1 OBJETO

Establecer un procedimiento que brinde los lineamientos de seguridad para las aplicaciones y servicios de negocio para la Previsora y la infraestructura que los soporta.

2 ALCANCE

Estos lineamientos se deben tener en cuenta para la implementación y mejoramiento de los servicios tecnológicos y las aplicaciones de la Previsora Seguros S.A en las fases de adquisición, desarrollo y mantenimiento teniendo en cuenta los parámetros de seguridad requeridos en la arquitectura que los soporta, ya sea que se encuentre a cargo de la Previsora o de un tercero.

CONTENIDO

3 DEFINICIONES

- **PLATAFORMA TECNOLÓGICA:** Es un conjunto de hardware y software que cumplen una función específica para prestar algún servicio.

- **APLICACIONES:** Son programas diseñados como herramienta que permite al usuario realizar diferentes tipos de trabajo.

- **BASES DE DATOS:** Conjunto de datos interrelacionados que pertenecen a un mismo contexto almacenados sistemáticamente.

- **COMUNICACIONES:** Conjunto de servicios, redes, software y equipos de comunicaciones que tienen como fin la mejora de la calidad de las comunicaciones entre diferentes sitios.

- **OFIMÁTICA:** Conjunto de herramientas utilizadas en oficina y se usan para diferentes funciones como crear, modificar, organizar, escanear, imprimir diferentes documentos.

- **DOMINIOS DE ASEGURAMIENTO:** Se define como los componentes de la infraestructura tecnológica a proteger como lo es **(**Aplicaciones, Sistemas Operativos, Bases de Datos y Comunicaciones)

- **PROVEEDOR:** Empresa o persona física, cuya actividad busca responder las necesidades del Cliente, que por su característica principal de servicio es intangible, pero así mismo el servicio está apoyado por bienes tangibles para lograr dicha actividad.

- **SISTEMA OPERATIVO:** Es un programa o conjunto de programas de un sistema informático que permite la administración eficaz de los recursos materiales, del usuario y de las aplicaciones.

- **APLICATIVO CORPORATIVO:** El aplicativo corporativo hace referencia a lineamiento de Grupo Aval, para la adquisición de un producto de un proveedor en particular, con un contrato macro, y políticas definidas para las filiales a nivel grupal.

- **APLICATIVO NO CORPORATIVO:** El aplicativo o desarrollo adquirido con un terceo, o ejecutado directamente en la compañía para fines particulares adaptados al negocio, con lineamientos internos.

- **OWASP:** The Open Web Application Security Project. Proyecto de seguridad para aplicaciones web de código abierto.

- **SDLC:** Software Development Life Cycle. Ciclo de vida de desarrollo de software.

- **SOFTWARE:** Programas y documentación de apoyo que permiten y facilitan el uso de la computadora además de automatizar procesos. El software controla el funcionamiento del hardware y el procesamiento de datos.

- **HARDWARE:** Conjunto de componentes físicos de un sistema informático.

- **VULNERABILIDAD:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

- **INTEGRIDAD:** Capacidad que garantiza que el código del software, activos manejados, configuraciones y comportamientos no puedan ser o no hayan sido modificados o alterados.

- **DISPONIBILIDAD:** Capacidad que garantiza que el software es operativo y accesible por los usuarios a quien va destinado.

- **CONFIDENCIALIDAD:** Capacidad que garantiza que el software preserva cualquiera de las características, activos manejados, ocultos o no accesibles a usuarios no autorizados.

- **AMENAZA:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

- **RIESGO:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

- **ACTIVO:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

- **HASH:** Función que asigna una cadena de longitud arbitraria a un valor de tamaño fijo de una manera determinista. Tal función puede o no tener aplicaciones criptográficas.

- **AMBIENTE DE PRUEBA:** Un ambiente de prueba describe la ubicación en la que se ven previamente los cambios en el software y son ajustados antes de su publicación final.

- **AMBIENTE DE DESARROLLO:** Un ambiente de desarrollo proporciona servicios integrales para dicha función, desarrollar software, permitiendo el uso de herramientas y funcionalidades no permitidas en ningún otro ambiente en forma “libre” para los usuarios de dicho ambiente.

- **AMBIENTE DE PRODUCCIÓN:** Es el entorno funcional de los procesos de negocio, cuyos usuarios son los funcionarios del ministerio, terceros y público en general y donde se captura, procesa y transforma los datos del negocio.

