

Informe de Seguridad

Autores:

Nawal Boukarssanna Bouazaoui

Paula Victoria Carrascosa Mancilla

Alejandro Terrazas Vargas



Índice

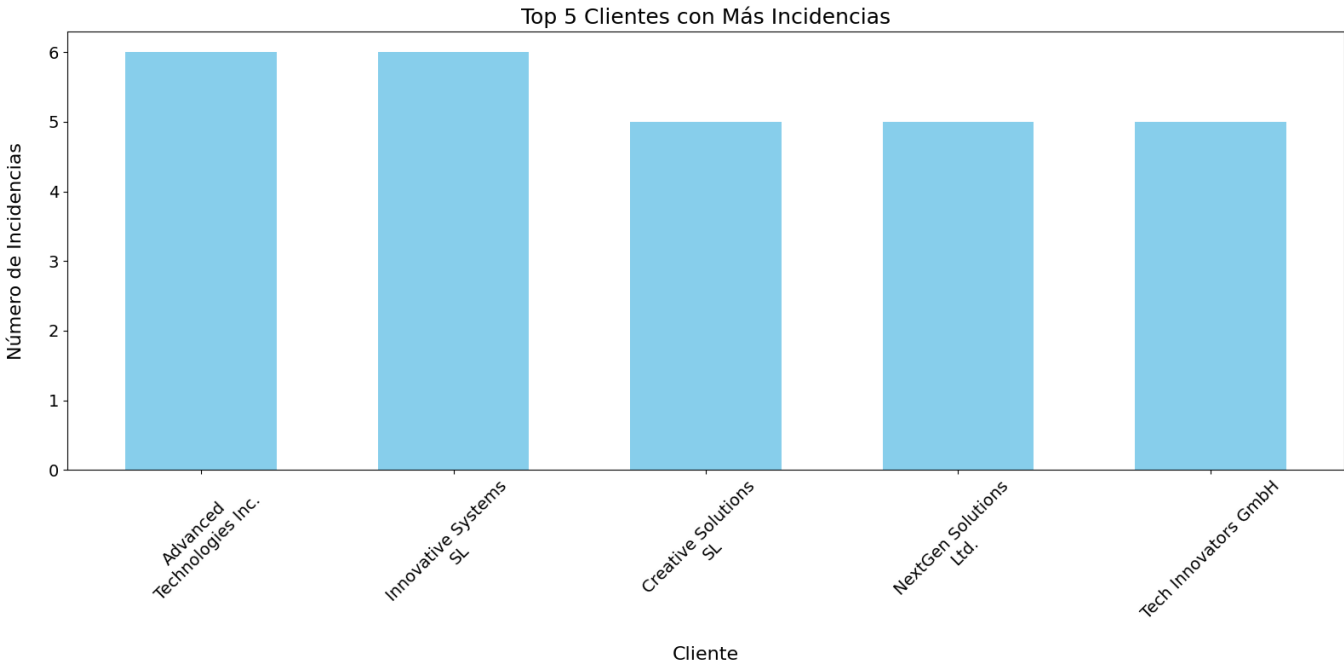
Top 5 Clientes con más Incidencias - Página 3

