U.A.E. CUERPO OFICIAL
BOMBEROS
BOGOTÁ D.C.

(Honor, Valor, Disciplina)

MANUAL DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

TIC-MN03

BOGOTÁ

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Para apoyar los procesos operativos y estratégicos de la UAECOB se debe realizar cambios e implantaciones en los sistemas por tal razón es necesario establecer lineamientos que deben cumplir los procesos de adquisición, desarrollo y mantenimiento de los sistemas garantizando que la seguridad de la información y ciberseguridad sea parte integral de estos.

Todo proyecto de desarrollo o adquisición de sistemas de información debe involucrar desde su fase de requerimientos de conceptos y puntos de vista del oficial de seguridad de la información quien debe apoyarse en las buenas prácticas previa aceptación de un sistema y en el marco regulatorio y jurídico que pueda influir en la sensibilidad de la información a ser tratada por este nuevo sistema de información o por cambios solicitados por los existentes.

2. MARCO LEGAL

Norma ISO 27001:2013
ISO/IEC 14598

3. OBJETIVO

Definir lineamientos de seguridad de la información y ciberseguridad, que permitan dar cumplimiento de la seguridad en todo el ciclo de vida del desarrollo de software, actualización y mantenimiento, para contar con sistemas de información seguros en la UAECOB.

4. ALCANCE

Este manual aplica a todos los niveles de la entidad que realicen funciones o tengan responsabilidades en los procesos de adquisición, desarrollo y mantenimiento de sistemas de información.

5. DEFINICIONES

Ambiente de desarrollo:

Conjunto de procedimientos y herramientas utilizadas por los desarrolladores para codificar, generar, depurar, actualizar, integrar, testear, validar y ejecutar programas[1].

Ambiente de prueba:

Es un término utilizado en el campo del software y desarrollo de sitios web previo a la producción. Describe la ubicación en la que se ven previamente los cambios en un sitio web o software y son ajustados antes de su publicación final**.**[2]

Ambiente de Producción:

Es donde están disponibles las funcionalidades necesarias de los softwares que automatiza un proceso de negocio[3].

Anexo de Seguridad de la Información:

Documento firmado entre las partes el cual define o establece los términos para el cumplimiento de buenas prácticas orientadas a una adecuada gestión de Seguridad de la Información alineadas a las políticas y/o definiciones implementadas en la UAECOB, como parte de una relación comercial o laboral[4].

Ciclo de Vida:

Conjunto completo de fases, transiciones y estados asociados en la vida de un servicio, producto o práctica.

Etapas consecutivas e interrelacionadas de un sistema del producto, desde la adquisición de materia prima o de su generación a partir de recursos naturales hasta la disposición final.

Derechos de propiedad intelectual:

Es el conjunto de normas que protegen al autor como creador de una obra en el campo literario y artístico, entendida ésta, como toda expresión humana producto del ingenio y del talento que se ve materializada de cualquier forma perceptible por los sentidos y de manera original[5].

Desarrollo Seguro de Software:

(Ciclo de Vida de Desarrollo de Software Seguro) es un proceso de desarrollo de software que ayuda a los desarrolladores a crear software más seguro y cumplir los requisitos de cumplimiento de seguridad, reduciendo al mismo tiempo los costes de desarrollo[6].

---

[1] Definición de la consultoría
[2] IBIDEM
[3] IBIDEM
[4] Definición de UAECOB
[5] FUENTE: http://www.cecolda.org.co/index.php/
[6] FUENTE: https://social.technet.microsoft.com/wiki/contents/articles/36676.ciclo-de-vida-de-desarrollo-seguro-de-software-es-es.aspx

Gestión del cambio:
(Práctica de gestión del cambio organizacional) Práctica que consiste en asegurar que los cambios que se realizan en una organización se implementan correctamente y sin contratiempos, y que los beneficios perduran gracias a la gestión del aspecto/factor humano[7].

Enmascaramiento u Ofuscación:
(Enmascaramiento de datos) es el proceso mediante el cual se cambian ciertos elementos de los datos de un almacén de datos, cambiando su información, pero consiguiendo que la estructura permanezca similar, de forma que la información sensible quede protegida[8].

Sistema de Información:
Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes que manejan información[9].

6. DESARROLLO

Para la UAECOB es muy importante la seguridad de la información, por tal razón se está desarrollando este manual con el fin de realizar un adecuado análisis de requerimientos y controles para el desarrollo, mantenimiento y adquisición de sistemas de información que brindan soporte a los procesos de la entidad.

