**Resultado de aprendizaje involucrados en la actividad:**

T7-17-29-5-5-1 RA2 [Critica] + [de manera objetiva y profesional, generando un documento que de cuenta de esto] + [para detectar falencias y/o problemas en los procesos de los sistemas de información] + [considerando las normas de calidad para el desarrollo de software que impulsa la disciplina]

[Creció un 27% el riesgo de que los usuarios de PC encuentren amenazas cibernéticas - Infobae](https://www.infobae.com/america/tecno/2020/07/07/crecio-un-27-el-riesgo-de-que-los-usuarios-de-pc-encuentren-amenazas-ciberneticas/)

Luego de leer el presente artículo con mucha atención y de relacionarlo con los temas que estuvimos tratando hasta el momento.

Debatir en cuanto a las medidas de prevención que se pueden implementar desde el punto de vista de un auditor de sistemas. (Cuáles serían las recomendaciones de Ud. como auditor?)

Respuesta:  
El artículo presentado refleja cómo el riesgo de ciberataques ha crecido de manera significativa en los últimos años, especialmente durante la pandemia, donde los usuarios domésticos y las organizaciones se volvieron más vulnerables frente a amenazas como malware, troyanos, aplicaciones falsas y técnicas de phishing. El incremento de la conectividad y el uso masivo de servicios digitales hizo que tanto personas como empresas se expongan a riesgos cada vez más avanzados, capaces de evadir las protecciones tradicionales. Esta situación demuestra que las medidas básicas ya no son suficientes y que es necesario adoptar un enfoque más integral en la protección de la información y los sistemas.

En este sentido, **como auditor de sistemas**, la medida clave no es solo instalar software de seguridad, sino **implementar un programa integral de ciberseguridad** que abarque controles técnicos, capacitación de usuarios, auditorías constantes y un marco de gobierno alineado con las mejores prácticas internacionales.

Por este motivo, las **medidas de prevención recomendadas desde la auditoría de sistemas** serían las siguientes:

**Controles técnicos básicos**

* Instalar y mantener **antivirus, antimalware y firewalls** en todos los equipos.
* Realizar **actualizaciones periódicas** de sistemas operativos y aplicaciones.
* Configurar **copias de seguridad automáticas** en medios seguros y externos.

**Protección en el uso diario**

* Usar **contraseñas robustas** y activar el **doble factor de autenticación (2FA)**.
* Acceder únicamente a **sitios web seguros (HTTPS)** y oficiales.
* Evitar descargas de archivos o clics en enlaces no solicitados.
* Restringir el uso de **equipos compartidos o públicos** para operaciones críticas.

**Capacitación y cultura organizacional**

* Capacitar a los usuarios en **detección de phishing, ingeniería social y apps falsas**.
* Implementar **campañas de concientización periódicas** con simulacros de ataques.
* Promover la **responsabilidad individual** en el uso de tecnologías dentro y fuera del trabajo.

**Auditoría y monitoreo**

* Realizar **evaluaciones periódicas de seguridad** sobre la infraestructura y aplicaciones.
* Aplicar **monitoreo continuo** para detectar actividades sospechosas en la red.
* Revisar **cumplimiento normativo** (ej. ISO 27001, leyes de datos personales).

**Gobierno y gestión de riesgos**

* Adoptar marcos de referencia como **COBIT 5**, ITIL o ISO 27000 para integrar la seguridad en el negocio.
* Definir **políticas y procedimientos formales de seguridad de la información**.
* Establecer un proceso de **mejora continua**, usando los incidentes como aprendizaje.