ANEXO REQUERIMIENTOS TECNICOS

SERVICIO DE ANÁLISIS DE VULNERABILIDADES DE LA INFRAESTRUCTURA TECNOLÓGICA, REDES DE VOZ Y DATOS, PAGINA WEB, INTRANET Y LAS APLICACIONES QUE SOPORTAN LA OPERACIÓN DE LA UCUNDINAMARCA

1. PRESTACION DEL SERVICIO - ETAPAS DEL PROCESO / ENTREGABLES

1.1 METODOLOGÍA

La ejecución del objeto se debe realizar incluyendo todos los aspectos de la guía de pruebas de OWASP versión 4.1 o última vigente y la Metodología de Pruebas de Seguridad de testeo Abierto (OSSTMM); WSTG además se deben realizar pruebas técnicas automáticas y manuales para comprobar las vulnerabilidades detectadas y buscar vulnerabilidades relacionadas en la última versión del top ten de OWASP. En resumen, se debe ejecutar pruebas que generen valor para la entidad en mínimo los siguientes frentes:

- Análisis de Vulnerabilidades.
- Test de Penetración (Interno / Externo).
- Web Application Testing.
- Auditoria de Red.
- Modelado de Amenazas.
- Revisión de código
- Ingeniería social

1.2 ALCANCE DEL SERVICIO A CONTRATAR

- La cantidad total de activos a evaluar durante el contrato, es la siguiente
    - 72 Servidores productivos
    - Servidores de desarrollo y pruebas
    - Dispositivos de red
    - Aplicaciones (internas y/o externas)
    - aplicaciones productivas
- Análisis de desarrollo seguro en producción y antes de salir a producción, corresponde a la identificación de riesgos, vulnerabilidades y oportunidades de mejora sobre los componentes del software de la Entidad por medio de una revisión manual y automática del código fuente de las aplicaciones en producción desde la perspectiva de seguridad informática.
- Aplicaciones en producción a las cuales se les debe realizar análisis de desarrollo seguro:
    - Aplicación 1: aproximadamente 20.000 veinte mil líneas de código.
    - Aplicación 2: Estado de cuenta que se clasifica así: Back 10000 líneas de código y FRONT 30.000 líneas de código.

1.3 Componentes a Ejecutar

1.3.1 Componente 1: Análisis y explotación de vulnerabilidades

Es la actividad de realizar pruebas informáticas internas y externas para identificar las debilidades de los servicios web y de la infraestructura tecnológica, las cuales

pueden llegar a ser explotadas por un atacante y causar afectación operativa, de imagen, de procesos entre otros. Se usan recursos como bases de datos de vulnerabilidades de aplicaciones, exploits que exploten dichas vulnerabilidades, pruebas manuales ejecutadas por un profesional de seguridad y pruebas automáticas ejecutadas con herramientas de software propias y/o comerciales, y/o libres, de escaneo de vulnerabilidades.

Por lo cual deben cumplir las siguientes actividades, pero no limitarse a las descritas a continuación:

- Solicitar la información que requieran para la realización de las pruebas de acuerdo a la planeación definida y tipo de prueba a realizar en los diferentes activos (direcciones de red fijas y públicas, servidores, firewalls, aplicaciones, accesos, detalle de los diferentes dispositivos etc.)
- Realizar escaneos para identificar los servicios que se están ejecutando en dispositivos remotos, equipos activos, sistemas operativos en el equipo remoto, existencia de filtros o firewalls, controles locales y perimetrales, entre otros, para posteriormente con esta información buscar las vulnerabilidades en la infraestructura y en los servicios identificados. Dichas pruebas se deben ejecutar de forma controlada sin causar afectación en la confidencialidad, integridad y disponibilidad de la información de la Entidad. Se debe tener en cuenta como mínimo, las siguientes condiciones en la ejecución del servicio contratado:
    - Evaluar los recursos de red, impresión y voz IP con el objetivo de identificar puertos, servicios y vulnerabilidades asociadas a:
        - ✓ Credenciales débiles o por defecto.
        - ✓ Falta de parches de seguridad.
        - ✓ Configuraciones débiles.
        - ✓ Fallos de seguridad reconocidos en la industria.
        - ✓ Protocolos inseguros o desactualizados.
        - ✓ Top ten del OWASP