Así mismo es importante tener en cuenta que la UAECOB incluirá controles de autenticación verificación en el análisis e implementación de los requerimientos de seguridad en el software y/o sistemas de información que se desarrollen o se adquieran y que se implementen buenas prácticas para un desarrollo seguro.

7. CONDICIONES GENERALES

Cuando los procesos hayan planificado la adquisición de un desarrollo, un mantenimiento o la adquisición de un sistema de información debe tener en cuenta los siguientes lineamientos:

[7] Glosario IT4+
[8] https://www.powerdata.es/enmascaramientode-datos
[9] ISO 27000:2018

i. La solicitud o requerimiento realizado se debe registrar de manera completa, clara y posible con todos los antecedentes o casos de uso necesarios para su buen funcionamiento.
ii. Que exista integración de los sistemas de información con los que cuenta la UAECOB.
iii. Que se ejecuten todas las pruebas necesarias antes de la puesta en funcionamiento en cualquier solución que se implemente.
iv. Que se documenten los sistemas de información y que se realicen las actualizaciones correspondientes cuando estas sean modificadas.
v. Toda adquisición, desarrollo o modificación de sistemas de información deberán incluir el suministro y/o actualización de la documentación correspondiente del sistema o módulo como las especificaciones funcionales, de seguridad, manual de Instalación y configuración; manual de administración, operación y mantenimiento, así como también el manual de usuario.
vi. Que sea actualizada la herramienta de inventario de sistemas de información con las modificaciones y adquisiciones que se generen.
vii. Que la seguridad de la información sea parte integral en el ciclo de vida de las aplicaciones.
viii. Que existan los ambientes de trabajo requeridos en el desarrollo de sistemas de información o implementación de sistemas de información que se adquieran (ambientes de desarrollo, pruebas, producción).
ix. Se entreguen los medios (programa fuente, programas objeto, licencias y manuales), de los sistemas de información para ser inventariados, contar con las garantías y licenciamientos como resultado de la adquisición o desarrollo realizado.

7.1 LINEAMIENTOS O RECOMENDACIONES

A continuación, se describen los lineamientos y las actividades necesarias para la adquisición, desarrollo y mantenimiento seguro de sistemas de información de la información.

Cumplimiento

Cada responsable que interviene en la correcta implementación de estos lineamientos de seguridad debe asumir la responsabilidad con la protección de los activos de información, basados en los riesgos de seguridad y ciberseguridad a los que puede estar expuesta la información.

Además, para dar cumplimiento con los lineamientos de seguridad, debe mantener tres ambientes independientes, uno para el desarrollo de software, otro ambiente para la realización de pruebas y un tercer ambiente para las operaciones de negocio basados en sistemas de producción y ningún ambiente puede influir en el desempeño y la seguridad de estos.

El proceso de gestión adquisición, desarrollo y mantenimiento de sistemas (sistema de información, programa o software) debe contemplar e incluir la gestión y procesamiento de datos personales; la Oficina de Tecnología como custodio de la información y los dueños de la información (dueño del proceso) como responsables de la información deben velar por el cumplimiento de todos los requisitos legales definidos en la Ley 1581 de 2012 para asegurar la debida protección de los datos personales.

Los lineamientos establecidos en este manual se deben impartir en la medida que desde la Oficina de Tecnología e Información se adquieren las herramientas o controles que ayuden al cumplimiento de cada uno de los aspectos de seguridad que se han establecido en éste.

7.2 Pautas o reglas

El proceso de gestión adquisición, desarrollo y mantenimiento de sistemas de información o software debe contemplar e incorporar como mínimo las siguientes reglas o características:

- Arquitectura de software
- Cifrado de datos
- Especificación de requerimientos
- Controles de seguridad de la información
- Calidad de software
- Estandarización de los mensajes de error y eventos de seguridad

- Seguridad informática
- Marco de interoperabilidad
- Metodologías de desarrollo
- Transferencia de los derechos patrimoniales sobre los productos desarrollados
- Documentación técnica y funcional
- Componentes de seguridad y privacidad de la información

7.2.1 Requisitos de seguridad para los sistemas de información

La seguridad de la información debe ser parte integral en el ciclo de vida de todos los sistemas de información o para mejoras de estos. Por tal razón se deben definir las medidas de seguridad desde la fase de análisis de requerimientos e incorporarlos en las etapas de desarrollo, implementación y mantenimiento.

