

# Consideraciones de seguridad para el desarrollo / despliegue de aplicaciones

## Contenido

1. Listado de chequeo de Aplicaciones para consideraciones de seguridad	1
1.1. Objetivo	1
1.2. Listado de control	1
2. Listado de chequeo de aplicaciones para clasificación de criticidad	3
2.1. Objetivo	3
2.2. Procedimiento de clasificación de la información	3
2.3. Evaluación de criticidad	4

## 1. Listado de chequeo de Aplicaciones para consideraciones de seguridad

### 1.1. Objetivo

El siguiente documento busca obtener un listado de control para analizar y promover las consideraciones de seguridad para el desarrollo/despliegue de la aplicación en su ambiente correspondiente.

### 1.2. Listado de control

#### Describir Objetivo funcional de la Aplicación

El objetivo de la aplicación es **facilitar y agilizar los procesos de atención y asistencia a las víctimas de delitos**, abarcando desde el registro inicial de los casos hasta su resolución. Esto incluye la gestión eficiente de turnos, documentación, seguimiento de las intervenciones realizadas por profesionales, y la integración con sistemas externos como CiDi, asegurando la trazabilidad y confidencialidad de la información manejada.

#### Indicar la Delegación a la que pertenece la Aplicación

Dirección de Asistencia a la Víctima del Delito, dependiente de la Subsecretaría de Justicia del Ministerio de Justicia y Trabajo de la Provincia de Córdoba.

#### Indicar Responsable de la Aplicación (nombre, delegación a la que pertenece)

Facundo Álvarez - Director de Jur. Innovación Tecnológica del Ministerio de Justicia y Trabajo de la Provincia de Córdoba.

#### Indicar Desarrollador de la Aplicación (Nombre de los desarrolladores y en caso de desarrollo de tercero, indicar empresa)

Ginkgo Soft S.R.L. (nombre comercial Bitsion).

#### Fecha inicial prevista de implementación

Sin definición.

#### Tipo de Aplicación

Cliente Servidor	
Aplicación web	X
Otro (especificar)	

En caso de aplicación web, con front-end indicar url de esta

<https://gestionasistencia.cba.gov.ar/>**¿Utiliza API? S/N**

Sí

**Esta prevista la utilización de recursos de información externos (Renaper / Afip / otros)**

SI /NO

No

En caso afirmativo indicar orígenes

**Aplicación Disponible en ambientes**

Solo en ambiente productivo

No

Disponible en otros ambientes (Indicar cuales)

Desarrollo, Testing, Producción

**Zona de Acceso a la Aplicación**

Solo Interna

Solo Internet (confirmar globalidad de publicación)

Interna e internet

X

**Plataformas (indicar versión)**

Sistema Operativo

Windows Server

Publicador web (apache,iis, etc)

iis

Plataforma de desarrollo (visual studio, .net, etc)

Visual Studio, Visual Code

Lenguaje de Programacion (c#, javascript, etc)

c#, javascript

Conexión con base de datos (Externa, local)

local

Motor de base de Datos (oracle, sql)

Oracle

**Delivery de tráfico**

App preparada para balanceo de carga (si-no)

No

Requiere balanceo de carga (si, no)

No

**Gestión de recursos con contenedores**

Si dispone (indicar tecnología y orquestador)

No dispone

X

**Despliegue continuo**

Si requiere (indicar herramienta)

No requiere

X

**Despliegue en Nube**

La aplicación residirá en la nube (indicar proveedor y adjuntar SLA del proveedor)

No se desplegara en la nube

X

**Funcionalidades y cifrado**

La App requiere de envío de correos al exterior

Sí

No

Sí. Solo a cuentas internas

X

El acceso a la App dispone de Cifrado

Si, HTTPS – Revisar gestión de certificado

X

  	RP10 – Consideraciones Seguridad APP
Si, Otro (indicar)	
No dispone	

Dispone la App de registro de eventos

Si (Listar cuales)	X (Consultar)
No	

### Administrador de contenidos

Login de usuarios

Validación por cidi	X
Validación propia	
No dispone	

## 2. Listado de chequeo de aplicaciones para clasificación de criticidad

### 2.1. Objetivo

Determinar la criticidad de la información manejada para una aplicación.

### 2.2. Procedimiento de clasificación de la información

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: Confidencialidad, Integridad y Disponibilidad.

Confidencialidad (marque la que corresponda)	
La información es considerada pública. Puede ser conocida y utilizada por cualquier persona (sea empleado del Organismo o no) sin necesidad de autorización alguna.	
La información es sólo para uso interno. Puede ser conocida y utilizada por todos los empleados del Organismo y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizado podría ocasionar riesgos y/o pérdidas leves para el Organismo o terceros.	X
La información es confidencial. Puede ser conocida y utilizada solamente por un grupo de empleados y su divulgación o uso no autorizado podría ocasionar pérdidas significativas al Organismo o a terceros.	
La información secreta. Puede ser conocida y utilizada solamente por un grupo muy reducido de empleados, generalmente de la alta dirección del Organismo, y cuya divulgación o uso no autorizado podría ocasionar pérdidas graves al organismo o a terceros.	

Marque la que corresponda	Sí	No
¿Se asignan distintos permisos a las personas para realizar las modificaciones en la información o contenido?	X	
¿Se realiza el control de acceso de los usuarios a través de un login o algún otro mecanismo?	X	
¿En caso de haber seleccionado otro, especifique el tipo: Mediante CiDi .....		

Integridad (marque la que corresponda)	
La modificación no autorizada de la información puede repararse fácilmente o no afecta a la operatoria del Organismo.	
La modificación no autorizada de la información puede repararse, aunque podría ocasionar pérdidas leves para el Organismo o terceros.	
La modificación no autorizada de la información es de difícil reparación y podría	X

ocasionar pérdidas significativas para el Organismo o terceros.	
---	--

La modificación no autorizada de la información no podría repararse, ocasionando pérdidas graves al Organismo o a terceros.	
---	--

Marque la que corresponda	Sí	No
¿Afectaría a la reputación del Organismo las modificaciones no autorizadas de la información o contenido?	X	
¿La no veracidad de la información o contenido puede afectar de alguna manera al Organismo?	X	
¿La pérdida o el daño producido puede ser grave para el Organismo si la información o contenido es modificada sin autorización?	X	
¿La pérdida de información puede afectar a la operatoria del Organismo?	X	

Disponibilidad (marque la que corresponda)	
La inaccesibilidad a la información no afecta la operatoria del Organismo.	
La inaccesibilidad permanente a la información durante un plazo mayor a una semana podría ocasionar pérdidas significativas para el Organismo o terceros.	
La inaccesibilidad permanente a la información durante un plazo mayor a un día podría ocasionar pérdidas significativas al Organismo o a terceros.	X
La inaccesibilidad permanente a la información durante un plazo menor a un día podría ocasionar pérdidas significativas al Organismo, al Sector Público Provincial o a terceros.	

### 2.3. Evaluación de criticidad

Se asignará un valor de criticidad a la aplicación en relación a su objetivo o propósito. Y con esto, se clasificará la información en una de las siguientes categorías:

CRITICIDAD NULA  
CRITICIDAD BAJA  
CRITICIDAD MEDIA  
CRITICIDAD ALTA