- Intentar obtener información como errores de programación, obtención de código fuente u otro tipo de información sensible ya sea interna y/o externa que puede ser utilizada por un atacante para afectar a la Entidad.
- Realizar Pruebas a aplicaciones WEB con métodos manuales y con herramientas licenciadas y libres para descubrir vulnerabilidades enfocadas en los 10 principales riesgos de seguridad de las aplicaciones web de acuerdo al Top Ten del OWASP:
    - A1 La inyección
    - A2 Autenticación rota
    - A3 Exposición de datos sensibles
    - A4 Entidades externas XML (XXE)
    - A5 Control de acceso roto
    - A6 Mala configuración de seguridad
    - A7 Cross-Site Scripting XSS
    - A8 Deserialización insegura
    - A9 Uso de componentes con vulnerabilidades conocidas
    - A10 Insuficiente registro y monitoreo

- Aplicar la guía para pruebas de seguridad (Web Security Testing Guide – WSTG)
- Intentar definir la arquitectura de red tanto para pruebas internas como externas.
- Identificar desde el exterior puntos de conexión a la red.
- Identificación de servidores, de versiona miento y características de dichos servidores.
- Identificar los rangos de las direcciones IP.
- Identificar configuraciones inadecuadas y puertas traseras en los sistemas informáticos.

Se entiende por explotación de vulnerabilidades las acciones que un atacante podría llevar a cabo a fin de aprovecharse de las vulnerabilidades encontradas y lograr obtener datos, privilegios, pivotear a otros sistemas y tomar control del o de los activos entre otras afectaciones de seguridad.

Por lo cual deben cumplir las siguientes actividades, pero no limitarse a las descritas a continuación:

- Realizar la planeación de las pruebas de explotación a las vulnerabilidades halladas tanto a nivel interno como externo, teniendo en cuenta toda la información obtenida previamente (direcciones Ip, aplicativos, usuarios, metadatos, puertos expuestos, ftp, y ftps, malas configuraciones etc.) y su respectiva criticidad e implementar mayor esfuerzo de explotación en las vulnerabilidades críticas y altas, generando los vectores de ataque, tipos de requerimientos para que el UDEC disponga la infraestructura necesaria para la realización de las pruebas de forma controlada, planear fechas a ser realizadas las pruebas y demás información que se considere relevante las cuales deben coordinarse y ser aprobadas previamente por el supervisor del contrato.
- Recolectar las evidencias de las explotaciones satisfactorias, así como de las evidencias de las ejecuciones realizadas y que no lograron explotar las vulnerabilidades, para ser presentadas en los informes ejecutivos y relacionadas en el informe final de ejecución contractual

1.3.2 Componente 2: Retest

Es la actividad de realizar pruebas de verificación a la solución de las vulnerabilidades presentadas en los diferentes entregables solicitados.

Para lo cual deben, pero no limitarse a lo descrito a continuación:

- Realizar una (1) pruebas de RETEST durante la ejecución del contrato a las vulnerabilidades halladas en los activos analizados.

1.3.3 Componente 3: Análisis y fortalecimiento de seguridad informática

Corresponde a la gestión que debe ser realizada por el analista de seguridad informática, la cual consiste en desarrollar, implementar y configurar las mejores prácticas en la plataforma tecnológica de la Universidad de Cundinamarca, para

reducir los riesgos de seguridad. Corresponde a las siguientes actividades, pero no limitarse únicamente a las descritas a continuación:

