Revisado / Vo.Bo.:

Gerente Sr. Desarrollo de Soluciones
Gerente de Arquitectura de Hardware
Gerente Sr. Seguridad informática

ÍNDICE

I. OBJETIVO, ALCANCE 2
II. DEFINICIONES 3
III. POLÍTICAS 4
III.1 Políticas Generales 4
III.2 Políticas Específicas 4
IV. ALCANCE DE SOLUCÍON 5
IV.1 Diagrama general de operación 6
V. IMPLEMENTACIÓN 7
V.1 Definición y Alcance 7
V.2 Revisión de Artefactos 7
V.3 Revisión de Código 9
V.4 Pruebas de seguridad 10
VI. VERIFICACIÓN 12
VI.1 Definición y Alcance 12
VI.2 Evaluación de Amenaza 12
VI.3 Administración de Vulnerabilidades 13
VI.4 Fortalecimiento del Ambiente 14
VII. GOBIERNO 15
VII.1 Actualización de Reglas 15
VII.2 Exclusión de Reglas 16
VII.3 Mitigación de Vulnerabilidades 17
VII.4 ABC de Usuarios 18
VII. ANEXO: SEGURIDAD DE LA INFORMACIÓN 20

I. OBJETIVO, ALCANCE

Objetivo

Este documento tiene como objetivo proporcionar al área de **Desarrollo de Soluciones** una guía detallada sobre cómo utilizar la herramienta "Fortify" de manera adecuada, así como también el mostrar cómo se encuentra constituida la misma, esto tomando como punto de referencia la integración de SSDLC (Secure Software Development Life Cycle) el cual prioriza la seguridad en el desarrollo de software desde la planificación y el diseño, identificando de manera temprana las brechas de seguridad a nivel código en Procesar.

Alcance

El presente documento es exclusivo para la operación de la herramienta Fortify , la cual es utilizada durante la etapa de desarrollo del SSDLC (Secure Software Development Life Cycle) con el objetivo de analizar y examinar el código fuente de manera estática sin ejecutarlo, en busca de patrones y vulnerabilidades conocidas que pudiesen ser explotadas por algún atacante en su etapa productiva, esto apegado y acotado al tipo de lenguajes que utiliza Procesar, particularmente el área de **Desarrollo de Soluciones**.

Dicho lo anterior, este documento esta dirigido a las siguientes áreas/gerencias:

Audiencia	*Propósito*
Equipo de Desarrollo de Soluciones	Conocer el proceso y los lineamientos que deben de implementarse en el SSDLC, para realizar el diseño seguro de las aplicaciones, con apoyo de la solución Fortify.
Gerente Sr. De Desarrollo de Soluciones	Conocer el proceso y los lineamientos que se deben seguir para el diseño e implementación del SSDLC, con el apoyo de la solución Fortify.
Gerente de Desarrollo de Soluciones Digitales y Moviles	Conocer los procesos de operación de la solución Fortify a través de los cuales se podrá evaluar su nivel de seguridad a nivel de código estático SSDLC, con apoyo de la solución Fortify.

Cualquier informacion adicional que se requiera en relacion al funcionamiento u operación de alguna otra herramienta apegada al análisis de código, será proporcionada por el área de **Desarrollo de Soluciones**.

II. DEFINICIONES

SSDLC	Ciclo de Vida del Desarrollo de Software Seguro (SSDLC en sus siglas en Ingles), es una secuencia estructurada y bien definida, de las etapas en Ingeniería de software, para desarrollar un producto deseado.
SCA	Analizador de código estático (SCA en sus siglas en Ingles), es quien interpreta el código y aplica las reglas correspondientes que se definan en la solución Fortify.
SCS	Centro de seguridad de software (SCS en sus siglas en Ingles), es quien muestra el resultado del escaneo de código, esto tras efectuar y aplicar las reglas previamente definidas en el SCA.
Base de Datos	Se define una base de datos como una serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular.
SonarQube	SonarQube (conocido anteriormente como Sonar), es una plataforma para evaluar código fuente. Es software libre y usa diversas herramientas de análisis estático de código fuente, para obtener métricas que pueden ayudar a mejorar la calidad del código de un programa.
HTTPS	Protocolo de Transferencia de Hipertexto Seguro (por sus siglas en inglés HTTPS), es un protocolo de la capa de aplicación para la transmisión de datos que y el cual se utiliza para acceder a un servidor web seguro.
Firewall	Un firewall o cortafuegos es un dispositivo de seguridad de la red que monitorea el tráfico de red -entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.
WAF	Firewall de Aplicaciones Web (WAF en sus siglas en Ingles), es un tipo de firewall que supervisa, filtra o bloquea el tráfico HTTP hacia y desde una aplicación web.
OWASP	Proyecto abierto de seguridad de aplicaciones web (OWASP en sus siglas en Ingles), es un estándar y marco de referencia internacional, dedicado a determinar y combatir las causas que hacen que el software sea inseguro.
Vulnerabilidad	En informática, una vulnerabilidad es una debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad.
Cross Site Scripting	Secuencia de comandos en sitios cruzados (XSS en sus siglas en Ingles), es una vulnerabilidad de seguridad que permite a un atacante inyectar en un sitio web código malicioso del lado del cliente.
SQL	Lenguaje de consulta estructurado (SQL en sus siglas en Ingles), es un lenguaje de dominio específico, diseñado para administrar, y recuperar información de sistemas de gestión de bases de datos.
SQL Injection	Inyección de lenguaje de consulta estructurado, es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.
Software (Aplicación)	Sistema informático, que comprende un conjunto de componentes lógicos necesarios, los cuales hacen posible la realización de tareas específicas. Permite a los usuarios llevar a cabo una o varias tareas específicas.

III. POLÍTICAS

III.1 Políticas Generales

1. Las políticas que se describen en este documento no contravienen las políticas generales de ***Procesar*** ni las políticas particulares de cada Dirección de Área.

