2025

MARCO NORMATIVO DE IT

ES0902 - Estándar de Seguridad
Agencia de Sistemas de Información

Agosto 2025

Índice

1 Introducción

El presente documento tiene por finalidad definir los requisitos que deben cumplir todas las aplicaciones del GCABA, como así también establecer la interacción con los distintos actores en el marco del proceso de desarrollo de dichas aplicaciones. En este sentido, corresponde mencionar que el presente Estándar de Seguridad se complementa con el estándar de Desarrollo, el cual se enfoca sobre los aspectos estructurales de las aplicaciones y su entorno de operación.

Se deja constancia que las definiciones utilizadas son aplicables tanto para las aplicaciones desarrolladas según especificaciones de las distintas reparticiones y agencias del GCABA, como para aquellas aplicaciones de software comerciales o desarrolladas por terceros con o sin adaptaciones a medida, independientemente de su condición comercial (ej. open source, licencia de uso, servicios Cloud, cesión de derechos, etc.).

***IMPORTANTE**: Salvo que para un proyecto en particular se especifique por contrato algún acuerdo diferente para alguno de los puntos detallados en este documento, todos los sistemas que se desarrollen en el ámbito de los proyectos de GCABA deben respetar la totalidad de los criterios aquí descriptos. En virtud de ello, la existencia de un contrato en estas condiciones, deberá contar con la aprobación de la Agencia de Sistemas de Información.*

2 Marco Normativo de TI

Toda solución de software deberá cumplir con lo expresado en el Marco Normativo de TI del GCABA, publicado en el boletín oficial del día 08-11-2013, Resolución 177-ASINF-2013, Resolución 239-ASINF/2014 y N° 12/ASINF/17. Dicha documentación se encuentra disponible en https://buenosaires.gob.ar/agencia-de-sistemas-de-informacion/estandares-de-la-agencia

3 Principios de Aplicaciones

Existen ciertos principios generales a nivel seguridad para ser implementados sobre el desarrollo de las aplicaciones haciéndolas seguras.

A Nivel Organización:

O1- Se deben respetar los principios y normativas vigentes de TI del GCABA

O2- El control de la seguridad informática debe estar a cargo de un organismo perteneciente al GCABA.

A Nivel Calidad:
C1- El mecanismo de autenticación a implementar en las aplicaciones debe basarse en el protocolo **OpenID Connect**, cumpliendo con los lineamientos de seguridad informática definidos por la ASI.
En todos los casos, el proveedor autorizado y obligatorio de identidad para la implementación de OpenID en los entornos del GCABA es **Keycloak**, gestionado por la DGSEI.

Las aplicaciones deberán:

- Integrarse con Keycloak utilizando los flujos adecuados de OpenID.
- Registrarse en el servidor correspondiente.
- Respetar las políticas de autenticación, autorización y protección de recursos definidas por la ASI.

Además, se deberá tener presente que no se brindarán credenciales sobre el anterior OpenID (https://oauth2-server.apps.buenosaires.gob.ar/). Por el contrario, las nuevas versiones de aplicaciones deberán actualizar la autenticación a la nueva solución, redirigiendo al usuario para el ingreso de sus credenciales a este portal de autenticación: https://identidad-gcaba.apps.buenosaires.gob.ar/.

La asignación de roles a los usuarios es una función que queda delegada a la propia aplicación, pudiendo utilizar grupos de AD de ser necesario. Se recomienda acotar la autenticación del usuario en base a su ubicación en el árbol de AD o por membresías de grupos.

