Decálogo Básico de Seguridad

1. La **cultura de la ciberseguridad**, la concienciación del empleado, debe ser uno de los pilares en lo que se asiente la ciberseguridad de cualquier organización.

2. **No abrir** ningún enlace **ni descargar** ningún fichero adjunto procedente de un correo electrónico que presente cualquier indicio o patrón **fuera de lo habitual**.

3. Utilizar **software de seguridad**, **herramientas antivirus** y **antimalware**, **cortafuegos** personales, **herramientas de borrado seguro**, etc. debe ser algo irrenunciable cuando se utiliza un **sistema de las TIC**.

4. **Limitar la superficie de exposición a las amenazas**, no solo hay que implementar medidas de seguridad que protejan el acceso a la información, sino que hay que determinar los servicios que son estrictamente necesarios.

5. **Cifrar la información sensible**, no hay otra alternativa.

6. Utilizar **contraseñas adaptadas** a la funcionalidad siendo conscientes de que la doble autenticación ya es una necesidad.

7. Hacer un **borrado seguro de la información** una vez que esta ya no sea necesaria o se vaya a retirar de uso el soporte en cuestión.

8. **Realizar copias de seguridad periódicas**, no existe otra alternativa en caso de infección de código malicioso tipo ransomware, pérdida de datos, averías del hardware de almacenamiento, borrado de información involuntaria por parte del usuario, etc.

9. **Mantener actualizadas las aplicaciones y el sistema operativo** es la mejor manera de evitar dar facilidades a la potencial amenaza.

10. Revisa regularmente la **configuración de seguridad aplicada**, los **permisos de las aplicaciones** y las **opciones de seguridad**.

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

Figura 6. Decálogo de seguridad