4 CONDICIONES GENERALES

4.1 POLÍTICA

Los activos de información tecnológicos que soporten el negocio de La Previsora y/o interactúen con terceras partes deben contar con estándares de aseguramiento y cumplir con la Circular CIR-375 POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

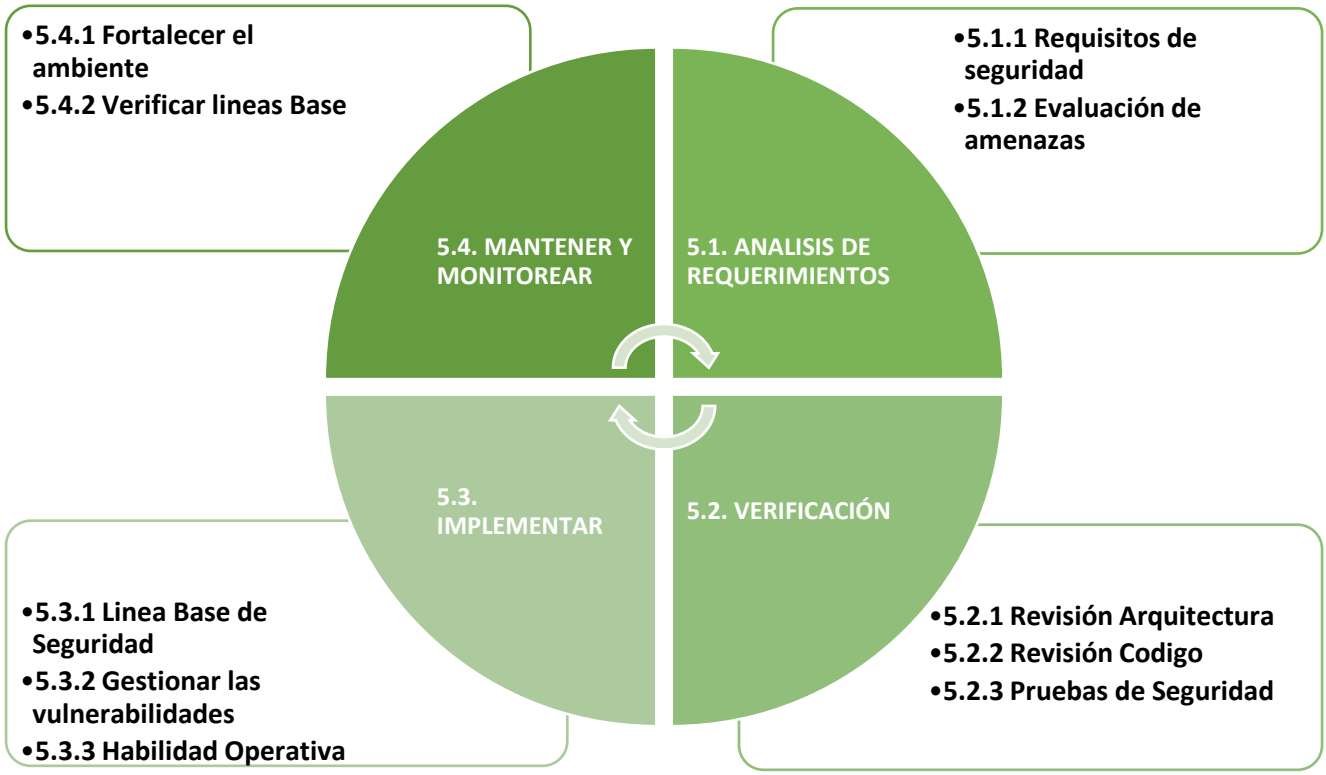
4.2 NORMAS GENERALES

- La implementación de las líneas base de Seguridad deben ejecutarse antes de que la plataforma o la aplicación ingresa a producción.
- Establecer buenas prácticas de seguridad para implementar el aseguramiento en las plataformas de la infraestructura tecnológica en cuanto a Aplicaciones, Sistemas Operativos, Bases de Datos y Comunicaciones de La Previsora S.A.
- Todos los activos de información tecnológicos de La Previsora deben cumplir con la implementación de los Líneas Base de Seguridad.

