Tecnologías de la Información BioCubaFarma

División de Ciberseguridad
Calle 18 N° 4310 e/ 43 Y 47, Miramar. La Habana, Cuba
Teléfono: 72152188-89
www.eti.cu

"Orientación sobre el correcto empleo de las TIC para administradores de infraestructuras/servicios y supervisión activa del contexto por parte del Especialista de Seguridad Informática"

Premisas gerenciales

Puntos a tener en cuenta:

1. *Funcionamiento de lo establecido en el Sistema de gestión de la Seguridad Informática (SGSI):*
   Cumplir con lo tipificado en la presentación del Plan de Seguridad informática a partir de la Caracterización del Sistema Informático, los resultados del Análisis de Riesgos, Políticas de Seguridad Informática, definición de Responsabilidades de los actores identificados por la entidad y Medidas y procedimientos de Seguridad Informática y los Anexos del PSI.

2. *Bastionado de bienes Informáticos*:
   Garantizar la seguridad de la información corporativa que almacenan los equipos a los que se conectan, mediante la incorporación de buenas prácticas de seguridad que permitan fortalecer el acceso privilegiado a la información, a través de la instalación de aplicaciones tales como: Volumen Cifrado Veracrypt (cuyo proveedor es el MININT, última versión entregada 1.19 que responde a un nivel de cifrado de disco y el tamaño del volumen cifrado variará en dependencia de las necesidades del cliente).

3. *Uso correcto de los recursos TIC*:
   Control y supervisión del correcto empleo de las TIC, con estricto cumplimiento de los legislado en la Gaceta Oficial No.45 ordinaria del 4 de julio de 2019, donde se identifica que el Sistema de Seguridad de las TIC se constituye a partir de los sistemas de seguridad existentes en las instituciones del país que posean o utilicen las TIC, en interés propio o de terceros, e incluye a Usuarios de las TIC.

4. *Autorizaciones de acceso a redes/servicios y privilegios de Administración de los sistemas*:
   Cumplir con lo establecido en la Política de Control de Acceso a Servicios Tecnológicos que debe estar enfocada en la definición, establecimiento, implementación, mantenimiento y mejora continua de los accesos lógicos a la información, de manera que los procedimientos que se definan (conforme a las necesidades de protección de los servicios), con sus controles y medidas asociadas, estén encauzados a hacer frente a las amenazas presentes y disminuir la probabilidad de explotación de posibles vulnerabilidades de los elementos básicos de este nuevo contexto digital, siempre enfocada garantizar la confiabilidad en el aseguramiento de la información.

5. *Responsabilidades del Usuario*:
   Estricto cumplimiento de los legislado en la Gaceta Oficial No.45 ordinaria del 4 de julio de 2019, donde se definen responsabilidades y deberes de los usuarios de las TIC y de los tipificado en cada PSI conformado por la empresa.

6. *Seguimiento de Supervisiones Internas de Seguridad anuales:*
   Establecer las directrices para el desarrollo de la auditoría a las TIC, en correspondencia con la categorización de los sistemas y actividades, y realizar la evaluación de los resultados obtenidos con la identificación de no conformidades detectadas.

Las medidas de control que se establezcan estarán concentradas en:

- El cumplimiento estricto del procedimiento donde se regula el sistema para el uso de las contraseñas de usuarios y dispositivos de la red, la autenticación de usuarios, denominación de equipos y el direccionamiento IP, así como la encriptación en la configuración de la conexión que lo requiera, así como la legislación vigente sobre este tema.
- El cumplimiento estricto del procedimiento donde se definen los tipos de sistemas de supervisión, control, detección y alarma que permiten reaccionar proactivamente y dar una respuesta efectiva ante amenazas de ciberseguridad;
- El cumplimiento estricto del procedimiento para que los administradores de redes puedan proponer herramientas complementarias y exista un mecanismo de autorización para incorporarlas;
- En la definición de un repositorio interno y su sistema de salvas que permita aplicar la gestión de las actualizaciones de seguridad;
- La puesta en marcha de mecanismos y herramientas para la gestión de las trazas de los servicios y sistemas informáticos;
- La implementación de la revisión de los sistemas y servicios que se instalen o empleen.
- Aplicación en computadoras o servidores habilitados de la instalación de barreras y otros medios de protección; incorporándose herramientas de seguridad que permitan el control y monitoreo de los servidores, servicios y usuarios de la red.