7.2.2 Análisis y especificación de los requisitos de seguridad de la información

Los requerimientos para la seguridad de la Información deben ser identificados y definidos desde la etapa del diseño, adquisición de nuevas soluciones o mejoras a sistemas existentes, igualmente deben cumplir como mínimo con los siguientes lineamientos o recomendaciones:

- Los sistemas de información deben mantener durante su ciclo de vida una gestión de riesgo, que permita identificar los niveles de exposición de la información de la UAECOB, cualquier cambio en el ciclo de vida de un sistema debe seguir los lineamientos definidos en el procedimiento de Gestión de Cambios Tecnológicos.

- Los responsables de la provisión de nuevas soluciones o mejoras en la UAECOB deben crear y mantener un marco de trabajo que controle el ciclo completo de adquisición y/o desarrollo y mantenimiento de soluciones de información.

- Los sistemas de información durante todo su ciclo de vida deben preservar la confidencialidad, disponibilidad, integridad, cumplimento legal y protección de la información.

- Los grupos de cada una de los procesos de la UAECOB que tenga la necesidad de solucionar, agilizar un proceso a través del desarrollo, mantenimiento o adquisición de una solución, sistema o software informático deberán generar un documento en el cual se establezcan los requerimientos y necesidades a solucionar.

La Oficina de Tecnología e Información de la Entidad encargada de controlar los procesos de adquisición, desarrollo y mantenimiento de sistemas, debe evaluar los requerimientos realizados por el área que necesite un nuevo sistema, producto o servicio de mejoramiento de software, con el fin de establecer la viabilidad de la solicitud; una vez evaluados los requerimiento se debe decidir si el producto será desarrollado, adquirido, mejorado por la UAECOB o por un tercero, el resultado debe ser documentado e informado al área interesada.

Los procesos documentados para desarrollo y adquisición de sistemas deberán tener en cuenta:

a. Seguridad para los accesos lógicos basados en los requisitos de los procesos de la UAECOB.
b. Segregación de funciones, aplicando el principio del menor privilegio.
c. Programas de control de cambios y administración de configuraciones.
d. Controles de Backup y recuperación.
e. Capacidad de seguridad y monitoreo de violaciones a la información. (Logs)
f. Protección de la información basada en su clasificación.
g. Satisfacción con los requerimientos de negocio.
h. Afectación al plan de continuidad de negocio (BCP).
i. Aspectos relacionados con desarrollo seguro.

Para el desarrollo, compra y mantenimiento de sistemas se deben seguir entre otros los siguientes lineamientos o recomendaciones de seguridad:

a. Contar con soporte para el sistema de información durante su ciclo de vida.
b. Todas las aplicaciones o sistemas de información deben contar con un administrador formalmente asignado.

c. Cada aplicación debe ser analizada para identificar los riesgos y determinar los controles apropiados.
d. Los mecanismos de seguridad definidos para una aplicación específica no deben ser alterados, pasados por alto o comprometidos durante su ciclo de vida.
e. Los controles de seguridad deben ser documentados y probados.
f. El proceso de revisión del diseño de aplicación debe incluir consideraciones de seguridad y control para garantizar que los programas se hagan según lo previsto.
g. El software desarrollado o comprado no debe reducir los niveles de seguridad establecidos en este manual.
h. El software no debe usar funciones privilegiadas del sistema operativo.
i. El equipo de desarrollo de sistemas y el administrador del sistema de información, son responsables de efectuar pruebas para asegurar que se han cumplido los requerimientos de seguridad.
j. En el caso que terceros sean contratados para desarrollar software, éstos deben cumplir con los lineamientos de seguridad para el desarrollo de software que se haya establecido en los acuerdos del contrato.
k. Los contratos relacionados con el desarrollo de sistemas por los funcionarios de la UAECOB, personal contratista, o por agentes externos a favor de la UAECOB deben indicar claramente los derechos de propiedad intelectual.
l. Todas las copias y documentación del software desarrollado para la UAECOB deben incluir los derechos de uso y propiedad en el documento de licenciamiento.
m. Debe existir un grupo interdisciplinario que ejerza la supervisión y control en todo proceso de compra, desarrollo y mantenimiento de aplicaciones. Conjuntamente el grupo debe realizar el análisis del requerimiento.
n. Deben existir mecanismos y herramientas para garantizar el control de versiones en los desarrollos de la UAECOB.
o. Si se adquiere un sistema el supervisor del contrato, debe validar que se cumplen los requerimientos, de la documentación, se respetan los derechos de marca, propiedad, garantía y licencia y, debe verificar si se tiene contemplado un soporte en todo su ciclo de vida.

