Ciberseguridad: cómo adoptar medidas para proteger sus activos de información”

En las últimas décadas, el desarrollo tecnológico ha impulsado nuevos modelos de negocio y formas innovadoras de brindar soluciones basadas en información, convirtiendo a los datos en un activo crítico para las organizaciones. Este contexto ha generado un nuevo entorno de amenazas que puede afectar la continuidad operativa de las empresas, ya que terceros pueden cometer fraudes financieros y delitos informáticos.

La **ISACA** define la ciberseguridad como la protección de los activos de información frente a amenazas que ponen en riesgo los datos procesados, almacenados y transportados en sistemas interconectados. La seguridad digital requiere que las empresas asuman una postura preventiva y proactiva.

Para reducir los riesgos, se recomienda adoptar prácticas como:

- Realizar **copias de seguridad periódicas**, preferentemente con respaldo en la nube.
- Instalar **antivirus y software de protección** frente a programas maliciosos.
- Elaborar **políticas internas de seguridad** para los empleados, considerando que muchos incidentes ocurren por descuidos o falta de conocimiento del personal.

Con el impacto de la digitalización, la ciberseguridad ha adquirido un papel estratégico, obligando a replantear los procesos tecnológicos de las compañías, ya que Internet las expone constantemente a ataques cibernéticos.

Las principales amenazas identificadas son:

- **Hackers**: ciberdelincuentes que adoptan nuevas estrategias para vulnerar la información de usuarios, especialmente mediante dispositivos móviles.
- **Malware**: programas maliciosos que dañan bases de datos, equipos y dispositivos móviles, pudiendo incluso espiar y controlar la actividad en línea.
- **Errores de programación**: fallos en el desarrollo de software que comprometen el funcionamiento de sistemas y aplicaciones.
- **Fallos electrónicos, siniestros o catástrofes naturales**: situaciones externas que afectan la seguridad y disponibilidad de la información.

Se destaca que los ataques informáticos no están dirigidos únicamente a grandes empresas o gobiernos. Cualquier organización o persona puede ser objetivo de los ciberdelincuentes, enfrentando riesgos que van desde la pérdida de datos hasta sanciones legales, multas o afectaciones a la reputación corporativa debido a la desconfianza de los clientes.