TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE TLALNEPANTLA

INSTITUTO TECNOLÓGICO DE TLALNEPANTLA.

TECNOLOGÍAS DE SEGURIDAD EN SOFTWARE.

DOCENTE: DÍAZ RINCÓN HILDA.

ALUMNO Y N^{o} CONTROL:

ALDAMA MÁRQUEZ JOEL JAIR - 15251870.

GRUPO: T91.

ACTIVIDAD: 3.1 CONTROLES EN APLICACIONES EN PRODUCCIÓN.

INDICE

INTRODUCCIÓN 2

DESARROLLO 3

CONCLUSIONES 128

BIBLIOGRAFÍA 129

CONTROLES EN APLICACIONES EN PRODUCCIÓN

INTRODUCCIÓN

En el presente documento, se llevara a cabo un trabajo de investigación sobre los controles en aplicaciones en producción, gracias a la información de ciertos documentos web en los cuales veremos temas como: Estándar de Verificación de Seguridad en Aplicaciones 3.0.1, Seguridad en aplicaciones, Proceso de Administración de la Operación (AOP), Series De Liderazgo De Seguridad: Estrategias de seguridad para el éxito, DevOps con controles, procedimiento para el desarrollo de aplicaciones informáticas, protocolo – paso a producción para la entrega de producto de nuevas soluciones tecnológicas, entornos existentes en el ciclo de desarrollo de software y despliegue de aplicaciones, la planeación y evaluación de los procesos productivos, la evaluación en el desarrollo de los procesos de producción para mayor eficiencia y control interno informático.

DESARROLLO

Seguridad en aplicaciones

La evolución rápida y constante de las técnicas de hacking es indiscutible: se estima que cada semana se publica al menos un incidente de seguridad que afecta a información sensible.

De 2005 a la fecha se cree que se ha comprometido la seguridad de más de 245 millones de registros conteniendo información sensible1 y según un estudio de Forrester Reseach, el costo para una organización por registro perdido/robado ronda entre $90 y $300 dólares.

De acuerdo al análisis de los resultados de más de 300 proyectos de hacking ético realizados durante los últimos 4 años por el Application Defense Center de Imperva, sólo el 5% de las aplicaciones están libres de vulnerabilidades.

Esto puede tener implicaciones importantes en los ambientes de producción. El costo de solucionar una vulnerabilidad en una aplicación en las fases tempranas de desarrollo es mucho menor que hacerlo ya que está en operación.

Se ha estimado que el costo por vulnerabilidad en la etapa de desarrollo es de aproximadamente $500 dólares, mientras que en la fase de pruebas llega a $7,000 dólares y en la fase de producción alcanza los $14,0005.

Pueden existir vulnerabilidades en las aplicaciones pero que no hayan sido encontradas por los expertos.

Puede haber vulnerabilidades no cubiertas por el alcance de las pruebas ya sea por falta de tiempo o de presupuesto.

Asimismo, pueden existir nuevas vulnerabilidades que se hayan descubierto o publicado después de haber sido realizado el estudio.

Cómo lograr seguridad en las aplicaciones

En nuestra experiencia la seguridad en las aplicaciones se logra a través de un enfoque integral que considere la combinación de una serie de elementos complementarios tales como aspectos tecnológicos, organizacionales y normativos.

Deberá considerarse la interacción entre distintas áreas de la organización entre las que al menos deben estar la de seguridad, de desarrollo, de operaciones y de bases de datos.

Evaluación aplicativa

El primer elemento a considerar es la evaluación continua de todas y cada una de las aplicaciones, considerando primero aquellas que son más críticas. Para ello es necesario iniciar con un inventario actualizado de todas las aplicaciones incluyendo versiones, actualizaciones, parches, configuraciones, etc.

De igual forma se deberá tener visibilidad de todas y cada una de las bases de datos existentes, sobre todo de aquellas que almacenan información sensible de la organización. Así como una clasificación de la información para distinguir claramente lo que es sensible de lo que no lo es.