7.2.3 Trazabilidad de las operaciones mediante LOGS

Se debe contemplar la implementación o parametrización de logs de eventos, con el fin de evidenciar actividades o accesos no permitidos a los sistemas de información que puedan causar violaciones a la confidencialidad, integridad o al no repudio, relacionando como mínimo los siguientes registros en el log.

a. Identificación del usuario.
b. Fecha, hora y detalle del acceso al sistema (log-on) y salida del sistema (log-off).
c. Identificación de la IP de donde se accede.
d. Registro de accesos exitoso o fallido.
e. Cambios en la configuración del sistema.
f. Hora de inicio y hora final de la actividad durante su logueo.
g. Estado (Create, Insert, Delete, Update).
h. Tiempo de retención del log

Además, se debe contemplar registro de eventos en los logs en los siguientes casos:

a. Creación, eliminación y modificación de datos.
b. Creación, eliminación y modificación de perfiles de usuario.
c. Cambios en la configuración o parametrización del sistema de información o base de datos.
d. Tiempo de la actividad en que se ejecutó y tiempo de finalizada la actividad.
e. Eventos que señalen alguna falla en la base de datos, desconexión o truncamiento de la base de datos.

7.2.4 Requerimientos funcionales de seguridad

- **Confidencialidad**

Considerando la clasificación para los activos de información de la UAECOB cada aplicación debe proveer los mecanismos para proteger la confidencialidad con base en su nivel de criticidad. (Cifrado, Control de Acceso y Registro Logs).

Los mecanismos de las aplicaciones desarrolladas para la UAECOB deben proveer:

a. **Cifrado de datos catalogados como públicos clasificados y públicos reservados:** Opción de cifrar los datos en tránsito (Ejemplo: VPN) y almacenamiento con un algoritmo criptográfico fuerte.

b. **Control de acceso:** Mecanismos de autenticación por usuario y contraseña siguiendo la política de control de acceso a la información de la UAECOB. Este control de acceso debe establecerse para cada activo de información con base en los accesos definidos por cada grupo responsable de los datos o por cada dueño de la información.

c. **Registro:** Permitir la parametrización para generar el registro en logs de eventos que permitan registrar los accesos a la información y así poder evidenciar potenciales violaciones a la confidencialidad de la información.

- **Integridad**

Para proteger la integridad de la información las aplicaciones deben desarrollar las siguientes utilidades, y deben ser aplicadas con base en la clasificación del activo de información:

a. **Control de acceso:** Equivale a la funcionalidad descrita para la protección de la Confidencialidad.

b. **Verificación por Hashing:** Opción que permita validar la integridad de los datos almacenados y/o transmitidos utilizando un campo de hashing que se genere con el algoritmo de cifrado fuerte, para las aplicaciones o sistemas de información críticos.

c. **Registro:** Permitir la parametrización para generar el registro en logs de eventos que permitan registrar los accesos a la información y así poder evidenciar potenciales violaciones a la integridad de la información.

- **Disponibilidad**

Para cumplir con los requerimientos de disponibilidad de la información y del sistema, se debe garantizar la validación de entradas de datos, procesamiento y calidad de datos, autenticación entre las interfaces del sistema.

7.2.5 Seguridad en los procesos de desarrollo y de soporte

- **Ambiente de desarrollo**

Juntamente con la evaluación de riesgos, realizada según la metodología de evaluación y tratamiento de riesgos de la UAECOB, se debe realizar periódicamente la evaluación de los siguientes aspectos:

a. Los riesgos relacionados con el acceso no autorizado al ambiente de desarrollo.
b. Los riesgos relacionados con los cambios no autorizados sobre el ambiente de desarrollo.
c. Las vulnerabilidades técnicas de los sistemas de TI utilizados en la UAECOB.
d. Los riesgos que puede traer una nueva tecnología para la UAECOB.

Es imprescindible y fundamental aplicar la metodología de riesgos en cada etapa del ciclo de vida de desarrollo de software y, así mismo, a cada uno los proyectos e iniciativas de desarrollo y adquisición de sistemas de información.

El uso de una metodología de análisis de riesgos permite gestionar de manera adecuada los riesgos que puedan afectar al negocio, como lo son los fraudes, afectación a los ciudadanos, fuga de información, incumplimientos regulatorios, impacto reputacional o imagen, impactos operativos, impactos financieros. Así mismo, debe aumentar el nivel de madurez de seguridad de la información y ciberseguridad de la Entidad.

Los cambios a los sistemas de información dentro del ciclo de vida se deben controlar mediante la aplicación de los lineamientos definidos en el “Procedimiento de Gestión de Cambios Tecnológicos”, con el fin de minimizar el impacto en las operaciones de negocio.

