ESCUELA
POLITÉCNICA
NACIONAL

Política de Aseguramiento de los Servicios de Aplicación en las Redes Públicas

Código	Política de Aseguramiento de los Servicios de Aplicación en las Redes Públicas
Versión:	1.0.0
Fecha de la versión:	23-02-2023
Creado por:	Grupo
Aprobado por:	Líder
Nivel de confidencialidad:	Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
23/02/2023	1.0.0	Grupo	Descripción básica del documento

Tabla de contenido

1. Objetivo, alcance y usuarios

Garantizar la protección de los servicios de aplicación que se ejecutan en las redes públicas, asegurando la confidencialidad, integridad y disponibilidad de la información, y evitando el envío de información no permitida o involuntaria.

2. Política de Aseguramiento de los Servicios de Aplicación en las Redes Públicas

Se debe tomar en cuenta los siguientes:

1. Cifrado de las comunicaciones: Todo servicio de aplicación que se ejecute en redes públicas deberá tener implementado un sistema de cifrado de las comunicaciones que garantice la confidencialidad de la información transmitida. Se recomienda el uso de algoritmos criptográficos de clave pública como SEAL por sus propiedades homomórficas.
2. Sistemas múltiples de autenticación: Se deberán implementar sistemas de autenticación que incluyan al menos dos factores, uno de los cuales deberá ser el correo electrónico. El correo electrónico servirá como una capa adicional de seguridad y permitirá al usuario recuperar la cuenta en caso de que haya perdido el acceso al otro factor de autenticación.
3. Uso de certificados digitales: Todo servicio de aplicación que se ejecute en redes públicas deberá contar con un certificado digital que permita la identificación segura del origen y destino de la información. El certificado digital deberá ser emitido por una entidad de confianza reconocida.
4. Sistemas de prevención de envío de información no permitida: Se deberán implementar sistemas de prevención de envío de información no permitida para evitar que se transmita información confidencial o personal de los usuarios sin autorización. Estos sistemas deberán estar configurados para bloquear el envío de información en caso de detectar contenido no permitido.
5. Sistemas de protección para envíos involuntarios de archivos: Se deberán implementar sistemas de protección para evitar el envío involuntario de archivos, ya sea por error del usuario o por ataque externo. Estos sistemas deberán ser capaces de detectar archivos sospechosos y bloquear su envío.

Se sugiere además considerar las siguientes recomendaciones:

- Se recomienda el uso de la herramienta Microsoft Threat Modeling Tool para modelar y analizar las amenazas potenciales a la seguridad de los servicios de aplicación en redes públicas.
- Se recomienda que los certificados digitales sean renovados periódicamente para garantizar la confidencialidad de la información.
- Se recomienda la utilización de técnicas de autenticación basadas en tokens de seguridad para garantizar la integridad de los procesos de autenticación.

- Se recomienda la implementación de sistemas de registro y supervisión para detectar posibles amenazas y vulnerabilidades en tiempo real.

Nota:

Si la aplicación no requiere el uso de redes públicas, se deberán tomar medidas para evitar el acceso no autorizado a la aplicación desde redes no autorizadas.

La política de aseguramiento de los servicios de aplicación en redes públicas busca garantizar la confidencialidad, integridad y disponibilidad de los datos y sistemas utilizados en la red pública. Para ello, se requiere el uso de sistemas de autenticación robustos, cifrado de comunicaciones y la implementación de sistemas de prevención de envío de información no permitida y protección contra envíos involuntarios de archivos. El uso de algoritmos criptográficos de clave pública como SEAL, el 2FA a través de correo electrónico y el uso de certificados digitales son recomendaciones clave para la seguridad de la aplicación en redes públicas. Es importante que los desarrolladores y responsables de seguridad implementen estas medidas para proteger a los usuarios y garantizar la confidencialidad y seguridad de la información.

3. Validez y gestión de documentos

Este documento es válido hasta el año 2026.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de obligaciones de la organización que ya existían pero que no fueron identificadas.
- Cantidad o monto de multas pagadas por el no cumplimiento de obligaciones.
- Cantidad de días de atraso en el cumplimiento de la obligación.

Líder
[firma]