III.2 Políticas Específicas

1. Los especialistas y líderes de la Gerencia de Desarrollo de Soluciones podrán iniciar y verificar el desarrollo de todas las aplicaciones seguras sin excepción, una vez que ingresen al equipo Fortify SSC y seguir los pasos descritos en este documento.
2. Los líderes de la Gerencia de Desarrollo de Soluciones serán los responsables de mitigar y justificar las vulnerabilidades y errores que arrojen los resultados del escaneo de código de cada aplicación, esto de acuerdo con lo descrito en este documento.
3. Los especialistas y líderes de la Gerencia de Desarrollo de Soluciones deberán acatar los lineamientos descritos en este documento con la finalidad de mantener un estándar de seguridad en el desarrollo de aplicaciones con una alta calidad.
4. Las Gerencias de Desarrollo, son las únicas autorizadas para modificar, eliminar o agregar lineamientos de este documento.
5. El área de la Oficialía de Seguridad de la Información se encargara de realizar la validación de las justificaciones y excepciones que se proporcionen por parte de la Gerencia de Desarrollo de Soluciones, con la finalidad de verificar el detalle de la vulnerabilidad y otorgar el visto bueno ya sea de la justificación (exclusión) o mitigación de la vulnerabilidad, siempre y cuando cumpla con los estándares del SSDLC, incluidos dentro de la propia herramienta la cual esta alineada a estándares y marcos de referencia internacionales, en materia de desarrollo de software seguro, como lo es OWASP, mismo que es aplicado por la Oficialía de Seguridad de la Información, revisando que dichas justificaciones (exclusiones) y mitigaciones, no pongan en riesgo a la operación de ***Procesar***.
6. El área de la Oficialía de Seguridad de la Información deberá realizar revisiones dentro de la herramienta (Fortify SCS) quincenalmente, en una sesión en conjunto con el equipo de Desarrollo de Soluciones. Tanto el área de área de la Oficialía de Seguridad de la Información como el de la Gerencia de Desarrollo de Soluciones, deberá realizar el seguimiento de las vulnerabilidades, a través del Fortify SCS, donde en ella se podrán emitir comentarios y justificaciones.

IV.ALCANCE DE SOLUCÍON

La Solución Tecnológica basada en Fortify - Static Code Analyzer (SCA) y en Fortify - Software Security Center (SSC), deberá ser capaz de:

1. Identificar la causa raíz de las vulnerabilidades de seguridad del código fuente.
2. Priorizar los problemas más graves.
3. Proporcionar orientación detallada para que los desarrolladores puedan resolverlos en menos tiempo, con la información y administración centralizada de seguridad de software.

Figura 1. Fases SSDLC

IV.1 Topología General de Solución

A continuación, se muestran las conexiones de comunicación y proceso general operacional en relacion a los componentes de la solución Fortify:

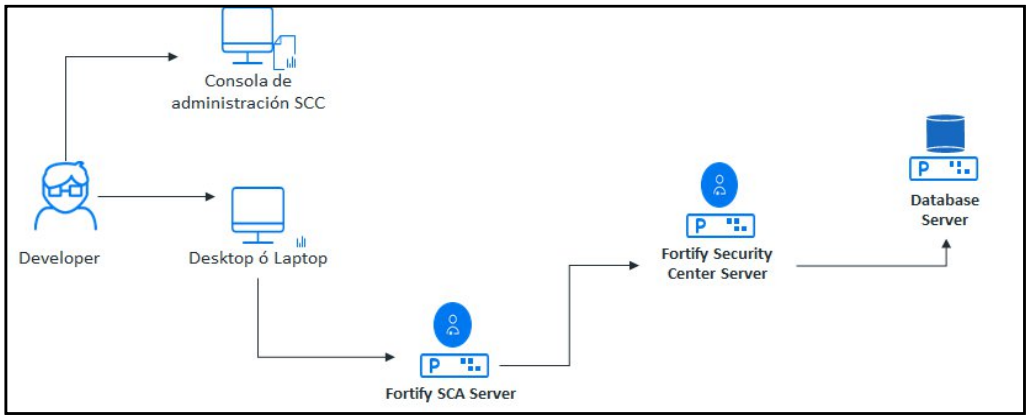

Figura 2. Esquema general de comunicación (Fortify)

Aquí se muestra la comunicación entre componentes, donde principalmente se observa la interacción del desarrollador con la infraestructura, donde el desarrollador desde su equipo tiene la posibilidad de cargar su código al sistema Fortify SCA, quien interpreta el código y aplica las reglas correspondientes que se definieron y que están en la sección (**Reglas *Procesar***), basado en documento (“Línea Base Reglas en Fortify (SSDLC)”).

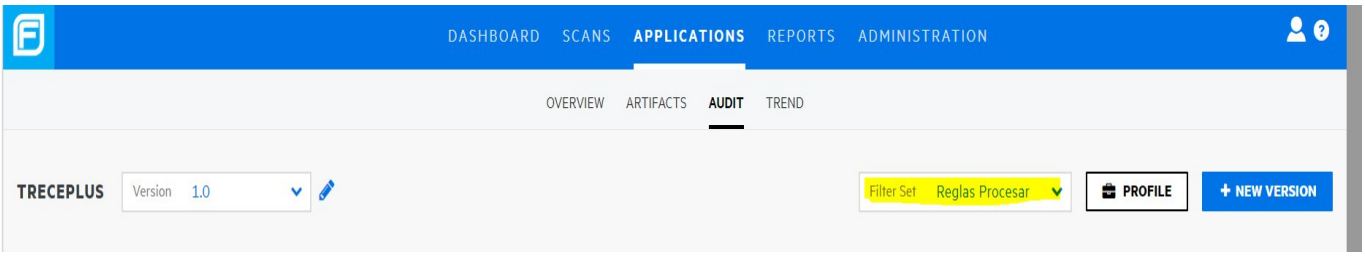

Figura 3. Filtro (Reglas Procesar)

Una vez que el Fortify SCA realiza dicha interpretación, el Fortify SCS, muestra el resultado del escaneo, esto tras efectuar y aplicar las reglas del filtro seleccionado (**Reglas *Procesar*),** el cual tiene su propio manejador de Base de Datos, donde almacena los resultados de los escaneos realizados.

Finalmente, todos estos resultados de los escaneos podrán ser visualizados y administrados, a través de la Consola de Administración SCC, misma donde se les dará seguimiento a las posibles vulnerabilidades detectadas en las aplicaciones.