- **Principios para desarrollo de sistemas seguros**

Para el desarrollo de software en la UAECOB se definen en este manual los lineamientos que garantizan la seguridad en el ciclo de vida del desarrollo del software, igualmente se deben diseñar controles adecuados en las aplicaciones existentes en la

UAECOB, para garantizar un correcto procesamiento de datos, validación de los datos entrada y de salida, validación de mensajes de error, conciliación de datos al cerrar las transacciones, etc.

Las aplicaciones o sistemas que se desarrollen en la UAECOB deben cumplir con principios mínimos de seguridad, para minimizar las brechas de seguridad, pérdidas y modificaciones no autorizadas o usos indebidos en la información de las aplicaciones, estas medidas deben ser dadas conforme a las buenas prácticas de metodologías de desarrollo seguro y normativa vigente.

- **Ambiente de Producción**

En este ambiente se encuentran las aplicaciones, archivos, bases de datos y demás, que soportan las operaciones de negocio en la UAECOB, por tal razón se deben considerar los siguientes requisitos:

a. Los analistas de desarrollo de sistemas de información no deben tener acceso al ambiente de producción.
b. Los cambios a los sistemas de información dentro del ciclo de vida del desarrollo y de las pruebas, e implementación en producción, se deben controlar mediante la aplicación de los lineamientos definidos en el “Procedimiento de Gestión de Cambios Tecnológicos”, con el fin de minimizar el impacto en las operaciones de negocio.

c. Para la atención de problemas en producción, será a través de un cambio aprobado y de conocimiento por el dueño de la información (dueño del proceso) contenida en el sistema de información y éste debe ser implementado por el administrador del sistema de información y/o base de datos.

d. Los cambios de emergencia cuando ocurren problemas bien sean de programas, de operación, de grabación o por deficiencia del sistema, deben ser evaluados, estar aprobados, gestionados por el área de desarrollo, documentados y presentados posteriormente socializados en la reunión de cambios.

e. Los cambios de emergencia sobre datos en producción deben ser autorizados por el dueño de la información, se deben documentar las razones del cambio, para

posterior revisión y formalización del cambio desde la plataforma de gestión de cambios.

f. Los datos deben ser sometidos a procesos de enmascaramiento u ofuscamiento con rutinas aprobadas.

g. Los grupos de la Entidad donde se gestionen datos personales deben implementar controles de cifrado sobre los sistemas de información, carpetas o archivos que manejen información personal.

- **Ambiente de Pruebas**

a. En la fase de pruebas de los sistemas de información desarrollados o adquiridos, no se deben utilizar datos de producción.

b. En el caso de que se llegare a utilizar datos de producción, estos deben ser entregados a un funcionario responsable de los mismos, quien debe firmar acuerdo de confidencialidad sobre los datos recibidos para pruebas. Una vez terminadas las pruebas estos deben ser borrados de manera segura.

c. En cumplimiento de los requisitos legales de privacidad y seguridad de la información, los datos de prueba no deben contener información que permitan la identificación de la persona natural o jurídica a la que pertenezca la información.

d. No se permite el acceso desde el ambiente de pruebas al ambiente de producción.

e. Los analistas de desarrollo de sistemas de información, software o proveedores deben tener un ambiente de pruebas con una separación entre infraestructura, plataforma y aplicaciones; conjuntamente deben tener datos enmascarados o transformados para proteger la confidencialidad de la información esto aplica para todas las plataformas.

f. Las pruebas deben dar evidencia de que los controles diseñados e implementados van a proteger la información contra acceso, divulgación, modificación, destrucción y uso no autorizado de la información.

g. Los datos deben ser sometidos a procesos de enmascaramiento u ofuscamiento con rutinas aprobadas. Cuando los datos deban ser usados en el ambiente de

pruebas, teniendo la autorización del responsable y/o custodio de la información.

h. Se deben analizar los riesgos y controles complementarios sugeridos, cuando se requieran copias de la información de los ciudadanos para la realización de pruebas contemplando controles necesarios para garantizar su destrucción, una vez concluidas las mismas.

i. El set de pruebas de seguridad debe permitir el análisis y la auditoría de la aplicación en todos los componentes, así como el análisis de la aplicación basado en pruebas de penetración y pruebas de seguridad, que permitan demostrar vulnerabilidades en el sistema. Para esto es importante:

- Integrar las pruebas al proceso de desarrollo de software.
- Establecer procesos que optimicen las pruebas de seguridad, alineadas a los requerimientos del negocio.
- Realizar pruebas de seguridad durante todo el ciclo de vida de desarrollo de software.
- Utilizar herramientas automatizadas y de confianza, así como personas con las habilidades apropiadas para la ejecución de estas.

