CIBERSEGURIDAD

PRINCIPIOS Y RECOMENDACIONES

Orientaciones y buenas prácticas

#SigueNuestraRuta | https://www.csirt.biocubafarma.cu
https://www.eti.cu

Nuestro día a día gira alrededor de actividades cada vez más digitalizadas y, por consiguiente, en un escenario digitalmente reformado, los retos de la seguridad de la información se modifican y complejizan. Esta nueva dinámica apuesta por una sistematicidad sobre el estado del entorno digital con una mirada reactiva y preventiva de la seguridad y el control de los flujos de información.

Estas recomendaciones son la primera parada en esta cuesta arriba hasta un nivel aceptable de seguridad. Nuestra estrategia es crear un sentido de urgencia de conciencia ante los peligros a los que se exponen los activos digitales como la información y la inminente necesidad de generar un cambio en la cultura organizacional.

PRINCIPIOS BÁSICOS

1

Confidencialidad

Conjunto de reglas que limita el acceso a la información

2

Integridad

Garantía de que la información es confiable y precisa

3

Disponibilidad

Garantía de acceso confiable a la información por parte de personas autorizadas

RECOMENDACIONES

- Establecimiento de una cultura sobre ciberseguridad a nivel organizacional con el involucramiento de todas las áreas .
- limitar la superficie de exposición a las amenazas aplicando el principio de defensa en profundidad.
- Aplicar actualizaciones de seguridad periódicamente sobre los sistemas y servicios mediante la correcta gestión de la tecnología empleada.
- Emplear herramientas que posibiliten la no proliferación de amenazas en entornos TI: antivirus, antimalware,cortafuegos personales, software de seguridad, herramientas de borrado seguro, entre otras.
- Inclusión de buenas prácticas de seguridad en servicios críticos: navegación web, correo, redes sociales, entre otros.
- Cifrado de la información sensible.
- Cumplimiento del marco legal vigente en materia de ciberseguridad.

Nueva Campaña de concienciación sobre ciberseguridad