Sensibilización y formación

Es indispensable sensibilizar a todas las partes interesadas sobre la existencia de los riesgos identificados en la etapa de evaluación aplicativa y transmitir claramente la necesidad de mitigarlos.

También se debe mejorar la formación de los grupos de seguridad y desarrollo. Es decir, los expertos en seguridad deben saber más sobre las aplicaciones y el ciclo de vida de

desarrollo de sistemas y las áreas de desarrollo tiene que saber más de seguridad y considerarla una parte integral del proceso SDLC.

Desarrollo seguro

Uno de los elementos clave para lograr la seguridad aplicativa es el uso de buenas prácticas en el desarrollo para que las aplicaciones sean seguras por diseño, desde las fases iniciales del SDLC hasta las pruebas y puesta en producción.

Arquitectura de seguridad

Finalmente como parte de la arquitectura de seguridad de las aplicaciones, se deberán considerar los controles normativos a implementar así como los controles tecnológicos a implementar; principalmente firewalls aplicativos y de base de datos para tener visibilidad del tráfico aplicativo y poder distinguir lo que es legítimo de lo que no lo es.

Entornos existentes en el ciclo de desarrollo de software y despliegue de aplicaciones

Cuando empezamos a programar una aplicación o una página web, necesitamos dos entornos: desarrollo y producción. La máquina de desarrollo suele ser nuestro propio ordenador en el que programaremos todo nuestro código. Por otra parte, tenemos el entorno de producción, que utilizaremos cuando queramos desplegar nuestra aplicación y hacerla pública.

Entorno de desarrollo

En el entorno de desarrollo se programa el software. Puede haber diferentes opciones: el propio ordenador del programador o incluso un servidor compartido por los desarrolladores para que creen la aplicación.

Entorno de testing

Es en este entorno en el que se ejecutan los tests y se realizan las pruebas de una determinada funcionalidad que hayamos desarrollado.

Entorno UAT: User Acceptance Testing

Las pruebas de aceptación de usuario forman la última fase de un proceso de pruebas. En este entorno, usuarios reales realizan pruebas para asegurarse de que los requisitos de desarrollo de software se han cumplido, es decir, que los desarrolladores han hecho una funcionalidad tal y como se ha pedido y el software es completamente usable.

Entorno de pre-producción o staging

El entorno de pre-producción o staging es, como su propio nombre indica, el último entorno al que vamos a desplegar nuestra aplicación antes de que vaya a producción.

Entorno de producción

Este entorno ya es accesible a todo el mundo. Si hemos configurado todos nuestros entornos de la misma manera, realizado pruebas exhaustivas del software, tests automatizados y seguido buenas prácticas, no deberíamos tener ningún problema en el despliegue.

DevOps con controles

Muchas empresas se desplazan hacia un abordaje de DevOps, donde los despliegues de software y las operaciones en curso de entornos de producción se encuentran incorporados en el ciclo de vida del desarrollo de software. En lugar de lanzar el código completo sobre el muro, desde el desarrollo hasta las operaciones cuando el software esté listo para el release en entornos de producción, DevOps incorpora el release a la producción dentro del proceso de release completo. Al utilizar DevOps, las empresas pueden moverse más rápidamente que nunca.

Visión general rápida de DevOps

DevOps es un abordaje que despliega software rápidamente cuando se ponen a disposición nuevos releases. Una de las metas primarias de DevOps es ayudar a las organizaciones a moverse rápidamente. La mayoría de las organizaciones utiliza una infraestructura de nube como el entorno operativo para sus equipos de DevOps. Ejecutar un conjunto de pruebas de regresión para la verificación del código y pruebas aleatorias para la preparación del entorno de producción.

Confirmar el código.

Ejecutar en producción hasta el próximo release. Todo este proceso, desde el principio al fin, menudo se conoce como una rutina de DevOps o playbook. Pero no todos los equipos de DevOps saben cómo aprovisionar la infraestructura correctamente para mantenerla de acuerdo con los requisitos de seguridad y conformidad de la organización. Los playbooks de DevOps casi siempre incluyen mecanismos de reversión.