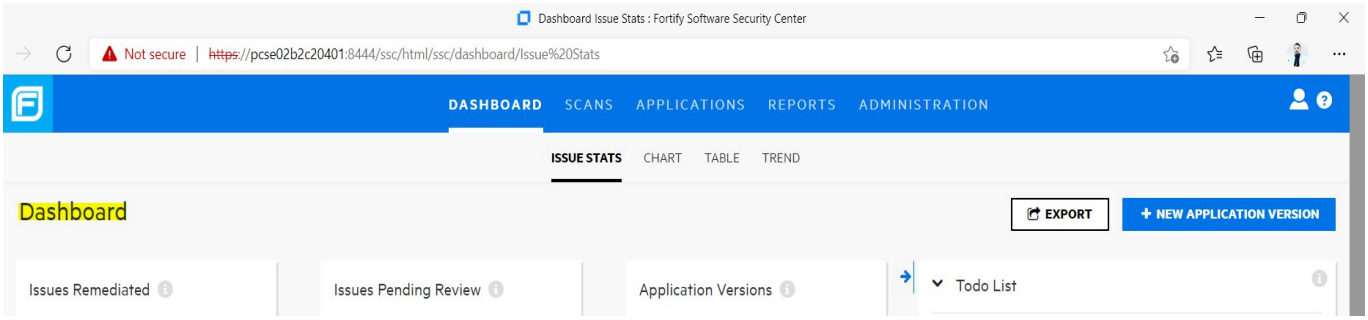

Figura 4. Dashboard general (ISSUE)

V. IMPLEMENTACIÓN

V.1 Definición y Alcance

Esta etapa está bajo el cargo del Área de Desarrollo de Soluciones, donde principalmente se realiza el seguimiento y análisis de los resultados de los escaneos a las aplicaciones y con base en ello, se implementen ajustes, políticas y controles de seguridad con la finalidad de mitigar los posibles errores y vulnerabilidades críticas que se lleguen a detectar en la herramienta.

A continuación, se detallan los tres procesos que conforman esta Etapa:

V.2 Revisión de Artefactos

Es donde se da la inspección de artefactos creados a partir del proceso de diseño (Diseño/arquitectura de software), para asegurar la provisión de mecanismos de seguridad adecuados y apegados a las expectativas de seguridad de ***Procesar***.

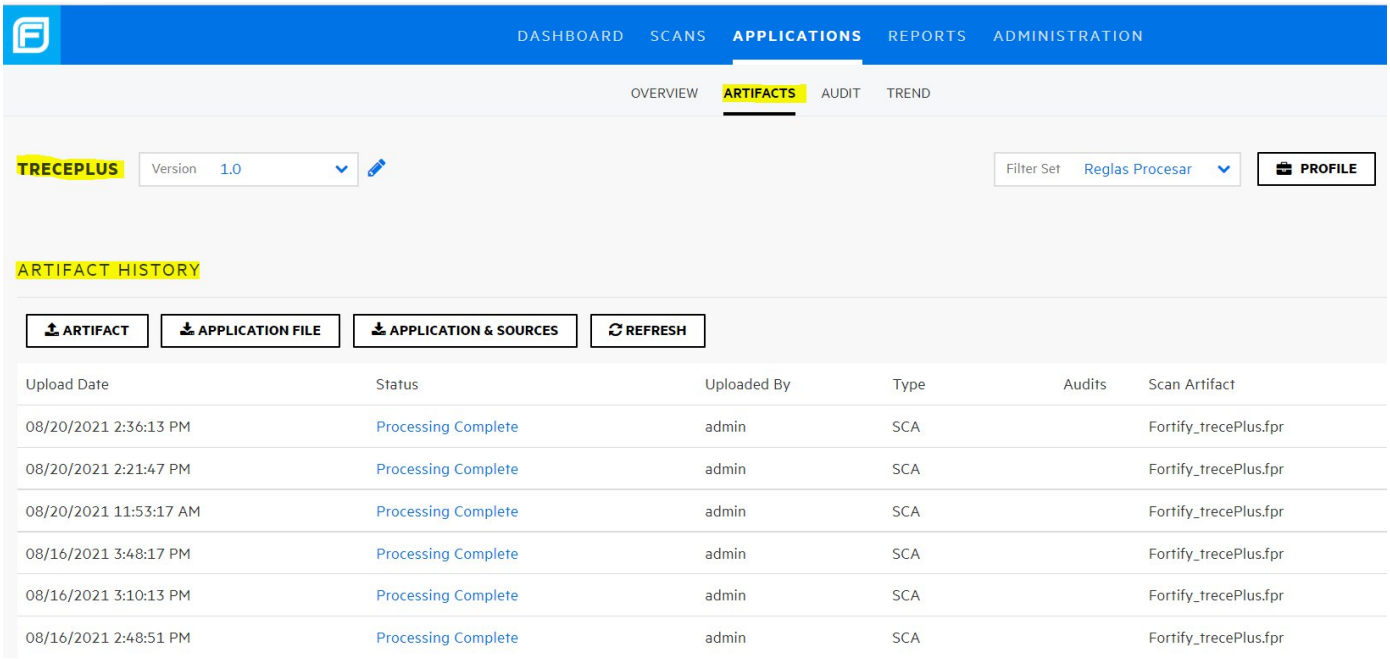

Figura 5. Histórico de Artefactos

En esta sección de la herramienta Fortify, en la opción Artifacts, se observa el detalle de los artefactos (archivos) que se obtuvieron del escaneo.

Adicional muestra el detalle de cada artefacto, indicando el día, hora y fecha en el que se realizó, así como el total de líneas de código escaneado.