- Apoyar en la mejora a la configuración y fortalecimiento de las Tecnologías desplegadas en la Universidad de Cundinamarca, en caso de llegar a requerirse.
- Definir políticas de monitoreo y reporte de las herramientas de seguridad.
- Generar la documentación de configuración de las herramientas que se asignen, mantenerla actualizada con la configuración de seguridad que se realice sobre cada una y entregar el informe de las actividades realizadas y la versión actualizada de la documentación de configuración (documento vivo) para cada periodo de facturación.
- Mantener las buenas prácticas de seguridad sobre las herramientas y generar recomendaciones para la mejora de las mismas.
- Proponer recomendaciones de mejora respecto al estado en el que se encuentran las herramientas de seguridad.
- Apoyar la identificación de riesgos de seguridad digital, cuando se requiera.
- Apoyar la investigación y respuesta a incidentes, cuando se requiera.
- Cumplir con los procedimientos establecidos en la Entidad.

1.3.4 Componente 4: Análisis de desarrollo seguro en producción y antes de salir a producción

Corresponde a la identificación de riesgos, vulnerabilidades u oportunidades de mejora sobre los componentes del software de la Entidad por medio de una revisión manual y automática del código fuente de las aplicaciones en producción y antes de salir a producción desde la perspectiva de seguridad informática.

A continuación, se describe información a tener en cuenta para el desarrollo del componente 4:

1.3.4.1 Aplicaciones en producción a las cuales se les debe realizar análisis de desarrollo seguro:

- Aplicación 1: aproximadamente 20.000 veinte mil líneas de líneas de código.
- Aplicación 2: Estado de cuenta que se clasifica así: BACK 10000 líneas de código y FRONT 30.000 líneas de código.

A nivel de la arquitectura verificar como mínimo:

- Escanear los archivos de configuración Web.config con el fin de determinar vulnerabilidades que contengan usuarios y password quemados, que las cookies sólo han de ser accesibles a través, del protocolo HTTP y se controlen mediante la opción httpOnlyCookies del archivo web.config, que se utilice la opción secure en las cookies de sesión como minino.

- Verificar que las aplicaciones cumplan con las pruebas unitarias, se requiere que el proveedor valide con una herramienta para identificar

bucles infinitos, SQL inyección etc., para evitar que se pueda versionar hasta que se soluciones las vulnerabilidades identificadas. Garantizar que previo a la salida a producción de una aplicación se identifique y solucionen las incidencias.

- Verificar que las aplicaciones no permitan la mala práctica de Hardcore.

- Garantizar que las librerías se encuentren en su versión más reciente y estable.

- Garantizar que todos los métodos o clases cumplan con un manejo y control de excepciones (bloques a través de try catch)

- Validar en las interfaces de usuario que no se expongan vulnerabilidades mediante mensajes no controlados o mensajes de error que revelen información de la infraestructura u otros datos que el usuario no debe conocer.

- Cumplir con los protocolos mínimos de seguridad de contraseñas definidos en la guía de contraseñas seguras (Se exija que sean alfanuméricas, de mínimo 8 caracteres, que contenga mayúsculas, minúsculas y caracteres especiales entre otros requerimientos a validar)

- Verificar que las aplicaciones posean solo un pool de aplicaciones asociado (Application Pool), con el fin que se garantice una relación de 1 a 1, ya que esta es una forma de aislar unas aplicaciones web de otras, confinándolas en su propio proceso y en sus propios límites de seguridad; ya que ayudan con la estabilidad general del sistema y la mejora de la seguridad.

- Verificar que solo haya un pool de conexión para una aplicación por base de datos (relación 1 a 1), para evitar que se sature el servidor de datos debido al consumo de recursos del servidor de base de datos.

- Verificar que las aplicaciones tengan configurados logs de auditoria, por ejemplo, Logs de consulta de giro, logs de consulta de saldos, si la aplicación presento caídas etc, con el fin de detectar amenazas, prevenir fugas de información, comportamientos inadecuados, mejorar la gestión y el control de información entre otros.

- Validar que antes de pasar a producción una aplicación el código este ofuscado.