La metodología de análisis de seguridad para la detección de brechas de seguridad, deben incluir las siguientes acciones:

- Análisis de Vulnerabilidades durante y después del desarrollo del software.
- Pruebas de Intrusión o de Penetración en la puesta en producción.
- Revisión y análisis de código estático.
- El ambiente no puede ser utilizado para evadir los controles de seguridad establecidos.
- Cualquier falla de seguridad en las pruebas del sistema de información o software, detectada y que no pueda ser contralada antes del paso a producción, debe ser reportado al Oficial de Seguridad de la Información y Ciberseguridad.

7.2.6 Programas fuente y objeto

a. En los desarrollos o adquisiciones de sistemas de información, los programas fuente y objeto deben ser entregados y recibidos por los funcionarios responsables

de su control.

b. Debe existir un área o funcionario responsable de la entrega de programas fuente que van a ser modificados y de su recepción una vez sean puestos en producción. Así mismo, para recibir los programas fuente y objeto producto de la adquisición de un nuevo sistema de información.

c. Personal ajeno al ambiente de desarrollo-pruebas no debe tener por ningún motivo de acceso a programas fuente, a utilitarios, a líneas de comando que puedan colocar en riesgo los sistemas de información.

d. El personal de soporte de TI debe tener acceso restringido a las librerías de programas fuente.

e. Se debe mantener un registro de auditoria de todos los accesos a las bibliotecas de programa fuente.

f. Las viejas versiones de los programas fuente deben ser archivadas con una clara indicación de las fechas y horas precisas en las cuales estaban en operaciones, junto con todo el software de soporte, el control de tareas, las definiciones de datos y los procedimientos.

g. El mantenimiento y la copia de los códigos fuentes de programas deben estar sujetas a los procedimientos estrictos de control de cambios.

7.2.7 Desarrollo Contratado por un Tercero

a. La UAECOB debe contar con un procedimiento para la selección de proveedores, en el cual se incluya los criterios para la evaluación de propuestas y para la ponderación del cumplimiento de los requerimientos.

b. Los procesos que participan en la selección y evaluación de proveedores tendrán la responsabilidad de preparar y negociar un contrato con el proveedor, estableciendo los requerimientos de la adquisición, incluyendo costos y plazos del producto, sistema o servicio de software a entregar. El contrato debe tener en cuenta los derechos de marca, uso, propiedad intelectual, garantía y licenciamiento.

c. Por cada proyecto o servicio contratado deberá tener un líder de proyecto en la UAECOB, encargado de velar por el cumplimiento de los acuerdos definidos.

d. Todo desarrollo a través de un tercero o de adquisición, debe contener los siguientes aspectos de seguridad de autenticidad del software:

- Derechos de Autor.
- Requerimientos mínimos de seguridad y calidad de datos.
- Licencia para uso del software desarrollado o adquirido.
- Aviso de uso y privacidad del software.

7.2.8 Pruebas de funcionalidad y aceptación de sistemas

El plan de pruebas debe describir las actividades que se efectuarán para demostrar que los sistemas cumplan con los requisitos previamente definidos.

a. Se deben definir procedimientos de pruebas de funcionalidad de los sistemas y aceptación de estos, para los sistemas de información nuevos, actualizaciones y nuevas versiones.

b. La aceptación de los sistemas debe ser basada en la estrategia y los criterios de aceptación definidos por la Oficina de Tecnologías e Información. Se debe tener en cuenta la preparación de los casos, datos, procedimientos y entorno de las pruebas, además, si aplica se debe establecer en qué grado se debe involucrar al proveedor.

c. Las pruebas técnicas y de funcionalidad del producto o servicio de software solo se debe aceptar cuando el producto satisfaga todas las condiciones de aceptación definidas.

d. Para la aceptación de los sistemas se debe cumplir con los criterios de evaluación definidos y validados por Seguridad de la Información definidas de la UAECOB.

e. Una vez se haya definido la adquisición del software, la Oficina de Tecnología e Información debe asumir la responsabilidad para la gestión de la configuración del software entregado, mediante el Procedimiento de Gestión de la Configuración.

7.2.9 Seguridad de servicios de las aplicaciones en redes y protección de transacciones

Se deben definir mecanismos que garanticen la protección de la información que se involucre en sistemas de información o aplicaciones que pasan sobre redes, evitando actividades de fraude, divulgación o modificación de información no autorizada entre otros.

Se debe garantizar integridad en la información involucrada en las transacciones de servicios de aplicaciones, previniendo la transmisión incompleta, el enrutamiento errado, la alteración no autorizada, la duplicación o reproducción de mensajes.