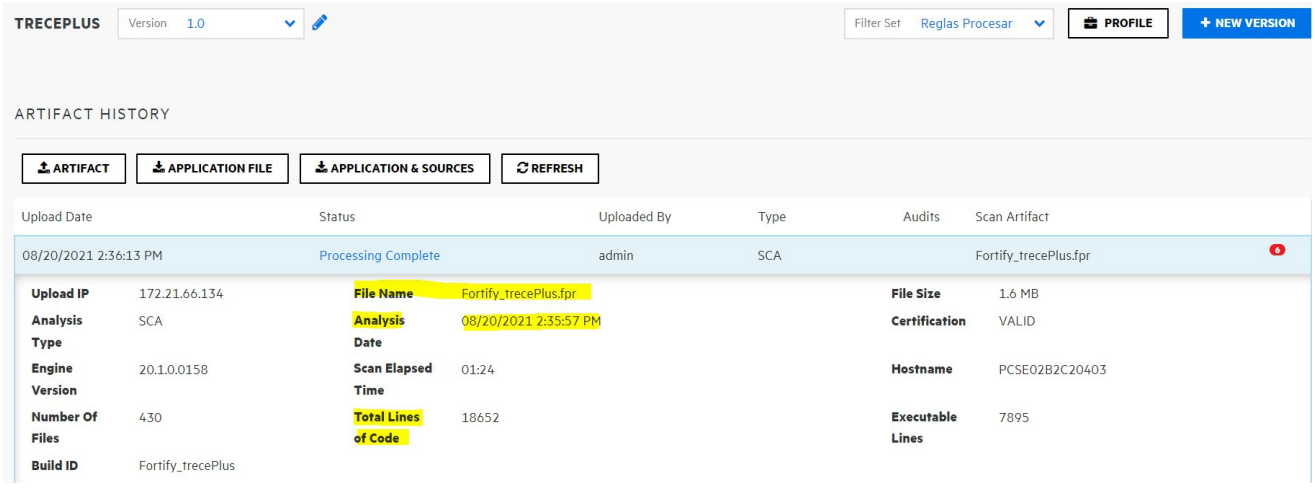

Figura 6. Detalle de Artefactos

V.3 Revisión de Código

Involucra la evaluación del código fuente de las aplicaciones en ***Procesar*** para, ayudar en el descubrimiento de vulnerabilidades y actividades relacionadas a la mitigación, como es el establecimiento de bases para las expectativas de la seguridad en programación.

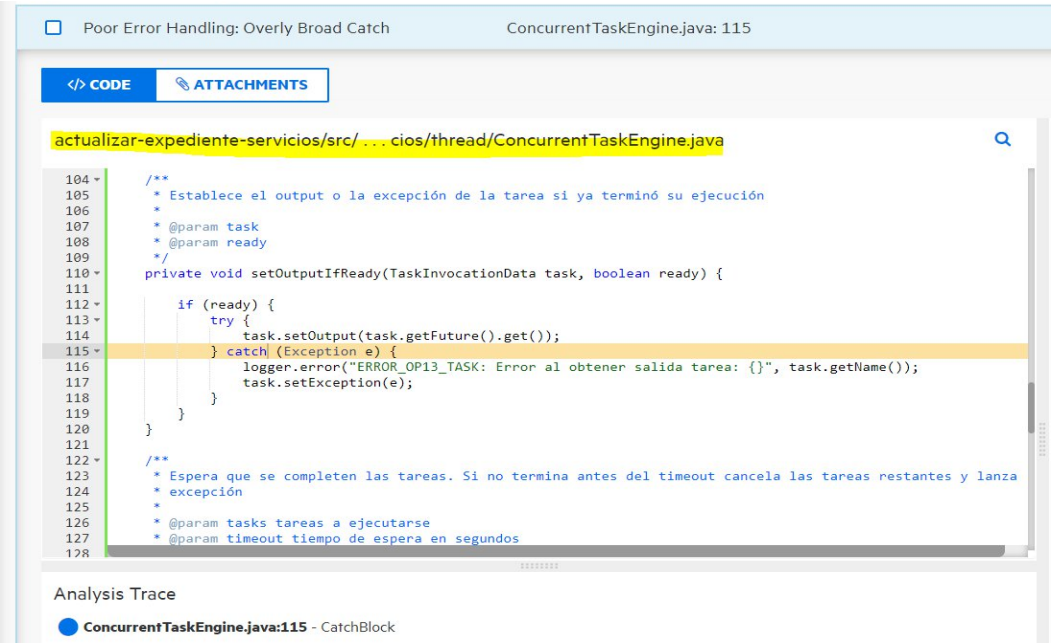

Figura 7. Detalle de Código

Como se observa en la imagen anterior, dentro de la herramienta, se le puede dar seguimiento al código de cada una de las aplicaciones escaneadas y te permite ver el detalle de los errores arrojados, e incluso te de la recomendación para remediar el error o vulnerabilidad detectada.

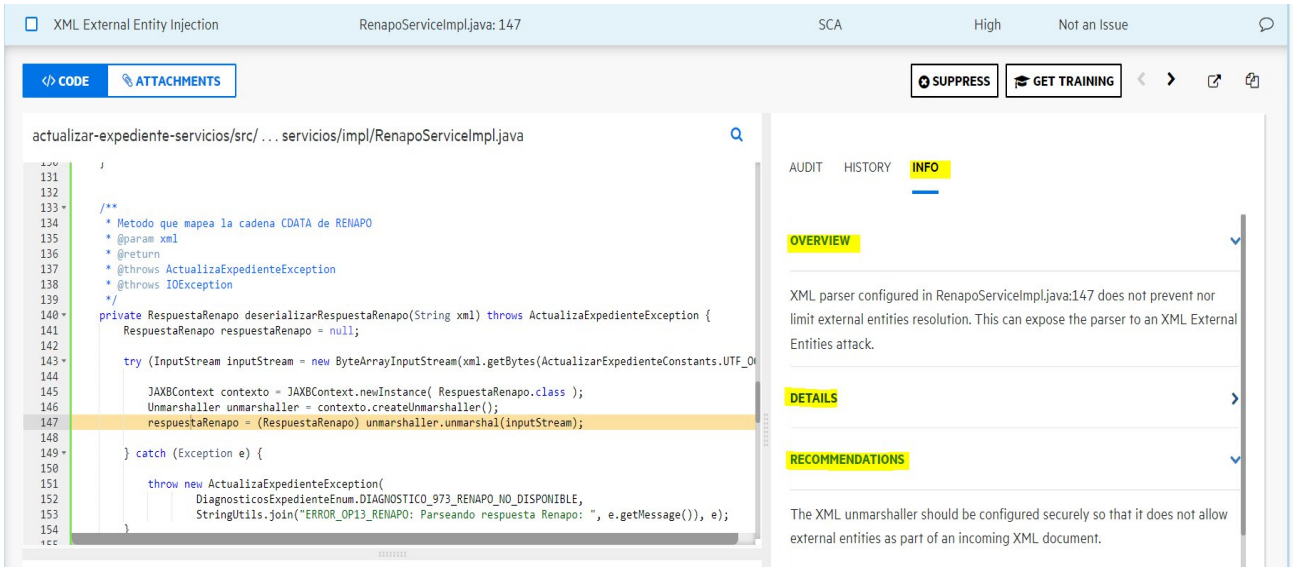

Figura 8. Información del Código

V.4 Pruebas de seguridad

Verificar el software de ***Procesar***, en su ambiente de pruebas para identificar vulnerabilidades y establecer un estándar mínimo para la liberación del software.