- A nivel de interoperabilidad verificar como mínimo:

    - Verificar que los servicios de interoperabilidad posean el uso de token o credenciales para realizar conexión en API REST Y SOAP y servicios de Windows, estas credenciales deben

cumplir con los patrones mínimos de seguridad en contraseñas.

- Verificar que no existan consultas quemadas dentro de las aplicaciones y que exista un único paquete por aplicación.
- Verificar en base de datos que las contraseñas no queden en texto plano.
- Validar comentarios en el código y que estos sean entendibles, en métodos y clases y a nivel de base de datos en paquetes y procedimientos.
- Identificar malas prácticas de desarrollo a nivel de código.
- Identificar que la declaración de variables, librerías, métodos o clases y demás artefactos estén en uso, para aquellas que estén en desuso recomendar la solución.
- Validar que las transacciones entre aplicación y base de datos se encuentren parametrizadas de acuerdo con las mejores políticas de seguridad para la capa de conexión.
- Validar que la gestión de archivos (carga, descarga de archivos, consulta de archivos) sea segura.
- Validar errores en el buffer de memoria.
- Validar que se encuentren perfiladas las aplicaciones tanto por perfil como por usuario, que se gestionen los usuarios y permisos.
- Validar interfaz de usuario que cumpla con los patrones mínimos requeridos en los diferentes formularios, por ejemplo, si el campo pide números que solo se pueda digitar números y no texto.
- Validar que las aplicaciones tengan certificado de seguridad vigentes.
- Validar asignación de variables
- Validar variables de sesión

1.4 ENTREGABLES

A continuación, se detalla la descripción mínima que deben tener los entregables, pero no limitarse a:

1. Plan de trabajo para la ejecución de las pruebas el cual deben entregar dentro de los cinco (5) primeros días calendario posteriores a la suscripción del contrato y donde se defina como mínimo:

    a) Introducción: El proveedor debe redactar la introducción del servicio contratado.
    b) Objetivos: El proveedor debe documentar los objetivos que se cumplirán con el servicio contratado.
    c) Alcance: El proveedor debe documentar el alcance del servicio contratado.
    d) Metas: EL proveedor debe definir las metas a lograr con el servicio contratado.

e) Monitoreo: El proveedor debe indicar como se realizará el monitoreo y seguimiento a la ejecución de las pruebas y a la remediación e vulnerabilidades
f) Niveles de riesgo: El proveedor debe proponer la escala de valoración (cuantitativa y cualitativa) de los niveles de riesgos que se utilizará para la valoración de la criticidad de cada vulnerabilidad.
g) Listado de actividades: El proveedor debe indicar cada una de las actividades que se desarrollaran durante las diferentes fases de las pruebas De análisis y explotación de vulnerabilidades.
h) Fechas/cronograma: El proveedor debe definir la propuesta de fechas de inicio de ejecución de las pruebas, tiempo de duración de las mismas y fechas de entrega de los informes.
i) Recursos: El proveedor debe especificar los recursos a utilizar durante cada una de las fases de la ejecución de las pruebas, tales como software utilizado, personas, bases de conocimiento, hardware, roles y usuarios necesarios especificando los permisos y el nivel de acceso que requiera sobre las diferentes aplicaciones e infraestructura del UDEC.

1.4.1 Entregables Componente 1: Análisis y explotación de vulnerabilidades

Informe técnico: Documento donde se detallen las pruebas realizadas como técnicas, insumos, software utilizado entre otros, el cual deben entregar culminadas las pruebas para cada bloque según el bimestre planeado y como mínimo debe contener, pero no limitarse a:

a) Los tipos de pruebas realizadas: Se debe indicar el tipo de prueba realizada por activo o grupo de activos (caja negra, caja gris, caja blanca, manual, u otro.)
b) Datos del activo analizado: Indicar la información del activo como nombre, IP, URL, tipo de activo bd, aplicación, dispositivo etc).
c) Vulnerabilidades detectadas: nombrar y describir las vulnerabilidades halladas en los diferentes activos analizados, así como la evidencia de la vulnerabilidad detectada. Estas vulnerabilidades deben relacionar también el código CVE y el código
d) Código CVE Y MITRE: Se debe relacionar el código CVE (Common Vulnerabilities and Exposure) y código MITRE (Common Weakness Enumeration) cuando aplique.
e) Criticidad de la vulnerabilidad: Se debe clasificar las vulnerabilidades de acuerdo al nivel de riesgo definido, por ejemplo: alto, medio, bajo e informativo.
f) Datos resumen: Se debe colocar la estadística de cuantas vulnerabilidades altas, cuantas medias, cuantas bajas, cuantas informativas se hallaron por cada análisis planeado según el plan de trabajo.
g) Confirmación de explotación: Se debe documentar la muestra seleccionada, el tipo de vulnerabilidades halladas, la criticidad y cuales se lograron explotar, además se debe presentar evidencia de la explotación y demás información relevante.

h) Relacionar el identificador de remediación: Se debe generar el plan de remediación para cada bloque de pruebas planeadas, en el informe técnico se puede relacionar el identificador de remediación y en el plan de remediación se puede colocar toda la información necesaria, con el fin de que el UDEC tenga presente dichas recomendaciones y pueda llegar a mitigar los riesgos existentes sobre los activos analizados.
i) Incluir otra información que de acuerdo a su experiencia pueda ser de importancia para el UDEC y deba estar contenida en el informe técnico.

Plan de remediación de vulnerabilidades: Proponer el plan de remediación para que el UDEC gestione la solución de las mismas, sugerir cuales deben ser solucionadas en el corto, mediano o largo plazo, y como mínimo debe contener:

a) Tipo de activo: Se debe relacionar el activo al cual le hallaron la vulnerabilidad.
b) Nombre de las vulnerabilidades: Cual es la vulnerabilidad, o vulnerabilidades existentes en el activo analizado.
c) Controles existentes: Describir los controles que logran identificar posee el activo analizado.
d) Prioridad de remediación: Asignar la recomendación de prioridad de atención a la vulnerabilidad teniendo en cuenta la criticidad de la vulnerabilidad y la criticidad del activo evaluado.
e) Fechas de inicio y fin: Se debe estimar el tiempo de solución para cada vulnerabilidad, la fecha debe partir desde el día que se realice la presentación de resultados a todos los involucrados.
f) Responsable: Se debe documentar quien será el responsable de brindar solución a la vulnerabilidad hallada, esto debe corresponder a un nombre de responsable.
g) Estado: Se debe agregar una columna de estados al plan de remediación para que el proveedor le haga el seguimiento de remediación, se propone sean: EN PROCESO, NO INICIADA, RETRASADA, SE ASUME, FINALIZADA Y RESUELTA.
h) Observaciones de seguimiento: Se debe llevar el control de las observaciones de los responsables de brindar solución con su respectiva fecha de seguimiento por parte del proveedor.
i) Incluir otra información que de acuerdo a su experiencia pueda ser de importancia para el UDEC y deba estar contenida en el plan de remediación.

Informe ejecutivo: Se refiere a un documento que contenga el resumen a nivel general de las vulnerabilidades halladas y explotadas por bloque de pruebas, así como datos estadísticos de relevancia para la toma de decisiones de los directivos, como mínimo debe contener:

a) Datos resumen: Se debe colocar la estadística de cuantas vulnerabilidades altas, cuantas medias, cuantas bajas, cuantas informativas se hallaron por cada análisis planeado según el plan de trabajo.

b) Activos más afectados: De acuerdo a los tipos de activos a evaluar, se debe documentar la estadística de cuáles son los que contienen mayor número de vulnerabilidades halladas y explotadas.
c) Vulnerabilidades más comunes: Documentar cuales fueron las vulnerabilidades más comunes que se detectaron en la plataforma tecnológica del UDEC, tendiendo en cuenta CVE y MITRE ejemplo: Vulnerabilidad permisos, privilegios y control de acceso, Problemas de validación de datos, Control de acceso no adecuado, Inyección de código, Inyección de SQL, Manejador de señales peligrosas no inhabilitado durante operaciones sensibles, etc.
d) Incluir otra información que de acuerdo a su experiencia pueda ser de importancia para el UDEC y deba estar contenida en informe ejecutivo.