- Los Líneas Base de Seguridad de activos de Información tecnológicos deben ser actualizados periódicamente en relación a los cambios significativos que se presenten en cuanto a:
    - Actualizaciones de software o plataforma.
    - Nuevas versiones de los componentes de infraestructura tecnológica.
    - Exposición de vulnerabilidades
    - Nuevas tecnologías relacionadas con los componentes tecnológicos que soportan negocio.
- Los componentes de infraestructura tecnológica de La Previsora custodiados y/o administrados por terceros, deben cumplir con los Líneas Base de Seguridad definidos y aprobados por La Previsora.
- El proveedor de un componente de infraestructura tecnológica debe establecer las mejores prácticas de Seguridad para el aseguramiento de la plataforma tecnológica estándar y no estándar de La Previsora y sus filiales.
- Establecer buenas prácticas de seguridad para implementar el aseguramiento en las plataformas de la infraestructura tecnológica en cuanto a Aplicaciones, Sistemas Operativos, Bases de Datos y Comunicaciones de La Previsora y sus filiales.
- Los Líneas Base de Seguridad se deben aplicar a servicios tecnológicos y a usuarios. En servicios tecnológicos como Sistemas Operativos, Aplicaciones, Bases de Datos y Comunicaciones; y en usuarios como Ofimática, Contraseñas y Accesos.
- Las aplicaciones sean internas o externas deben contar con buenas prácticas de configuración, así como uso de protocolos seguros.
    - Aplicaciones Internas: WEB deben contar con certificado SSL expedido por la enditas certificadora interna.
    - Aplicaciones externas: WEB deben contar con certificado SSL expedido por un ente externo legal certificado.
- Las aplicativos y servicios de TI de La Previsora se debe contar con la separación de los ambientes (Segmentación de Red) en ambientes de desarrollo, pruebas y producción
- La plataforma IT no estándar debe contar con un respaldo y/o manual de configuración segura, emitida por el proveedor. Con el fin de garantizar que la plataforma y/o desarrollo sean confiables.

5 SLDC - **CICLO DE VIDA DE DESARROLLO DEL APLICACIONES.**

El siguiente documento mostrara una guía práctica para tener encuentra tanto en la adquisición de software como en el desarrollo seguro e implementación de aplicaciones y servicios de TI basado de metodologías SLDC (ciclo de vida desarrollo de software y OWASP. Teniendo en cuenta las siguientes etapas.



Ilustracion1. Fases de Seguridad en desarrollo seguro, implementación de aplicaciones y servicios de TI

5.1 ANÁLISIS DE REQUERIMIENTOS

Etapas	ACTIVIDADES
5. 1.1 Requisitos de seguridad	Como inicio de esta fase se debe contemplar y definir los riesgos de seguridad a los que estará expuesta la aplicación o servicio de TI; para definir de forma adecuada estos riesgos se deben realizar los siguientes pasos: 1. Conformar un grupo de análisis de riesgos entre el área dueña del proyecto, tecnología, seguridad informática y seguridad de la información. 2. Descomponer la aplicación e identificar componentes clave (como arquitectura física y lógica, niveles de aplicación, presentación y base de datos, etc). 3. Determinar los riesgos asociados a cada componente de la aplicación o servicio. 4. Asignar un valor a cada riesgo. 5. Decidir cómo responder a los riesgos ante una materialización. 6. Identificar las técnicas, tecnologías o controles necesarios para mitigar los riesgos identificados. Aunque los riesgos se definen por medio de los pasos indicados anteriormente existen algunos riesgos que son inherentes independiente del tipo de aplicación o servicio, los cuales deben ser contemplados en el análisis y son los siguientes:

	Riesgos generales de desarrollo de una aplicación 1. Spoofing Identity: Suplantar la identidad de otro usuario o servicio. 2. Tampering with Data: Modificar maliciosamente datos almacenados. 3. Repudiation: Imposibilidad de identificar el autor de una acción. 4. Information Disclosure: Divulgar información a usuarios no autorizados. 5. Denial of Service: Provocar que un servicio deje de funcionar. 6. Elevation of privilege: Conseguir privilegios mayores a los asignados. Adicional a los riesgos asociados al desarrollo o implementación de la aplicación o servicio, se debe definir la valoración de los mismos para lo cual se debe seguir: Factores para determinar el nivel de riesgo 1. Damage Potencial: ¿Qué tan importante es el daño de esta amenaza? 2. Reproducibility: ¿Qué tan reproducible es la vulnerabilidad? 3. Exploitability: ¿Qué tan fácil es de explotar? 4. Affected Users: ¿Cuáles y cuántos usuarios se verían afectados? 5. Discoverability: ¿Qué tan fácil de descubrir es la vulnerabilidad?
5.1.2 Evaluación de amenazas	Después de realizar la evaluación de los riesgos, dicha evaluación da como resultado el análisis de los riesgos que deben ser mitigados estableciendo los requerimientos de seguridad, estos requerimientos deben ser integrados en la arquitectura, diseño y construcción de la aplicación o servicio; como requerimientos básicos se indican los siguientes, los cuales deben validarse teniendo en cuenta el documento “FO-STI-002 Lista de Verificación Lineamientos de Seguridad”. 1. Capa de Aplicación a. Aplicaciones expuestas a internet. b. Validación de entradas. c. Administración de autenticación y contraseñas. d. Manejo de errores y logs. e. Protección de datos del sistema. f. Manejo de archivos En caso de que el Portal dentro de sus funcionalidades requiere el cargue de archivos por parte delcliente: g. Control de Acceso. h. Prácticas de Codificación. 2. Capa de Comunicación a. Capa de Sistema Operativo. b. Sistema Operativo. c. Servidores de aplicación (Web).