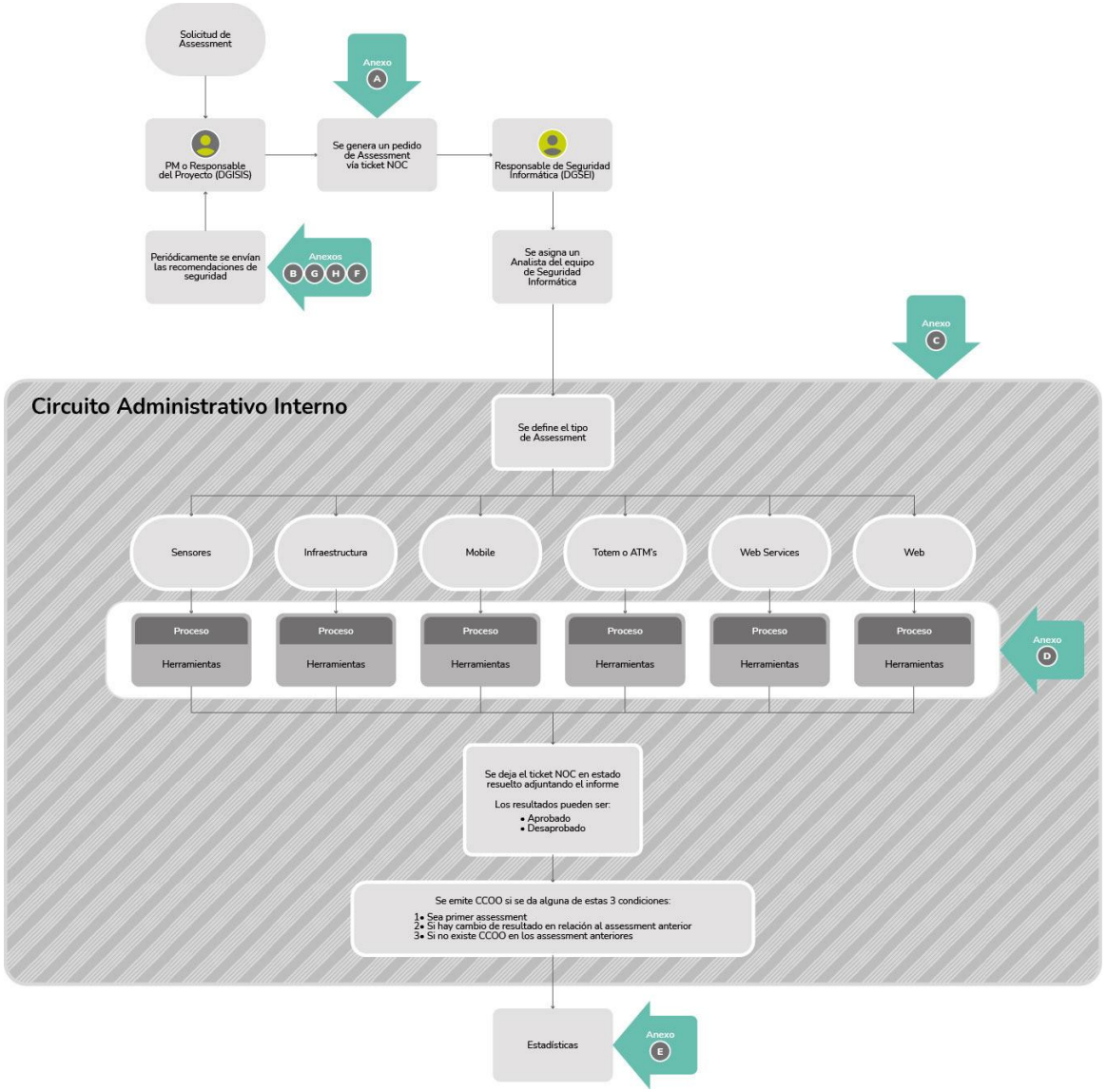
C2- Las aplicaciones homologadas deben tener el aprobado a nivel seguridad en el ambiente QA.

C3- Las aplicaciones deben respetar las herramientas versionadas y autorizadas que se indican en el documento Estándar de Desarrollo, en su sección “Versiones y Herramientas aceptadas por la ASI”.

4 Proceso para el control a nivel de Seguridad Informática

En un contexto donde los ataques y la búsqueda de vulnerabilidades para explotar son parte de la rutina, las aplicaciones deben implementar mecanismos cada vez mejores y más inteligentes con el objeto de prevenir y mitigar los daños que todo tipo de intrusión externa y/o interna pudieran ocasionar.

En este proceso se manejarán dos actividades específicas para un mejor control de las aplicaciones, el primero se realizará por intermedio de un sistema automatizado y el segundo mediante un circuito interno de la DGSEI, el cual se detalla en la siguiente imagen:



5 Entregables

Para poder realizar los análisis específicos de seguridad se deberá proveer de los elementos que se necesiten de acuerdo al tipo de activo que se deberá trabajar.

Además, para aplicaciones y servicios web, se deberá completar el formulario para la aplicación de políticas de WAF suministrado por el equipo de Prevención.