Actas de revisión: Las actas que se hayan generado en cada actividad, reunión, bloque de pruebas y demás. Se deben presentar en formato del UDEC.

Informe para la Universidad de Cundinamarca debe contener:

a) Vulnerabilidades detectadas
b) Vulnerabilidades remediadas
c) Total, vulnerabilidades detectadas durante el contrato
d) Vulnerabilidades altas detectadas
e) Vulnerabilidades altas remediadas
f) Total, vulnerabilidades altas durante el contrato
g) Plataforma tecnológica analizada (activos)
h) Total, de elementos de la plataforma tecnológica (cantidad)
i) Cantidad de aplicaciones con análisis de código
j) Total, de aplicaciones analizadas durante el bimestre
k) Cantidad de componentes que deben ser objeto de pruebas de intrusión
l) Cantidad de componentes objeto de pruebas de intrusión

Demás documentos de las pruebas, que de acuerdo con su experiencia puedan ser de importancia para el UDEC.

1.4.2 Entregables Componente 2: Retest

Informe técnico de retest: Documento donde se detallen las pruebas realizadas como técnicas, insumos, software utilizado entre otros, para las pruebas de verificación de remediación a las vulnerabilidades o debilidades halladas en los activos evaluados según el alcance, el cual deben entregar culminadas las pruebas de retest y como mínimo debe contener, pero no limitarse a:

a) Los tipos de pruebas realizadas: Se debe indicar el tipo de prueba realizada por activo o grupo de activos (caja negra, caja gris, caja blanca, manual, u otro.)
b) Datos del activo analizado: Indicar la información del activo como nombre, Ip, URL, tipo de activo bd, aplicación, dispositivo etc).
c) Vulnerabilidades detectadas: nombrar y describir las vulnerabilidades halladas en los diferentes activos analizados, así como la evidencia de

la vulnerabilidad detectada. Estas vulnerabilidades deben relacionar también el código CVE y el código.

d) Código CVE Y MITRE: Se debe relacionar el código CVE (Common Vulnerabilities and Exposure) y código MITRE (Common Weakness Enumeration) cuando aplique.
e) Criticidad de la vulnerabilidad: Se debe clasificar las vulnerabilidades de acuerdo al nivel de riesgo definido, por ejemplo: alto, medio, bajo e informativo.
f) Datos resumen: Se debe colocar la estadística de cuantas vulnerabilidades altas, cuantas medias, cuantas bajas, cuantas informativas se hallaron por cada análisis planeado según el plan de trabajo.
g) Confirmación de explotación: Se debe documentar la muestra seleccionada, el tipo de vulnerabilidades halladas, la criticidad y cuales se lograron explotar, además se debe presentar evidencia de la explotación y demás información relevante.
h) Relacionar el identificador de remediación: Se debe generar el plan de remediación para cada bloque de pruebas planeadas, en el informe técnico se puede relacionar el identificador de remediación y en el plan de remediación se puede colocar toda la información necesaria, con el fin de que el UDEC tenga presente dichas recomendaciones y pueda llegar a mitigar los riesgos existentes sobre los activos analizados.
i) Estado de la vulnerabilidad: Se debe documentar si la vulnerabilidad fue resuelta o aun continua vigente, de acuerdo a los resultados de las pruebas de retest.
j) Incluir otra información que de acuerdo a su experiencia pueda ser de importancia para el UDEC y deba estar contenida en el informe técnico.

