DECÁLOGO DE CIBERSEGURIDAD

01

Aumentar la capacidad de vigilancia de las redes y los sistemas. Es indispensable contar con el adecuado equipo de ciberseguridad.

Increase network and system surveillance capability. Appropriate staff.

02

Monitorización y correlación de eventos. Uso de herramientas capaces de monitorizar el tráfico de red, usuarios remotos, contraseñas de administración, etc.

Centralised record management tools. Monitoring and correlation of events (network traffic, remote users, administration passwords, etc.).

03

Política de Seguridad Corporativa restrictiva. Adecuación progresiva de los permisos de usuario, servicios en la "nube" y la utilización de dispositivos y equipos propiedad del usuario (BYOD).

Restrictive Corporate Security Policy. With more restrictive user grants, practical approximation of services in the cloud and use of devices and equipment owned by the user (BYOD).

04

Configuraciones de seguridad en todos los componentes de la red corporativa. Se incluirán los dispositivos móviles y portátiles.

Setting configurations in all corporate network components, including mobile devices and laptops.

05

Uso de productos, equipos y servicios confiables y certificados. Redes y sistemas acreditados para información sensible o clasificada.

Use of certified and trusted products, equipment and services. Accredited networks and systems for handling sensitive or classified information.

06

Automatizar e incrementar el intercambio de información. Reciprocidad con otras organizaciones y Equipos de Respuesta a Incidentes de Seguridad de la Información (CERTs).

Automate and increase the information exchange. Reciprocal work with other organisations and CERTs.

07

Compromiso de la Dirección con la ciberseguridad. Los cargos directivos deben ser los primeros en aceptar que existen riesgos y promover las políticas de seguridad.

Management should be committed to cybersecurity. Management should be the first to accept the risk and promote these policies.

08

Formación y la Sensibilización de usuarios (eslabón más débil de la cadena). Todos y cada uno de los niveles de la organización (dirección, gestión e implantación) deben ser conscientes de los riesgos y actuar en consecuencia.

Training and awareness raising at user level. Every level of the organization (management, employees and professionals) should be aware of the risk and act accordingly.

09

Atenerse a la legislación y buenas prácticas. Adecuación a los distintos estándares (en el caso de las Administraciones Públicas al Esquema Nacional de Seguridad -ENS-).

Compliance with Legislation and best practices. Adaptation to them and to the different cybersecurity standards.

10

Trabajar como si se estuviese comprometido. Suponer que los sistemas están ya comprometidos o lo estarán pronto y proteger los activos fundamentales.

WORKING AS IF YOU WERE COMPROMISED. To assume that the systems are already compromised or that they will be soon and to protect critical assets.

CCN Centro Criptológico Nacional

ccn-cert centro criptológico nacional