E1 - Web Services

Entregable	Contenido
Estructura	• Toda la descripción de los métodos que utiliza el Web Service. • Ejemplos específicos de la utilización de dichos métodos.
Datos	• Los datos necesarios para su utilización.
Servicio	• Se debe especificar el tipo de Web Service (ej.:SOAP, RESTful) • Descripción de Integraciones

E2 - Aplicaciones Web

Entregable	Contenido
Especificaciones	• URL o IP • Usuarios con todos los roles que se manejen en la aplicación a revisar.
Documento de Arquitectura	• Descripción de los servicios • Descripción de integraciones • Modelo lógico y físico de datos • Arquitectura tecnológica (sistema operativo, software de base, motor de base de datos, etc.)

E3 - Aplicaciones Mobile

Entregable	Contenido
Especificaciones	• APK • Usuarios con todos los roles que se manejen en la aplicación a revisar.
Documento de Arquitectura	• Descripción de los servicios • Descripción de integraciones • Modelo lógico y físico de datos • Arquitectura tecnológica (sistema operativo, software de base, motor de base de datos, etc.)

E4 - Servidores

Entregable	Contenido
Especificaciones	• IP • Usuario Administrador

Entregable	Contenido
Documento de Arquitectura	• Descripción de los servicios • Arquitectura tecnológica (sistema operativo, software de base, motor de base de datos, etc.)

E5 - Totem

Entregable	Contenido
Especificaciones	• Activo Físico • Usuarios con todos los roles que se manejen en la aplicación a revisar.
Documento de Arquitectura	• Descripción de los servicios • Descripción de integraciones • Topología y modularización • Modelo lógico y físico de datos • Políticas globales de diseño (concurrencia, almacenamiento de datos, mecanismos de comunicación, mecanismos de seguridad, manejo de errores, etc.) • Arquitectura tecnológica (sistema operativo, software de base, motor de base de datos, etc.) • Dimensionamiento acorde a las especificaciones no funcionales.

6 Principios de Seguridad

Vulnerabilidades:

Vu1 - Toda página de autenticación debe contener captcha o bloqueo de usuarios por intentos de sesión, funcionalidad que se encuentra contenida en OpenID.

Vu2 - Todo dato sensible no puede ser enviado en texto plano.

Vu3 - Toda aplicación que se cierra a través de las ventanas o en forma directa del browser, no debe dejar la sesión activa.

Vu4 - Toda sesión en stand by, tiene que tener un tiempo límite para su utilización. Esto, independientemente del límite de tiempo que posee el token de autenticación del OpenID.

Vu5 - Toda validación del lado del cliente, debe estar espejada del lado del servidor.

Vu6 - Todos los mensajes de error deben estar customizados.

Vu7 - Todo el software de base debe estar configurado para no entregar datos privados.

Vu8 - Los perfiles de usuarios armados en las aplicaciones deben respetar los roles asignados.

Vu9 - Las aplicaciones que expongan funcionalidades accesibles sin autenticación a través de interfaces públicas (web o API), deberán contemplar mecanismos de control de uso que mitiguen riesgos por consumo excesivo o automatizado de recursos y garanticen la estabilidad del servicio.

Vu10 - Para mejorar la seguridad en las aplicaciones, se debe tener en cuenta la información suministrada en los siguientes links:

- Aplicaciones Web: https://owasp.org/www-project-top-ten/
- API's y/o Web Services: https://owasp.org/www-project-api-security/
- Aplicaciones Mobile: https://owasp.org/www-project-mobile-top-10/

Versionados:

Ve1 - Las aplicaciones deben respetar las herramientas versionadas y autorizadas que se indican en el Estándar de Desarrollo en la sección “Versiones y Herramientas aceptadas por la ASI”.

Ve2 - En relación a las versiones indicadas como más seguras, antes de utilizarlas se debe consensuar con el área de Infraestructura si está permitido su uso.

7 Condiciones de Aceptación

A Nivel General

G1 - Cabe destacar que el cumplimiento del punto 6 no asegura la aprobación de un assessment de seguridad.

G2 - Las aplicaciones se aprobarán, a nivel seguridad, si las vulnerabilidades detectadas son de una categoría de riesgo bajo, siempre y cuando no supere la cantidad de 10 vulnerabilidades de esta categoría.

G3 - Cuando se reenvíe una aplicación al área de Seguridad, se procederá a controlar el 100% de las vulnerabilidades informadas, pero se tomará en cuenta el punto G2 para su aprobación.

G4 - Cuando se vuelve a realizar el análisis de una aplicación que en versiones anteriores tiene un informe de vulnerabilidades, no se controlará solamente las vulnerabilidades detectadas previamente, sino que se procederá a un control total. Por lo tanto, se pueden presentar nuevas vulnerabilidades y también se tomará en cuenta el punto G2.