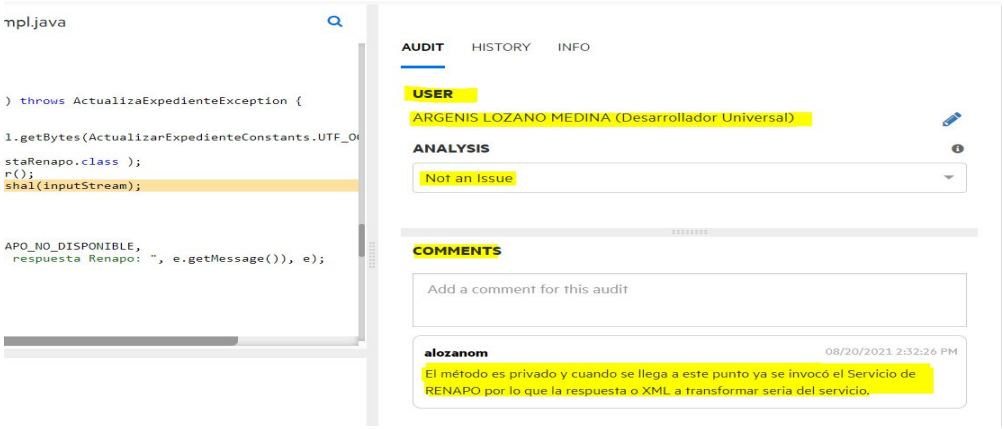

Figura 9. Justificación de Vulnerabilidades (Comentarios y Análisis)

En la imagen anterior, se puede observar cómo se da el seguimiento puntual de las vulnerabilidades y errores registrados en la herramienta Fortify (SCS), esto en la sección de Audit, ya que en cada vulnerabilidad el desarrollador, de acuerdo a su análisis y conocimiento de la operación selecciona la categoría del análisis que va de acuerdo a lo revisado, así mismo

el coloca la justificación o detalle del error o vulnerabilidad, esto según sea el caso, es decir indicara si es necesario mitigarla o si corresponde a una justificación. Es importante mencionar que la justificación (exclusión) y evidencias de alguna mitigación de las vulnerabilidades, también se puede realizar por correo electrónico, notificando a la **Oficialía de Seguridad de la información,** con la finalidad de darle seguimiento a dichas vulnerabilidades, donde principalmente el equipo verificara el detalle de la vulnerabilidad y otorgara el visto bueno ya sea de la justificación (exclusión) o mitigación de la vulnerabilidad, siempre y cuando se verifique que sea válida y cumpla con la Metodología de Análisis de Riesgos que es aplicada por la **Oficialía de Seguridad de la Información**, verificando que dichas justificaciones (exclusiones) y mitigaciones no pongan en riesgo a la operación de ***Procesar***.

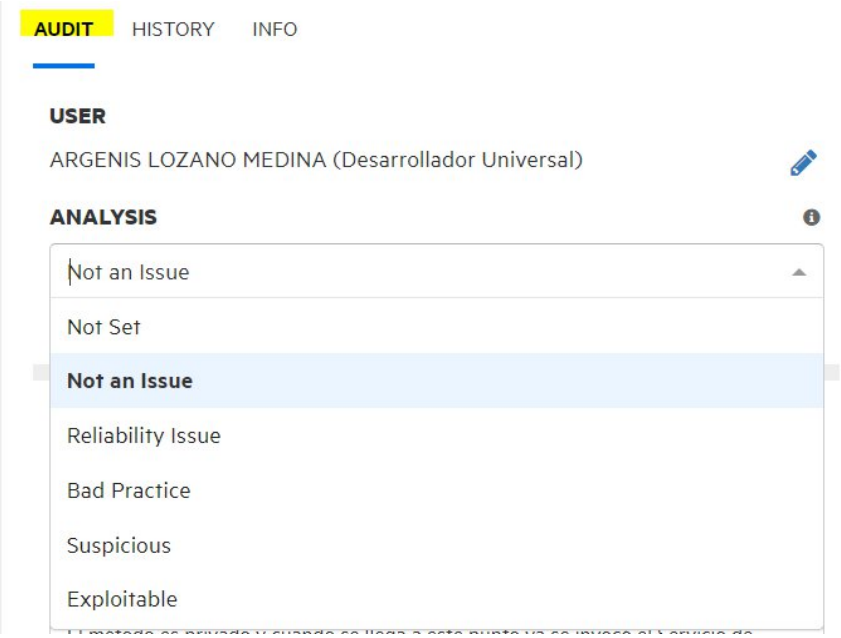

Figura 10. Selección de Análisis

VI. VERIFICACIÓN

VI.1 Definición y Alcance

Esta etapa está bajo el cargo del Área de la Oficialía de Seguridad, donde principalmente se realiza la validación y seguimiento en conjunto con el Área de Desarrollo de Soluciones, de las vulnerabilidades y errores registrados en las aplicaciones escaneadas en el Fortify (SCS), principalmente se valida que las justificaciones y comentarios emitidos en la herramienta por parte de equipo de desarrollo, estén conforme a lo registrado en la herramienta y no representen un riesgo a la operación, por lo que quincenalmente, se tiene una sesión con el equipo de desarrollo, donde se revisan las vulnerabilidades detectadas y se valida que se tengan los comentarios y los análisis en cada una de la aplicaciones que cuenten con vulnerabilidades críticas, esto con la finalidad de tener una continuidad en el proceso y se cuenten con aplicaciones seguras y que pueden ser puestas en producción.