	d. Privilegios en el entorno de ejecución. 3. Capa de Base de Datos. 4. Soporte al Portal o sitio web. 5. Controles de acceso a la red. 6. Controles servicios en la nube.

5.2 VERIFICACIÓN

Etapas	ACTIVIDADES
5.2.1 Revisión Arquitectura	El diseño de la aplicación o servicio debe cumplir, después de implementados los requerimientos de seguridad de la arquitectura de la aplicación definidos en la fase inicial, con las siguientes condiciones: 1. Reducción de Superficie de ataque. 2. Criterio del menor privilegio. 3. Fallar de manera segura. 4. Criterio de defensa en profundidad. 5. Diseño seguro de mensajes de error. 6. Diseño seguro de autenticación. 7. Separación de privilegios. 8. Administración segura información Sensible. 9. Diseño de Auditoría y Logging.
5.2.2 Revisión Código	Después de revisar que el diseño cumpla con los requerimientos de seguridad establecidos en la primera fase se debe verificar que la aplicación o servicio también cumpla con estos requerimientos por lo cual se deben revisar los siguientes parámetros. 1. Controlar tamaño y tipo de datos. 2. “Sanitizar” los valores de entrada y salida. 3. Eliminar o “escapear” caracteres especiales. 4. Transformar los datos de entrada a un “encoding” establecido. 5. Reemplazar sentencias SQL dinámicas por Stored Procedures. 6. Evitar generar código con valores ingresados por el usuario. 7. No mezclar datos con código. 8. Capturar errores de capas inferiores y no mostrarlos al usuario. 9. Se deben utilizar APIs previstas para el acceso a funciones específicas del sistema operativo. No se debe permitir que la aplicación o servicio ejecute comandos directamente en el sistema operativo, menos aún mediante la invocación de una shell. 10. Utilice seguros “locks” para evitar múltiples accesos simultáneos a los recursos o mecanismos de sincronización (por ejemplo: semáforos) para evitar condiciones de borde (race conditions). 11. Se deben proteger las variables y recursos compartidos de accesos concurrentes inadecuados.

	12. Si la aplicación o servicio requiere privilegios especiales, se deberán elevar los privilegios solo cuando sea necesario y devolverlos (bajar privilegios) lo antes posible. Mantener los privilegios especiales únicamente cuando sea estrictamente necesario. 13. No se debe utilizar datos provistos por el usuario para ninguna función dinámica. 14. Se debe evitar que los usuarios introduzcan o modifiquen código de la aplicación. 15. Se debe revisar todas las aplicaciones secundarias, código provisto por terceros y bibliotecas para determinar la necesidad del negocio para su utilización y validar el funcionamiento seguro, ya que estos pueden introducir nuevas vulnerabilidades. 16. Se debe implementar mecanismos seguros para las actualizaciones. Si la aplicación o servicio realiza actualizaciones automáticas, utilizar firmas criptográficas para el código y asegurarse que el cliente que descarga la aplicación verifique dichas firmas. 17. Utilizar canales encriptados para las transferencias de código desde el servidor de actualización.
5.2.3 Pruebas de Seguridad	Después de realizar la verificación tanto del diseño como del código de la aplicación o servicio se deben ejecutar pruebas de seguridad para constatar que la aplicación saldrá a producción sin vulnerabilidades que puedan afectar o comprometer los datos. Para las pruebas de seguridad se debe tener en cuenta los siguientes parámetros que se deben probar: 1. Requerimientos de autenticación. 2. Requerimientos de complejidad de contraseñas. 3. Bloqueo automático de cuenta. 4. Restricciones de acceso según diseño. 5. Mecanismos de registro y logging. 6. Mensajes de error especificados. 7. Susceptibilidad a inyección de código SQL o Scripting. 8. Tecnologías en la construcción de la aplicación o servicio Ejemplo: versiones de librerías de Java. **Nota:** Aunque estos parámetros son los básicos recomendados, las pruebas de seguridad se deben definir de acuerdo con los resultados de la Evaluación de los riesgos realizada.

