La publicación de este decálogo se enmarca dentro del Mes Europeo de la Ciberseguridad

"Trabajar como si se estuviese comprometido", principal recomendación del CCN en su Decálogo de Ciberseguridad

- **Se trata de diez ideas para promover, conseguir y mantener un nivel óptimo de seguridad en las organizaciones.**

Madrid, 27 de octubre de 2015. El Centro Criptológico Nacional (CCN), en el marco del ***Mes Europeo de la Ciberseguridad***, organizado por ENISA (Agencia Europea de las Redes y de la Información) ha publicado el Decálogo de Ciberseguridad, el cual pretende servir de manual de buenas prácticas para estar preparados ante posibles ciberataques.

MES EUROPEO DE LA SEGURIDAD CIBERNÉTICA

Se trata de diez ideas para promover, conseguir y mantener un nivel óptimo de seguridad en las organizaciones frente a cualquier ciberataque. Por ello es necesario implantar las siguientes recomendaciones:

1. **Aumentar la capacidad de vigilancia de las redes y los sistemas.** Para ello, es indispensable contar con el adecuado equipo de ciberseguridad interno o en su defecto, disponer de una consultoría externa de eficacia debidamente contrastada.
2. **Disponer de herramientas de gestión centralizada de registros**, incluyendo monitorización y correlación de eventos que permitan una apropiada detección de intrusos. Las herramientas utilizadas deberán ser capaces de monitorizar el tráfico de red, usuarios remotos, contraseñas de administración, etc.
3. Establecer una adecuada **Política de Seguridad Corporativa**, que contemple una adecuación progresiva de los permisos de usuario, cada vez más restrictivos, así como una aproximación práctica a los servicios en la "nube" y la utilización de dispositivos y equipos propiedad del usuario.
4. Aplicar **configuraciones de seguridad** a los distintos componentes de la red corporativa, incluyendo a los equipos móviles y portátiles.
5. Emplear **productos, equipos y servicios confiables y certificados** junto con **redes y sistemas acreditados** para el manejo de información sensible o clasificada del grado que se determine.

27 de octubre de 2015

6. **Automatizar e incrementar el intercambio de información** con los Equipos de Respuesta a Incidentes de Seguridad de la Información (CERT) mediante procedimientos ágiles y flexibles.
7. La **Dirección debe estar comprometida con la ciberseguridad**. Es fundamental que los cargos directivos sean los primeros en aceptar que existen riesgos y deben promover estas políticas.
8. Es necesario **Promover la Formación y la Sensibilización** en todos los niveles.
9. Se debe tener en cuenta en todo momento **atenerse a la Legislación y buenas prácticas**: adecuación a distintos estándares (en el caso de las AAPP al ENS)
10. Es preciso que la **Organización trabaje como si estuviera comprometida**. En este supuesto, la resiliencia cobra especial importancia como factor a tener en cuenta.

El ***Mes Europeo de la Ciberseguridad*** tiene como principal objetivo concienciar a los ciudadanos de la necesidad de preservar la información y abogar por un cambio en la percepción de las ciberamenazas mediante la promoción de la seguridad de los datos y la información, la educación, el intercambio de buenas prácticas y la competencia.

En esta ocasión, el lema de la campaña es "**Stop, Think, Connect. Cyber Security is a Shared Responsibility**" (*Para, piensa, conéctate. La Ciberseguridad es una responsabilidad compartida*) y en ella se han presentado más de 125 actividades a lo largo de 25 países europeos.

Sobre CCN-CERT, CERT Gubernamental Nacional

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del ENS.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas clasificados**, a sistemas de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

MÁS INFORMACIÓN
CCN-CERT
eventos@ccn-cert.cni.es
+34 670 29 20 05
Síguenos en
www.ccn-cert.cni.es/
@CCNCERT

27 de octubre de 2015