Top 5 Tipos de Incidencias por Tiempo Promedio - Página 3

Top 10 Vulnerabilidades Más Frecuentes - Página 3

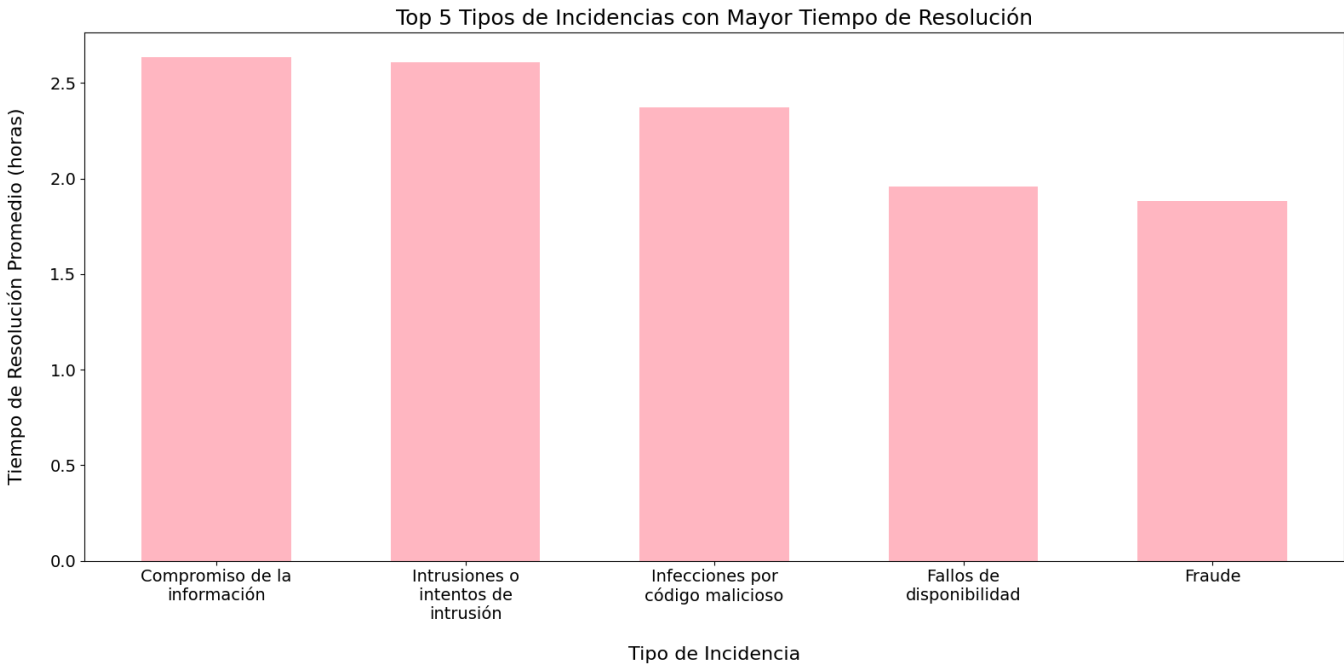
Top 5 Clientes con más Incidencias

Cliente	Incidencias
Advanced Technologies Inc.	6
Innovative Systems SL	6
Creative Solutions SL	5
NextGen Solutions Ltd.	5
Tech Innovators GmbH	5



Top 5 Tipos de Incidencias por Tiempo Promedio

Tipo de Incidencia	Tiempo Promedio (horas)
Compromiso de la información	2.63
Intrusiones o intentos de intrusión	2.61
Infecciones por código malicioso	2.37
Fallos de disponibilidad	1.96
Fraude	1.88



Top 10 Vulnerabilidades Más Frecuentes

ID del CVE	Descripción
CVE-1999-0095	The debug command in Sendmail is enabled, allowing attackers to execute commands as root.
CVE-1999-0082	CWD ~root command in ftpd allows root access.
CVE-1999-1471	Buffer overflow in passwd in BSD based operating systems 4.3 and earlier allows local users to gain root privileges by specifying a long shell or GECOS field.
CVE-1999-1122	Vulnerability in restore in SunOS 4.0.3 and earlier allows local users to gain privileges.
CVE-1999-1467	Vulnerability in rcp on SunOS 4.0.x allows remote attackers from trusted hosts to execute arbitrary commands as root, possibly related to the configuration of the nobody user.
CVE-1999-1506	Vulnerability in SMI Sendmail 4.0 and earlier, on SunOS up to 4.0.3, allows remote attackers to access user bin.
CVE-1999-0084	Certain NFS servers allow users to use mknod to gain privileges by creating a writable kmem device and setting the UID to 0.
CVE-2000-0388	Buffer overflow in FreeBSD libmytinfo library allows local users to execute commands via a long TERMCAP environmental variable.
CVE-1999-0209	The SunView (SunTools) selection_svc facility allows remote users to read files.
CVE-1999-1198	BuildDisk program on NeXT systems before 2.0 does not prompt users for the root password, which allows local users to gain root privileges.

