidas económicas por destrucción de información o paralización de la actividad derivadas del mal funcionamiento de un sistema informático son letales para una compañía. Los planes de contingencia evalúan estos riesgos, también disponen de los medios necesarios para mitigarlos o para lograr su máxima atenuación.

Las copias de seguridad en la nube para empresas son el medio ideal a la hora de disfrutar de una capa adicional de seguridad. También los planes de disaster recovery para empresas. Además, facilitan el acceso con distintos dispositivos al sistema de información con un mínimo coste de mantenimiento.

El backup en la nube colabora en la adquisición de una visión integrada de herramientas, procesos y personal implicados. Para las tecnologías de datos la actualización permanente es un respaldo imprescindible para emprender con confianza otras iniciativas.

En definitiva, los exploits ponen de manifiesto que en los sistemas operativos y aplicaciones existen fallos o defectos de diseño. La rapidez con las que emprenden acciones para corregir sus efectos crece cada día. Por eso, las inversiones en seguridad descubren su valor cuando se mantiene en el tiempo el funcionamiento normal de un sistema.

Fuente de infomación: datos101.com