1.4.3 Entregables Componente 3: Análisis y fortalecimiento de seguridad informática

Documento vivo de configuración de herramientas: Corresponde a un documento que se debe actualizar constantemente, que refleje los cambios o estado actual de cada herramienta de seguridad asignada y según el alcance definido, el cual o los cuales deben entregar para cada periodo de facturación y como mínimo debe contener, pero no limitarse a:

a) Nombre de cada herramienta
b) Link de acceso
c) Configuración técnica cada herramienta
d) Versión
e) Licencia (vigencia, tipo, toda la información que sea relevante al respecto)
f) Políticas configuradas
g) Usuarios que tienen acceso
h) Propuestas de mejora respecto al estado en el que se encuentran las herramientas.
i) Demás información que se considere relevante deba estar contenida en el informe.

Informe de revisión de la gestión del proveedor de servicios en cuanto a la administración de seguridad de la plataforma dispuesta para el UDEC y como mínimo debe contener, pero no limitarse a:

a) Verificación de controles de seguridad configurados en las diferentes herramientas teniendo en cuenta los controles del anexo A de la norma ISO 27001:2013, el manual de políticas de seguridad digital del UDEC y la documentación misma del proveedor, temas a tener en cuenta:

   - Control de acceso
   - Seguridad de las operaciones
   - Controles automáticos
   - Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio
   - Relaciones con los Proveedores
   - Gestión de Incidentes de Seguridad de la Información

b) Recomendaciones, debe realizar las recomendaciones de mejora de acuerdo al resultado de la verificación.

1.4.4 Entregables Componente 4: Análisis de desarrollo seguro en producción y antes de salir a producción

Informe técnico del análisis y desarrollo seguro en producción y antes de salir a producción: Documento donde se detallen las pruebas realizadas como técnicas, insumos, software utilizado entre otros, el cual deben entregar culminadas las pruebas para cada aplicación en producción o aplicación antes de salir a producción, y de acuerdo a la planeación que se programe, como mínimo debe contener:

a) Los tipos de pruebas realizadas: Se debe indicar el tipo de prueba o técnica realizada por aplicación.
b) Datos de la aplicación analizada: Indicar la información de la aplicación como nombre, Ip, URL, líneas de código, e información técnica relevante de la misma.
c) Vulnerabilidades detectadas: nombrar y describir las vulnerabilidades o debilidades halladas y la evidencia de lo detectado. De ser posible relacionarles el código CVE y el código MITRE
d) Criticidad de la vulnerabilidad o debilidad: Se debe clasificar las vulnerabilidades o debilidades de acuerdo al nivel de riesgo definido, por ejemplo: alto, medio, bajo e informativo.
e) Datos resumen: Se debe colocar la estadística de cuantas vulnerabilidades o debilidades se identificaron como altas, cuantas medias, cuantas bajas, por cada análisis realizado.
f) Relacionar el identificador de remediación: Se debe generar el plan de remediación las vulnerabilidades o debilidades halladas, en el informe técnico se puede relacionar el identificador de remediación y en el plan de remediación se puede colocar toda la información necesaria, con el fin de que el UDEC tenga presente dichas recomendaciones y pueda llegar a mitigar los riesgos existentes sobre las aplicaciones analizadas.

g) Incluir otra información que de acuerdo a su experiencia pueda ser de importancia para el UDEC y deba estar contenida en el informe técnico.

Informe ejecutivo análisis y desarrollo seguro en producción y antes de salir a producción: Se refiere a un documento que contenga el resumen a nivel general de las vulnerabilidades o debilidades halladas, así como datos estadísticos de relevancia para la toma de decisiones de los directivos, como mínimo debe contener, pero no limitarse a:

a) Datos resumen: Se debe colocar la estadística de cuantas vulnerabilidades o debilidades altas, cuantas medias, cuantas bajas según lo planeado y ejecutado.
b) Aplicaciones más afectadas: De acuerdo a las aplicaciones evaluadas y en la medida que se vayan ejecutando los análisis a las diferentes aplicaciones según cronograma, se debe documentar la estadística de cuáles son los que contienen mayor número de vulnerabilidades o debilidades.
c) Vulnerabilidades o debilidades más comunes: Documentar cuales fueron las vulnerabilidades o debilidades o malas prácticas más comunes que se detectaron en el desarrollo de las aplicaciones del UDEC, tendiendo en cuenta CVE y MITRE si es posible.
d) Incluir otra información que de acuerdo a su experiencia pueda ser de importancia para el UDEC y deba estar contenida en informe ejecutivo.