A continuación, se detallan los tres procesos que conforman esta Etapa:

VI.2 Evaluación de Amenaza

Involucra identificar los ataques potenciales contra el software que gestiona ***Procesar***, con el fin de comprender mejor los riesgos y facilitar su gestión.

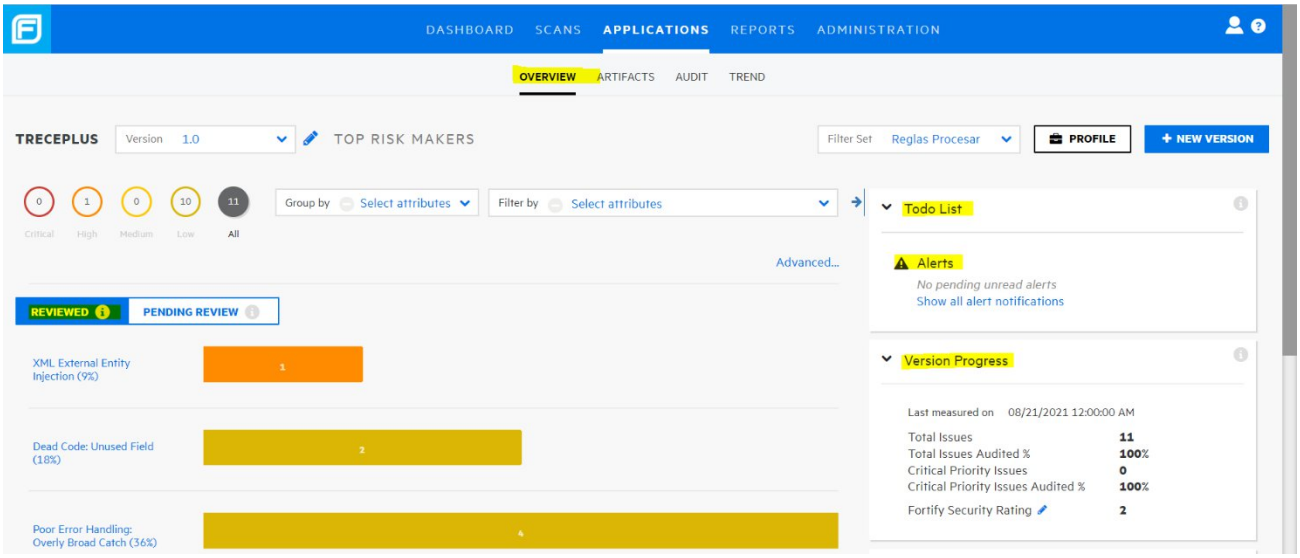

Figura 11. Dashboard de Vulnerabilidades

Dentro de la herramienta, se cuenta con un Dashboard general, el cual permite identificar las diferentes vulnerabilidades detectadas en los escaneos y con ello poder darle seguimiento a cada una de ellas.

VI.3 Administración de Vulnerabilidades

Involucra generar reportes internos de vulnerabilidades para limitar la exposición a datos sensibles, recopilar datos y así mejorar el programa de aseguramiento en ***Procesar***.

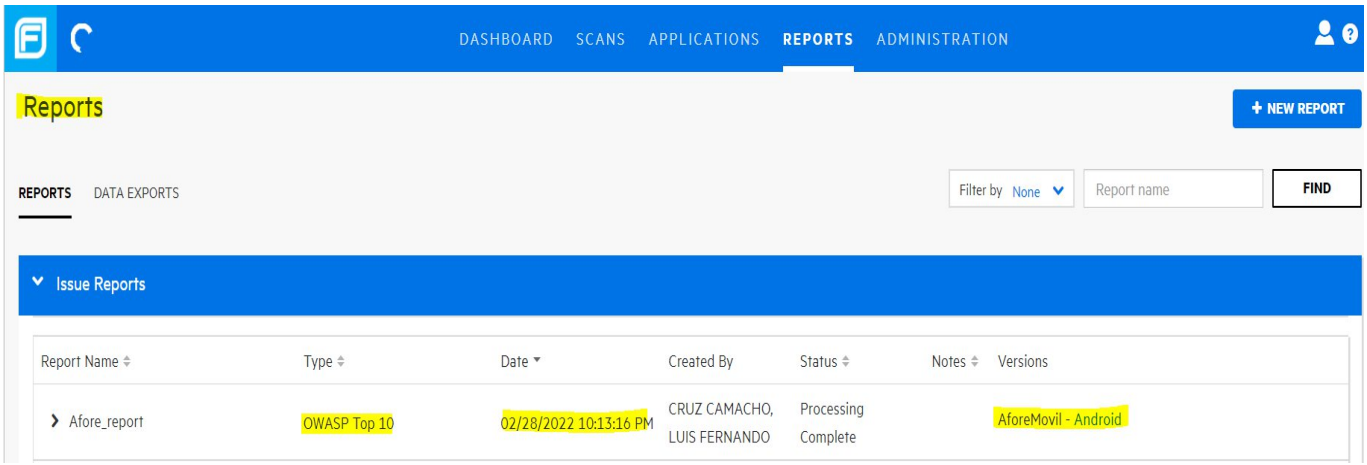

Figura 12. Dashboard de Reportes

Como se observa en la imagen anterior, dentro de la herramienta, es posible generar reportes, los cuales permiten tener el detalle puntual de cada aplicación que fue escaneada, así como de las vulnerabilidades y sus propias recomendaciones, permitiendo contar con un mejor ciclo de mejora continua. Los reportes están en formato PDF.

