BOLETÍN ESPECIAL DE SEGURIDAD INFORMÁTICA N.- 2019-ESFORSE-TICS-001, SOBRE MEDIDAS DE PREVENCIÓN ANTE POSIBLES CIBERATAQUES.

¿Qué es un CIBERATAQUE?

Un CIBERATAQUE es la explotación deliberada de sistemas informáticos y redes dependientes de la tecnología. Estos ataques utilizan códigos maliciosos para alterar la lógica o los datos del ordenador, lo que genera consecuencias perjudiciales que pueden comprometer información y provocar delitos cibernéticos, como el robo de identidad.

ALCANCE

Los ciberataques pueden implicar un equipo muy unido de hackers de élite que trabajan bajo el mandato de un estado nación. Su intención es crear programas que aprovechen fallas previamente desconocidas en el software.

MEDIDAS PARA PREPARARSE ANTE UN POSIBLE CIBERATAQUE:

- Cambiar las claves de sus equipos informáticos y sistemas, utilizando claves fuertes. (Debe contener símbolos, mayúsculas, minúsculas, números e inclusive una extensión mayor a 10 caracteres).
- Durante los horarios de 12H30 a 14H30 y a partir de las 17H30, los equipos informáticos deben ser apagados en su totalidad, si algún departamento requiere que equipos informáticos accedan fuera de horario, deberán indicar a la unidad de Tics a fin de registrarlo en el servidor de dominio.
- Permanecer atentos ante intentos de aplicación de ingeniería social para extraer información PHISHING (utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.)
- La instalación de servicios informáticos (software) por parte de terceros deberá realizarlo con la presencia de personal de Tics.
- Se prohíbe guardar en el disco duro del equipo y en carpetas compartidas documentos que tengan la calificación de secretísimo, secreto y reservado.
- Respaldar toda la información de los equipos informáticos en discos externos, únicamente en el equipo debe estar almacenado la mínima documentación para mantener la operatividad del mismo.
- Todos los usuarios de personal que no se encuentra activo en el instituto serán inactivadas, por lo que deberán gestionar la creación de nuevos usuarios, si fuera el caso. Permanecer atento ante cualquier información sobre el inicio de los ataques y comunicar inmediatamente a la unidad de Tics.

REPORTE DE INCIDENTES:

Reporte el incidente al Departamento de TICS, a través de red telefónica interna mediante la ext. 194