PROTOCOLO DE SEGURIDAD ANTE RIESGOS DE SEGURIDAD DIGITAL

IES TRINIDAD ARROYO

Desarrollar un plan de seguridad digital ante riesgos en la red del centro es fundamental para proteger la información y los recursos tecnológicos de la institución. Los pasos a seguir en nuestro plan de seguridad digital son:

1. Evaluación de riesgos. Es realizada por el responsable TIC del centro (al inicio del curso y siempre que la situación lo requiera) a partir del análisis de las posibles amenazas, entre ellas:

    - Malware: El malware, como virus, gusanos, troyanos y otros tipos de software malicioso, puede infectar los sistemas de la red del IES. Esto puede resultar en la pérdida de datos, interrupción de los servicios y comprometer la seguridad de los usuarios.

    - Hacking: Los ataques de hackers pueden resultar en la pérdida o el robo de datos sensibles, interrupción de los servicios, daño a los sistemas de la red del IES y otros efectos negativos.

    - Phishing: Los correos electrónicos de phishing pueden engañar a los usuarios del IES para que proporcionen información confidencial, como contraseñas y datos bancarios, que pueden ser utilizados para acceder a los sistemas de la red.

    - Robo de identidad: El robo de identidad puede ocurrir cuando los hackers obtienen acceso a información personal de los usuarios del IES, como nombres, direcciones, números de seguro social, entre otros.

    - Accesos no autorizados: El acceso no autorizado a la red del IES puede permitir a los atacantes realizar acciones indeseadas, como cambiar o eliminar datos, o instalar software malicioso.

    - Accesos a sitios web maliciosos: Los usuarios del IES pueden ser dirigidos a sitios web maliciosos que contienen malware o engañarlos para que descarguen archivos no deseados.

    - Descarga de software malicioso: Los usuarios pueden descargar software malicioso sin saberlo, lo que puede afectar los sistemas de la red del IES.

    - Robo o pérdida de dispositivos móviles: Los teléfonos inteligentes y tabletas, pueden contener información sensible y pueden ser robados o perdidos, lo que puede resultar en la exposición de datos sensibles.

- Errores humanos: Los errores humanos, como la selección de contraseñas débiles o la falta de actualización de software, pueden crear vulnerabilidades en la red del IES que pueden ser explotadas por atacantes.

2. Establecer políticas de seguridad: Una vez que se han evaluado los riesgos, se establecen políticas de seguridad, claras y precisas para el personal y los estudiantes del IES. Estas políticas incluyen aspectos como la gestión de contraseñas, el acceso a la red, la descarga de software, entre otros.

    - Política de contraseñas: Esta política establece los requisitos de seguridad que deben cumplir las contraseñas de los usuarios del IES, como la longitud mínima, la complejidad y la caducidad. También se recomienda el cambio periódico de contraseñas.

    - Política de acceso y autenticación: Esta política define los procedimientos de autenticación que siguen los usuarios para acceder a la red del IES. Requiere la autenticación multifactorial y limitar el acceso solo a usuarios autorizados.

    - Política de actualización de software: Esta política establece que todos los dispositivos conectados a la red del IES tendrán el software actualizado con las últimas actualizaciones y parches de seguridad.

    - Política de uso de dispositivos móviles: Esta política establece los requisitos de seguridad que cumplen los dispositivos móviles, como el cifrado de datos, el bloqueo remoto en caso de robo o pérdida, y la instalación de software de seguridad.

    - Política de gestión de datos sensibles: Esta política define los procedimientos para la gestión de datos sensibles, como los datos personales de los miembros de la comunidad educativa del IES. Incluye la restricción del acceso a estos datos solo a usuarios autorizados.

    - Política de uso de Internet: Esta política establece las reglas y restricciones sobre el uso de Internet por parte de los usuarios del IES.

    - Política de gestión de dispositivos: Esta política define los procedimientos para la gestión de dispositivos de la red, como servidores, equipos y dispositivos de red. Incluye la supervisión del uso de los dispositivos, el control de acceso y la eliminación segura de los datos almacenados en ellos.

- Política de formación y concienciación: Esta política establece la necesidad de capacitar a los usuarios de la red del IES sobre las medidas de seguridad, como la importancia de la selección de contraseñas seguras, la detección de correos electrónicos de phishing y el uso adecuado de los dispositivos móviles.

3. Implementar software de seguridad: el centro cuenta con un software que incluye antivirus, firewall, detección de intrusos, entre otras funcionalidades.
4. Realizar copias de seguridad: El centro realiza copias de seguridad regularmente. Estas copias de seguridad se almacenan en un lugar seguro y accesible en caso de emergencia.
5. Formar a toda la comunidad educativa: todos los usuarios de la red del IES conocen las políticas de seguridad para identificar posibles amenazas y comunicar cualquier incidente de seguridad.
6. Plan de contingencia en caso de un incidente de seguridad. Pasos a seguir:
    - Identificación y notificación del incidente a la comisión TIC.
    - Evaluación y clasificación del incidente: el responsable evalúa su alcance, gravedad y posibles efectos.
    - Contención del incidente para limitar el daño causado y evitar que se propague a otros sistemas o dispositivos.
    - Análisis de lo ocurrido para determinar la causa del incidente, los sistemas y datos afectados, y el alcance del daño.
    - Restauración de la red.
    - Comunicación durante todo el proceso de respuesta al incidente con todas las partes interesadas de forma oportuna, precisa y transparente.
    - Evaluación y mejora una vez que el incidente ha sido resuelto con el fin de identificar áreas de mejora y actualizar el plan de contingencia para futuros incidentes.

Este protocolo de seguridad ante riesgos de seguridad digital es integral y se actualiza de forma regular.