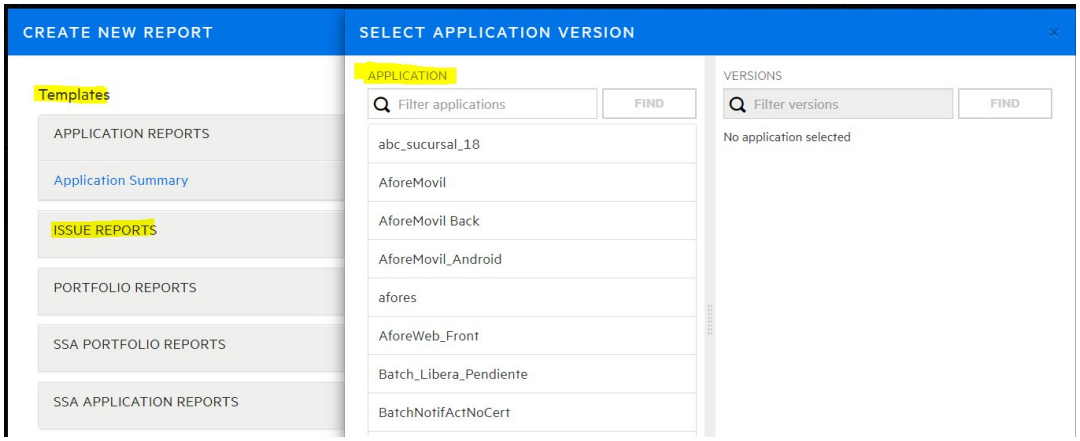

Figura 13. Creación de nuevo Reporte

Finalmente, posterior a todas las revisiones y seguimiento puntual dentro de la herramienta Fortify, así como de las mitigaciones de las vulnerabilidades y justificación de aquellas que lo requieran (sin poner en riesgo la operación), se procede al acuerdo, con el área de desarrollo de soluciones, para la puesta en marcha de una aplicación en ambiente productivo.

VI.4 Fortalecimiento del Ambiente

Implica la implementación de controles para el ambiente operativo que rodea a los programas de ***Procesar***, para reforzar la postura de seguridad de las aplicaciones que han sido implementadas.

Para el tema del fortalecimiento del ambiente y del ciclo del SSDLC, se cuenta con la protección a nivel WAF, donde se configuran controles y políticas de seguridad adicionales, que permiten fortalecer el ambiente, ya que se cuenta con un monitoreo constante de las aplicaciones y se aplican acciones de bloqueos ante ataques conocidos como por ejemplo (Cross Site Scripting y SQL Injection).

A continuación, se muestran los perfiles configurados dentro del WAF:

Politica WAF	Estado	Contexto	Virtual Server	IP
Polic_WAN_237_http	Blocking	/sici	VS_WAN_237_http VS_WAN_237_https	192.168.1.237
Policy_ServiciosInternos_http_199	Blocking	/CertificadoTraspasos	VS_ServiciosInternos_http	192.168.1.199
Policy_TramitesSar_Pulssar	Blocking	/TramitesSar	VS_PSFTPRODM_443	192.168.4.10
Policy_login2_https (SIRI)	Blocking	/siri-web	VS_login2_http	192.168.4.39
		/login		
		/siri-web	VS_login2_https	
		/login		
Folio Registro Traspaso	Blocking	/Traspasos/FolioRegistroTraspaso	VS_wsprocesar_8443	192.168.1.73

Figura 14. Perfiles de Seguridad configurados en WAF-F5

VII. GOBIERNO

VII.1 Actualización de Reglas

1. La **Oficialía de Seguridad de la Información**, será el responsable del análisis y configuración de las nuevas reglas que vaya publicando Fortify (cada seis meses). Dichas reglas son publicadas en el portal de soporte técnico de Micro Focus, accediendo mediante una cuenta activa y registrada en el sitio web de Micro Focus. Las reglas y parches per se, se encuentran en el apartado de “Descargas”.

2. La **Oficialía de Seguridad de la Información**, con base en el criterio de selección definido en la línea base de reglas, se integrarán estas reglas de acuerdo con la infraestructura y lenguajes con los que cuenta ***Procesar***, es importante mencionar que la actualización de estas reglas se verá reflejada en la herramienta Fortify SCS, en el filtro "**Reglas *Procesar***".

3. La **Oficialía de Seguridad de la Información,** en común acuerdo con el **Área de Desarrollo de Soluciones**, mantendrá al tanto de las nuevas reglas configuradas en la herramienta a través de un correo, para que el **Área de Desarrollo de Soluciones,** pueda conocer las nuevas reglas que aplicaran en los escaneos de validación de vulnerabilidades en las aplicaciones.

4. El **Área de Desarrollo de Soluciones**, con base en los escaneos realizados a las aplicaciones realizará la validación de vulnerabilidades (reglas), esto con la finalidad de indicar a través de un correo a la **Oficialía de Seguridad de la Información** las reglas que ellos consideren pueden aplicarse y tomarse en cuenta para futuros escaneos.

5. La **Oficialía de Seguridad de la Información** revisará dicha propuesta y procederá a configurar las nuevas reglas.

6. La **Oficialía de Seguridad de la Información,** en caso de que identifique que no aplique alguna regla que propuso aplicar el **Área de Desarrollo de Soluciones**, deberá notificar con la debida justificación, sobre el mismo correo de la propuesta inicial, para que en común acuerdo con el **Área de Desarrollo de Soluciones** se sepa que, no se procederá a configurar dicha regla en la herramienta.

VII.2 Exclusión de Reglas

1. El **Área de Desarrollo de soluciones**, realizará validaciones de errores en código fuente, con base en lo que detecta la herramienta SonarQube, la cual es administrada por el área de **Arquitectura de Hardware** y con la cual el equipo de **Desarrollo de Soluciones** procederá a corregir o excluir algún elemento en código, esto de ser necesario, únicamente se debe tomar en cuenta que las modificaciones en código se realizarán cuando se contrapongan con el Fortify SCS, una vez realizada la modificación el equipo de desarrollo, tendrá que notificarla por correo electrónico a la **Oficialía de Seguridad de la Información,** esto con la finalidad de tener en común acuerdo que fue lo que se corrigió o excluyó y que no se contraponga con la herramienta Fortify SCS, la cual es validada y administrada por la **Oficialía de Seguridad de la Información.**

2. La **Oficialía de Seguridad de la Información**, será el responsable en conjunto con el **Área de Desarrollo de Soluciones**, de la gestión de exclusiones de reglas que se encuentren configuradas en la consola Fortify SCS (“**Reglas *Procesar***").

3. La **Oficialía de Seguridad de la Información**, será el responsable de realizar las exclusiones de reglas, para los escaneos a las aplicaciones.

4. El **Área de Desarrollo de Soluciones**, con base en los escaneos ejecutados a las aplicaciones, realizará un análisis del resultado de las reglas arrojadas y será el responsable de indicar y justificar las exclusiones que determine, esto a través de un correo dirigido a la **Oficialía de Seguridad de la Información**.