5.3 IMPLEMENTAR

Etapas	ACTIVIDADES
5.3.1 Línea Base de Seguridad	Implementa y deje evidencia de las lineas base de seguridad sobre los sistemas de información bajo las siguientes capas: • Capa de aplicación.

	• Capa de comunicación. • Capa de Sistema Operativo. • Capa de Base de Datos. • Soporte al portal o sitio web.
5.3.2 Gestionar las vulnerabilidades	Como resultado de las pruebas y revisiones hechas de la fase anterior (5.2.3 pruebas de seguridad) es probable que se identifiquen brechas de seguridad (vulnerabilidades) las cuales deben ser remediadas o mitigadas y tener en cuenta la posibilidad de implementar controles compensatorios de acuerdo a la complejidad de las mismas. Es de obligatorio cumplimiento que previo a la puesta en producción, se realice la remediación o mitigación de todas las vulnerabilidades clasificadas de impacto alto y medio, en los casos en que no aplique dicho aseguramiento o no sea posible su implementación deberá quedar documentado e incluir el análisis realizado para la toma de la decisión. El incumplimiento de esta premisa puede traer como consecuencia la materialización de riesgos de seguridad de la información con graves consecuencias para la Compañía.
5.3.3 Habilidad Operativa	Después de que la aplicación o servicio se encuentre en producción con los riesgos de seguridad controlados, se debe contar con que los administradores de TI tanto de la aplicación o servicio como del ambiente de implementación tengan el conocimiento para realizar instalaciones de nuevas versiones de la aplicación o parches de seguridad tanto en los componentes de la aplicación o servicio como en el ambiente de implementación.

5.4 MANTENER Y MONITOREAR

Etapas	ACTIVIDADES
5.4.1 Fortalecer el ambiente	En las etapas y fases anteriores se realizó el aseguramiento de la aplicación o servicios en el ambiente utilizado para el desarrollo, pero el ambiente de producción en donde se implementará también debe estar seguro ya que se puede deshacer el aseguramiento realizado en etapas anteriores. Las aplicaciones interactúan con los siguientes ambientes: • Base de datos • Sistema operativo • Motor Web • Configuraciones de RED Estos ambientes deben ser fortalecidos con la implementación de líneas base de seguridad. A continuación, se presentan las líneas base, las cuales deben ser consultadas en el FO-PET-003Inventario Líneas Base Previsora, Cada administrador de TI o líder de TI en el proyecto deberá buscar la línea base que aplique a la tecnología requerida y será responsable por su completa implementación, en los casos en que no aplique dicha medida de protección o no sea posible su implementación deberá quedar documentado e incluir el análisis realizado para la toma de la decisión. El incumplimiento de esta premisa puede traer como

	consecuencia la materialización de riesgos de seguridad de la información con graves consecuencias para la Compañía.
5.4.2 Verificar líneas Base	La Gerencia de Riesgos, bajo Seguridad de la Información periódicamente realiza monitoreo de la ejecución del aseguramiento en plataformas tecnológicas, aleatoriamente sobre lo reportado.

6 DOCUMENTOS RELACIONADOS

CÓDIGO	NOMBRE DE DOCUMENTO
CIR-375	POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
FO-STI-002	LISTA DE VERIFICACIÓN LINEAMIENTOS DE SEGURIDAD
FO-PET-003	INVENTARIO LÍNEAS BASE PREVISORA

	ELABORÓ	REVISÓ	APROBÓ
NOMBRE (S)	Lorena Pedroza	Cindy Marcela Aguilera	Edilberto Pineda
CARGO (S)	Especialista de Infraestructura y Servicios de TI	Subgerente de Infraestructura y Servicios de TI	Gerente de Tecnología de la Información

CONTROL DE CAMBIOS	
VERSIÓN	**CAMBIO REALIZADO**
1	Versión cargada en 26/jun./2019 Actualización de documento
2	Actualización de documento alineado a buenas practicas Solicitud de Documento No 825