Toda aplicación en la cual se establezca la realización de operaciones sobre redes públicas deberá cumplir como mínimo con los siguientes requerimientos:

a. Se deben implementar algoritmos y protocolos necesarios para brindar una comunicación segura.

b. Realizar como mínimo una vez al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados en la realización de transacciones por este canal. Sin embargo, cuando se realicen cambios en la plataforma que afecten la seguridad del canal, se debe realizar una prueba adicional.

c. Cada sistema de información debe cumplir con tiempos máximos de inactividad cuando la sesión de ingreso al sistema se haya establecido y, ésta deje de ser utilizada, solicitando un nuevo proceso de autenticación para ingresar (time out).

d. Todos los escaneos de vulnerabilidades y pruebas de penetración deben ser ejecutadas por el proveedor que la UAECOB ha autorizado para realizar estas actividades.

7.2.10 Aseguramiento del Ambiente de las Aplicaciones

El proceso de aseguramiento pretende conocer, construir y mantener las garantías sobre el ambiente en el cual se ejecuta la aplicación, mejorando la postura de seguridad de cada componente de la solución y de la aplicación misma.

La Oficina de Tecnología e Información, debe velar porque los ambientes tecnológicos sean revisados y asegurados a través de la implementación de buenas prácticas de seguridad, herramientas tecnológicas y diversas capas de monitoreo y defensas que limite el riesgo y los daños que puedan ser causados por la explotación de una vulnerabilidad, para lo cual debe:

a. Establecer y mantener la línea base de configuración del ambiente para la correcta ejecución de la aplicación y de cada uno de los componentes.
b. Identificar e instalar las actualizaciones y parches de seguridad.
c. Monitorear el estado de las líneas base de configuración del ambiente que soporta las aplicaciones.
d. Validar el estado de salubridad del ambiente respecto de las mejores prácticas.
e. Incluir dentro del programa de auditoría la verificación de la configuración del ambiente.
f. Establecer apropiadas listas de control de acceso.

7.2.11 Capacitación y Desarrollo de Capacidades

El personal que es responsable y que interviene en las diferentes etapas del ciclo de vida del desarrollo de software debe contar con las capacidades y conocimientos necesarios en los diferentes tópicos de desarrollo seguro, entre éstos están:

a. Realizar capacitaciones y entrenamientos técnicos en seguridad.
b. Construir y mantener actualizadas las guías técnicas para desarrollo seguro.
c. Realizar capacitaciones y entrenamientos para roles específicos dentro del aseguramiento de aplicaciones.
d. Generar sesiones con expertos de seguridad para mejorar los conocimientos y aplicación de buenas prácticas de seguridad, a los equipos que intervienen en el ciclo de vida de desarrollo.
e. Definir bases de datos de conocimiento con los tópicos más relevantes de seguridad de las aplicaciones.

7.2.12 Seguridad en aplicaciones móviles

Los dispositivos móviles corporativos (teléfonos inteligentes, Tablet, portátiles), son herramientas de trabajo que se deben utilizar únicamente para el desarrollo de actividades relacionadas con los procesos de la Entidad, es así como:

a. Las aplicaciones móviles deben responder a la necesidad de proteger los datos de las aplicaciones de negocio y en especial aquellos que son sensibles como los datos de las personas e información crítica de la UAECOB.

b. La información debe ser procesada, almacenada y transmitida de acuerdo con su clasificación, suministrada por el dueño del proceso, aplicación o sistema de información, validando a su vez la seguridad de la API que hace llamado a la información sensible desde estos dispositivos móviles, además la información no debe quedar en los dispositivos móviles.

c. Cuando se almacenen datos sensibles en el dispositivo (sólo en caso de ser estrictamente necesario), se debe utilizar mecanismos de cifrado de archivos apropiados y seguros.

d. Verifique que a nivel de seguridad de almacenamiento y sistema operativo esté habilitado y que el dispositivo esté protegido por un PIN o código de seguridad.

e. Las aplicaciones móviles deben implementar mecanismos de manejo de sesiones para prevenir el acceso no autorizado a la aplicación y a sus datos.

f. Los controles de autenticación y autorización deben ser implementados en el servidor y no en el dispositivo.

g. Para los mecanismos de autenticación basados en contraseñas, asegure la existencia de una política de seguridad que garantice el cumplimiento de esta.

h. Implemente mecanismos de protección ante ataques de fuerza bruta para los controles de autenticación en los dispositivos móviles.

i. Asegure que cualquier dato colectado está en cumplimiento con los requerimientos dados por las regulaciones locales.

