MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

Hallazgos relevantes

Los resultados del total de 226 instituciones analizadas:

● 188 instituciones NO cuentan con personal especializado en Ciberseguridad que administren los sistemas.

● 28 instituciones tienen sistemas desarrollados por terceros, pero NO contemplan aspectos de seguridad.

● 41 instituciones NO realizan copias de seguridad de los sistemas que tienen alojados por un tercero.

● De los sistemas que se encuentran administrados por terceros el 28.8% (65 instituciones) no cuentan con un registro de la actividad que realizan los administradores en sus sistemas.

● Existen 38 instituciones que no han implementado sistemas de protección y seguridad DNS.

● 104 (46%) instituciones no poseen sistemas de protección EDR

● 43.8%, 99 instituciones NO han implementado doble factor de autenticación en sus sistemas.

● 38.9%, 88 instituciones tienen sistemas operativos fuera de soporte, sin embargo, ese número es mayor ya que muchas indicaron que solo tenían unos pocos equipos, por lo que el porcentaje aumenta a casi un 50%.

● 94 (41.6%) instituciones NO han realizado auditorías de seguridad en sus servidores.

● 51 instituciones NO tienen políticas definidas para las copias de seguridad.

● 38.1% (86) instituciones NO realizan pruebas de restauración de copias de seguridad realizadas.

● 16.4% (37) instituciones NO tiene configurado el sitio para evitar ataques de tipo SQL injection.

● 42.9% (97) instituciones NO cuentan con servicios innecesarios activos como SSH, FTP, telnet.

● 32.3% (73) instituciones NO han configurado un límite de accesos concurrentes para evitar ataques de denegación de servicios DDoS.