Actas de revisión: Las actas que se hayan generado en cada actividad, reunión, bloque de pruebas y demás. Se deben presentar en formato del UDEC.

Plan de remediación del análisis y desarrollo seguro en producción y antes de salir a producción: Proponer el plan de remediación para que el UDEC gestione la solución de las vulnerabilidades o debilidades, y sugerir cuales deben ser solucionadas en el corto, mediano o largo plazo, y como mínimo debe contener:

a) Nombre de la aplicación: Se debe relacionar en la aplicación a la cual le hallaron la vulnerabilidad o debilidad.
b) Nombre de las vulnerabilidades: Cual es la vulnerabilidad o debilidad existente en la aplicación revisada analizado.
c) Controles existentes: Describir los controles que logran identificar posee lo analizado.
d) Prioridad de remediación: Asignar la recomendación de prioridad de atención a la vulnerabilidad teniendo en cuenta la criticidad de la vulnerabilidad y la criticidad del activo evaluado.
e) Fechas de inicio y fin: Se debe estimar el tiempo de solución para cada vulnerabilidad, la fecha debe partir desde el día que se realice la presentación de resultados a todos los involucrados.
f) Responsable: Se debe documentar quien será el responsable de brindar solución a la vulnerabilidad hallada, esto debe corresponder a un nombre de responsable.
g) Estado: Se debe agregar una columna de estados al plan de remediación para que el proveedor le haga el seguimiento de

remediación, se propone sean: EN PROCESO, NO INICIADA, RETRASADA, SE ASUME, FINALIZADA Y RESUELTA.

h) Observaciones de seguimiento: Se debe llevar el control de las observaciones de los responsables de brindar solución con su respectiva fecha de seguimiento por parte del proveedor.
i) Incluir otra información que de acuerdo a su experiencia pueda ser de importancia para el UDEC y deba estar contenida en el plan de remediación.

Documento de resultados y propuesta de mejora al procedimiento de gestión de requerimientos de desarrollo tecnológico: Se refiere a un documento que contenga el resultado de la revisión del procedimiento y los documentos complementarios del mismo (lista de chequeo de seguridad en las aplicaciones, procedimiento de control de cambios y despliegue, procedimiento de migración de datos, formato plan de pruebas, actas de reuniones) así como las recomendaciones y propuesta de mejora al mismo enfocando fuertemente las recomendaciones en los pasos a seguir, pruebas, herramientas y prácticas regulares a tener en cuenta para el desarrollo seguro de las aplicaciones, que estas apunten a la incorporación y puesta en práctica de actividades recurrentes para fortalecer la seguridad en el desarrollo, como mínimo debe contener, pero no limitarse a:

a) Resultados de la revisión del procedimiento y de los documentos complementarios.
b) Recomendaciones de mejora (puede ser directamente en el procedimiento y documentos complementarios con control de cambios)
c) Tipos de pruebas, etapas de ejecución de las pruebas dependiendo el lenguaje de desarrollo (java, .net etc), buenas prácticas y herramientas aplicadas para la ejecución de componente 4 y que recomienden se deben incorporar en el procedimiento actual para el desarrollo de software y que a futuro deban utilizarse.

Documento de buenas prácticas y recomendaciones a tener en cuenta a futuro en el desarrollo de las aplicaciones en todo su ciclo de vida: Se refiere a un documento que contenga recomendaciones relacionadas con el fortalecimiento de la seguridad en el desarrollo, estandarización de buenas prácticas y demás recomendaciones que faciliten la escalabilidad, el mantenimiento, el testeo y resolución de errores. Es importante recomendar la integración de este documento al procedimiento.

EDILSON MARTINEZ CLAVIJO
Director de Sistemas y Tecnología
Universidad de Cundinamarca