j. Se debe hacer uso de factores de autenticación múltiple para las aplicaciones que dan acceso a datos sensibles (algo que sé, algo que tengo, algo que soy), desde dispositivos móviles.

k. Se debe hacer uso de credenciales de usuario «Handle Password Credentials Securely» para este control se indican los siguientes aspectos de seguridad:

- Nunca almacene la contraseña en texto claro.
- En lo posible, hacer uso de tokens, Como OAuth (que permiten determinar a qué se solicita acceso por parte de la aplicación y a qué se autoriza acceder por parte del usuario).
- No almacene ninguna contraseña en el código fuente de aplicaciones.
- Asegure que los datos en tránsito viajen protegidos y cifrados desde los dispositivos móviles, debido a que pueden ser interceptados y modificados.

7.2.13 Servicios de Back-End, Servidores de la Plataforma Móvil y las APIs

Se debe contar con medidas específicas para proteger los backends de aplicaciones móviles, Esto incluye el aseguramiento de los Web Services, APIs y protocolos empleados para conectarse con las plataformas de back-end, así como la infraestructura tecnológica y software utilizado por la aplicación móvil, además:

- Se debe analizar periódicamente en busca de vulnerabilidades.
- Mantener el servidor de la plataforma móvil, completamente actualizado.
- Establecer los mecanismos necesarios para llevar a cabo un análisis forense, si de un incidente se trata.
- Utilizar medidas para prevenir ataques de denegación de servicio.

7.2.14 Protección de la Privacidad en dispositivos Móviles

Los diseños de aplicaciones móviles deben evitar la divulgación de la información personal o privada desde el dispositivo móvil.

La seguridad del software en los dispositivos móviles debe contemplar actualizaciones teniendo en cuenta los siguientes aspectos:

- No distribuya las aplicaciones a través de repositorios inseguros.
- Las aplicaciones deben estar diseñadas para aceptar actualizaciones de seguridad.
- Establezca canal de comunicaciones seguros, para que los usuarios pueden reportar fallos de seguridad a través de éstos.

Tenga en cuenta, a la hora de desarrollar una aplicación móvil aspectos importantes que pueden ser identificados como buenas prácticas en la construcción de software para dispositivos móviles, entre éstos contemplar:

- La validación de todas las entradas de información.
- Minimizar las líneas de código y su complejidad.
- Utilizar analizadores de código, para buscar fallos de seguridad.
- Utilizar funciones seguras con el fin de prevenir desbordamientos de búfer, etc.
- Ejecutar las aplicaciones con el mínimo nivel de privilegios.

Los atacantes pueden forzar a la aplicación a utilizar datos especialmente diseñados que modifiquen la lógica de la aplicación móvil, evadiendo los controles de acceso y de divulgación de información, para lo cual es importante asegurar la aplicación con sensores biométricos que pueden ser aplicados por hardware seguro o utilizar doble factor de autenticación para los funcionarios de la UAECOB.

7.2.15 Documentación

El desarrollo, adquisición y mantenimiento de sistemas de información o software es un proceso imprescindible en la Entidad, por tal motivo es necesario incorporar en la entrega de estos productos, las pruebas y la documentación que son a su vez un factor de soporte en todo el ciclo de vida del desarrollo del software. Es así como se relaciona la siguiente documentación para que se contemple en todas las entregas de estos productos:

- Modelo entidad relación de la base de datos.
- Inventario de versionamiento de los sistemas de información o software.
- Informe de la estructura de los datos.
- Manual de Usuario.
- Manual Técnico.
- Manual de Instalación.
- Informe de pruebas funcionales.
- Informe de pruebas de vulnerabilidades y remediadas.
- Informe de aseguramiento o hardening para el componente hardware.
- Acta de control de cambios para la puesta en producción.

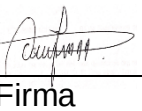
1. DOCUMENTOS RELACIONADOS

CÓDIGO	DOCUMENTO
	Herramienta de clasificación de activos de la información

2. CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
01	31/12/2021	Creación del documento

3. CONTROL DE FIRMAS

Elaboró José Hernán Morales Martha Patricia Mateus	**Cargo** Contratista OAP Contratista OAP	Firma  
Revisó Cristian Suarez Oswaldo García	**Cargo** Vo.Bo. de Mejora Continua - OAP Líder de Tecnología OAP	Firma  
Aprobó Hernando Ibagué Rodríguez	**Cargo** Jefe (Encargado del 27 al 31 de diciembre 2021) Oficina Asesora de Planeación	Firma