



Te ofrecemos el Boletín de Ciberseguridad [#CubaPorLaVida](#)



BOLETIN DE CIBERSEGURIDAD ¡MANTENTE INFORMADO!



DIRECCIÓN GENERAL DE SALUD PÚBLICA, SECCIÓN SEGURIDAD Y PROTECCIÓN

MEDIDAS DE CIBERSEGURIDAD APLICADAS EN LA DGS, PARA FORTALECER EL SISTEMA DE SEGURIDAD INFORMÁTICA

1. Descargar solo de fuentes oficiales y verificadas. Todos los Programas deben activarse y actualizarse utilizando funciones/herramientas proporcionadas por desarrolladores auténticos, ya que las herramientas de activación ilegales ("Cracks") y los actualizadores de terceros pueden contener malware.
2. No abrir los archivos adjuntos/enlaces que se encuentran en correos electrónicos y mensajes spam, ya que pueden ser maliciosos y causar infecciones. Tener cuidado extremo al navegar en internet, ya que los contenidos fraudulentos y peligrosos en línea suelen parecer legítimos/inocuos.
3. Tener instalado, bien configurado y actualizado los antivirus aprobados. El software de seguridad debe utilizarse para realizar análisis periódicos del sistema y eliminar las amenazas.
4. Tener habilitado y configurado correctamente el firewall de las estaciones de trabajo y servidores.
5. No usar recursos compartidos mediante protocolo SMB (puerto 445), en la red.
6. Mantener actualizado los parches de seguridad de su sistema operativo y aplicaciones.
7. Tener desplegado y gestionar adecuada y oportunamente un sistema de monitoreo de tráfico de red y eventos de sistemas operativos y servicios, que les permita identificar posibles amenazas.
8. Mantener actualizadas y debidamente protegidas, en ubicaciones físicas externas, las salvadas de seguridad de infraestructuras, plataformas, servicios y otros componentes requeridos, que les permitan recuperarse ante un incidente.
9. Formar al personal responsable de las TIC (tecnología informática y de las comunicaciones) en las mejores prácticas de seguridad, para asegurarse de que conoce las últimas amenazas.
10. Controlar la implementación de las medidas en la DGS y sus instituciones subordinadas.

¿QUÉ ES CIBERSEGURIDAD?

Ciberseguridad es un término que resume una serie de actividades, procedimientos y tecnologías que se utilizan para mantener la protección de los sistemas informáticos, los datos privados que se almacenan en forma digital, junto con el hardware y el software. Hay muchas medidas que encajan en la definición de ciberseguridad.

Las medidas de ciberseguridad incluyen cortafuegos, criptografía, sistemas de detección de intrusos, diseño especial con protección adicional y otras formas de control de seguridad.



ACTUALIDAD EN CUBA Y EL MUNDO

Cultura informativa sobre ciberseguridad

CUBA ADVIERTE SOBRE ACTUALES AMENAZAS A LA CIBERSEGURIDAD.

- En el día dedicado a la Ciberseguridad en la XIX Convención Informática 2024, el viceministro de Comunicaciones Ernesto Rodríguez afirmó que como nunca antes abundan falsas atribuciones políticamente motivadas para ataques cibernéticos en el afán de justificar acciones hostiles contra los Estados. El vicetitular de comunicaciones explicó que en 2023 entre los principales ataques estuvieron los clop, un virus tipo ransomware, diseñado para eliminar herramientas y soluciones de seguridad de los sistemas que infecta, que dañó a grandes empresa y el Departamento de energía de estados unidos. Rodríguez enfatizó en que la ciberseguridad no se alcanza de manera total por estar sujeta al tiempo, a los embates favorables y desfavorables del desarrollo tecnológico y el incremento del talento humano, por lo que debe considerarse un asunto y una urgencia de la seguridad nacional.

EEUU Y REINO UNIDO ACUSAN A CHINA: SU RED DE CIBERESPIONAJE COMPROMETE A MILLONES DE USUARIOS

- En esta ocasión el protagonismo lo acaparan EEUU, Reino Unido y China. Y es que los dos países han acusado a China de montar una compleja trama de ciberespionaje que persigue recabar información privada de legisladores, periodistas, académicos y empresas. Entre estas últimas se encuentran algunas compañías que tienen contratos vigentes con los Departamentos de Defensa de EEUU y Reino Unido. Según los investigadores estadounidenses, el grupo de hackers ha logrado comprometer cuentas de correo electrónico personales, correos de índole profesional, cuentas de almacenamiento en la nube y registros de llamadas telefónicas de varios millones de ciudadanos estadounidenses. Según las autoridades de Reino Unido su impacto en su propio país ha sido similar al que este grupo chino ha tenido en EEUU. Las embajadas de China en Reino Unido y EEUU han negado que su país esté detrás de esta operación de ciberespionaje. Sin embargo, esta declaración no ha evitado que los Gobiernos estadounidense y británico hayan desplegado un paquete de sanciones dirigido expresamente a la empresa que según ellos está estrechamente vinculada al Ministerio de la Seguridad del Estado de China

¡ALERTA!

Si usted recibe algún correo de un destinatario desconocido, y además viene acompañado con algún fichero adjunto, que la curiosidad no lo tienta, no abra ese fichero, notifique al Responsable de Seguridad Informática de la institución, para el correspondiente análisis y reporte de incidencia.

Manténgase informado sobre las principales políticas de ciberseguridad de la institución. Recuerde siempre que:

❖ El desconocimiento no lo exonera de la responsabilidad.

¿Qué es Correo Spam?

El correo electrónico no solicitado, denominado spam, figura entre los mayores problemas de la comunicación electrónica. Representa hasta el 50% de todas las comunicaciones por correo electrónico.

El spam es cualquier forma de comunicación no solicitada que se envía de forma masiva Su forma más frecuente es un correo electrónico de publicidad enviado a un gran número de direcciones. Enviar spam es ilegal



DECRETO-LEY 35

¿En qué consiste?

Reglamento sobre el modelo de actuación nacional para la respuesta a incidentes de ciberseguridad, marca la actuación por etapas claramente definidas y con acciones concretas.

Estos documentos, le dan fortaleza a la gestión de la ciberseguridad en Cuba, contribuye a una mejor coordinación y cooperación de los involucrados, estandariza los procesos y pondera el carácter preventivo como vía para evitar incidentes y su posible repercusión.

RESOLUCIÓN 105

ACETAF OFIC

DE LA REPÚBLICA DE CUBA
MINISTERIO DE JUSTICIA

Información en esta primera
versión Oficial No. 102, Ordenada por el 1º de agosto de 2024

COORDINADOR DEL SISTEMA
Ejército Revolucionario en Cuba
Comando en Jefe del Poder Judicial
Comando en Jefe de la Armada Revolucionaria
Comando en Jefe de la Fuerza Armada Revolucionaria
Comando en Jefe de la Policía Nacional Revolucionaria
Comando en Jefe de la Guardia Nacional Revolucionaria
Comando en Jefe de la Brigada de Vigilancia y Control de Tráfico Aéreo
Comando en Jefe de la Brigada de Vigilancia y Control de Tráfico Marítimo
Comando en Jefe de la Brigada de Vigilancia y Control de Tráfico Terrestre
Comando en Jefe de la Brigada de Vigilancia y Control de Tráfico Espacial
Comando en Jefe de la Brigada de Vigilancia y Control de Tráfico Cibernético