5. La **Oficialía de Seguridad de la Información**, validará la justificación realizada por el **Área de Desarrollo de Soluciones** con el debido sustento y contemplando los activos

de información con los que cuenta la infraestructura de ***Procesar***, procederá a documentar y excluir las reglas indicadas en la consola Fortify SCS ("**Reglas *Procesar***").

6. La **Oficialía de Seguridad de la Información,** en caso de que no concuerde con alguna exclusión de regla que propuso el **Área de Desarrollo de Soluciones**, deberá notificar con la debida justificación, sobre el mismo correo de la propuesta inicial, para que en común acuerdo con el **Área de Desarrollo de Soluciones** se conozca que, no se procederá a excluir dicha regla en la herramienta.

VII.3 Mitigación de Vulnerabilidades

1. La **Oficialía de Seguridad de la Información**, con base en los resultados de los escaneos a las aplicaciones, será el responsable en conjunto con el **Área de Desarrollo de Soluciones**, de la gestión de mitigación de las vulnerabilidades, esto de acuerdo con el reporte de resultados que se muestra en la consola Fortify SCS ("**Reglas *Procesar***").

2. La **Oficialía de Seguridad de la Información**, podrá notificar a el **Área de Desarrollo de Soluciones,** las correcciones y mitigaciones de vulnerabilidades que considere se puedan realizar, esto con base en un análisis realizado a partir de la validación del reporte de resultados del escaneo a las aplicaciones.

3. El **Área de Desarrollo de Soluciones**, con base en los escaneos ejecutados a las aplicaciones, realizará un análisis del resultado de las vulnerabilidades arrojadas y será el responsable de indicar y mitigar las vulnerabilidades que determinen de acuerdo con en el análisis generado (priorizando conforme a la severidad e impacto de la vulnerabilidad), siendo las vulnerabilidades críticas las principales en atender (En un periodo no mayor a tres meses), a esto se le dará seguimiento sobre la herramienta Fortify (SCS) y además se deberá notificar a través de un correo dirigido a la **Oficialía de Seguridad de la Información**. De no ser mitigadas dichas vulnerabilidades, el servicio o aplicación no podrá salir a producción.

4. El **Área de Desarrollo de Soluciones,** podrá indicar o notificar a través de la herramienta Fortify (SCS) o por un correo dirigido a la **Oficialía de Seguridad de la**

Información, su debida justificación y sustento cuales vulnerabilidades no podrán ser mitigadas o atendidas, esto ya sea porque se cuenta con algún control de seguridad compensatorio o porque de acuerdo con la naturaleza de la operación de ProceSAR no aplica su corrección (falso positivo).

5. La **Oficialía de Seguridad de la Información**, validará la justificación realizada por el **Área de Desarrollo de Soluciones** con el debido sustento y contemplando los activos de información con los que cuenta la infraestructura de ***Procesar***, procederá a confirmar y dar el visto bueno para que no se mitiguen las vulnerabilidades indicadas conforme al análisis compartido en la herramienta Fortify (SCS) o vía correo.

6. La **Oficialía de Seguridad de la Información,** en caso de que no concuerde con la justificación que indico el **Área de Desarrollo de Soluciones**, deberá notificar con la debida justificación, comentando en la herramienta Fortify (SCS) o sobre el mismo correo de la propuesta inicial, para que en común acuerdo con el **Área de Desarrollo de Soluciones** se determinen las vulnerabilidades que se deberán mitigar.

VII.4 ABC de Usuarios

1. La **Gerencia Sr. De Seguridad informática** será el responsable en conjunto con la **Gerencia de Seguridad Operativa**, de la gestión de altas, bajas y cambios de permisos de usuarios en la consola Fortify.

2. La **Gerencia Sr. De Seguridad informática** será la responsable de configurar las altas, bajas y cambios de permisos de usuarios en la consola Fortify.

3. El **Área de Desarrollo de Soluciones**, podrá realizar la solicitud de un requerimiento relacionado a ABC de usuarios a través del flujo expuesto en el documento “GR_PP025 P de Admon. de Acceso a Recursos Tecnológicos Restringidos_28_26042022” .

4. La **Oficialía de Seguridad de la Información**, validará que el requerimiento cuente con toda la información necesaria para la baja, alta o cambios de permisos del usuario solicitado, para lo cual se considerará lo siguiente:

    - Nombre completo del solicitante del ABC

- Nombre de cuenta de dominio Procesar que se dará de alta, se eliminara o se modificara.

En caso de que no falte ningún dato, la **Gerencia Sr. De Seguridad informática a petición de la Gerencia de Seguridad Operativa** procederá a realizar en la consola de Fortify la baja, alta o cambio solicitado.

5. La **Oficialía de Seguridad de la Información,** será responsable de la captura de la evidencia correspondiente para la documentación y notificación a el **Área de Desarrollo de Soluciones**, finalmente se procede a realizar la notificación del requerimiento terminado.

VII. ANEXO: SEGURIDAD DE LA INFORMACIÓN

En ***Procesar*** contamos con un sistema de gestión de seguridad de la información basado en la norma internacional ISO27001, de este sistema se desprende un Manual de Seguridad identificado con la clave **GR_MS001**, en donde se describe la metodología y los controles necesarios para su cumplimiento y efectividad.

Se tienen identificados los activos más importantes relativos a la Seguridad de la Información, basados en la Metodología de Análisis de Riesgos, que es aplicada por la Oficialía de Seguridad de la Información, en donde las evidencias y registros derivados de este procedimiento, se deben asegurar en su Confidencialidad, Integridad y Disponibilidad. Los responsables, deben identificar la clasificación de la información de acuerdo con las políticas establecidas, en el **GR_MS001 Manual de Seguridad**.

Es responsabilidad de todos y cada uno de los miembros de ***Procesar***, conocer, entender y aplicar la Política de Seguridad de la Información. De igual forma es su responsabilidad reportar de manera inmediata al área de Seguridad, cualquier incidente real o potencial relacionado con la información de ***Procesar*** y los activos identificados.

Es compromiso de todo el personal de ***Procesar***, conocer las políticas de seguridad, así como el **GR_MS001 Manual de Seguridad**., que es la base general de los lineamientos de la Oficialía de Seguridad de la Información de la empresa.