La nube para DevOps

La nube se acciona por software y tiene muchas capas. La infraestructura de la nube se factura, por lo general, en un modelo por estilo de utilidad, pague según el uso.

Adopción de la nube

Eventualmente, la adopción seria de la nube se vuelve descentralizada, y muchos equipos acceden a la infraestructura de la nube. Y muchos simplemente no saben o no entienden los requisitos de seguridad de la organización o cómo implementarlos en entornos de nube definidos por software. Cuando se combina con la complejidad de las grandes empresas, unidades comerciales, equipos distribuidos y varios regímenes de conformidad, este problema se vuelve más y más difícil de gestionar a escala.

El abordaje de DevOps para resolver los problemas

Muchos equipos de DevOps automatizan ambos despliegues y retrotracción de nuevas aplicaciones y releases de aplicaciones. Las pruebas, con frecuencia, se enfocan en el comportamiento de la aplicación, correcciones de códigos y, algunas veces, en la evaluación de la seguridad. Los equipos de desarrollo tienden a dominar los grupos de DevOps, sin embargo, pueden carecer de los antecedentes para verificar la optimización o configuración de la infraestructura. Implementar un conjunto de controles de seguridad y configuración puede brindar a los ejecutivos clave la protección y tranquilidad que necesitan para permitir que los equipos de DevOps operen rápidamente, sin poner a la organización en riesgo.

Percepción de seguridad de DevOps

La principal preocupación que las grandes organizaciones tienen acerca de DevOps es la falta de enfoque en la seguridad. Sin embargo, frecuentemente se sacrifica, de modo que los equipos y sus entornos no se limiten.

Seguridad de la nube

Una de las razones por las que la percepción de seguridad de DevOps es tan negativa es que con la infraestructura de la nube, puede ser difícil gestionar el número de controles de seguridad y configuraciones que necesiten programarse. En un diseño de arquitectura de aplicación de la nube sencilla, hay, por lo menos, diez controles exclusivos para implementar y configurar correctamente. Algunos ejemplos:

- ¿Están activados los registros de auditoría para todos los recursos de la infraestructura?
- ¿Están configuradas correctamente las reglas del firewall?
- ¿Se utilizan los certificados de SSL en los puntos correctos?
- ¿Los certificados de SSL son válidos e inmunes a partir de las vulnerabilidades conocidas?
- ¿Las cuentas de servicios son utilizadas correctamente y seguras para el lanzamiento de los servicios?
- ¿Tienen las cuentas de servicios los permisos, políticas y rotación de clave apropiadas?
- ¿Tienen las subredes el tamaño adecuado?

¿Qué controles se necesitan?

Uno de los desafíos importantes para las organizaciones en la adopción de la nube es definir las políticas y estándares que desean implementar para sus entornos de nube. Estos requisitos pueden variar por aplicación y, a menudo, vienen de las diversas partes interesadas.

- Los entornos de producción pueden tener el nivel más alto de restricción de seguridad.
- Los entornos de prueba y desarrollo podrían tener un enfoque en controlar los costos, aunque no se permita ningún acceso de fuera de la organización.
- Las aplicaciones de back office probablemente necesiten conectarse nuevamente a las redes corporativas

Estas herramientas pueden inspeccionar y tomar medidas para los problemas identificados. Las organizaciones utilizan códigos, convenciones de nombres, región de la nube o ubicación de la cuenta para determinar qué conjuntos de controles de configuración se aplican a cada aplicación o carga de trabajo, en adición a las políticas globales que se aplican universalmente.

Proceso de Administración de la Operación (OAP).

AOP1 Establecer: Los mecanismo de operación y mantenimiento de los sistemas, aplicaciones, infraestructura y servicios de TIC.

El responsable de este proceso deberá:

1. Formalizar el mecanismo de operación de TIC para los sistemas, aplicaciones y servicios de TIC, a través del Mecanismo de operación y mantenimiento de TIC.
2. Definir e implementar, herramientas tecnológicas para notificar y rectificar fallas críticas en las tareas de la operación, con la finalidad de prevenir fallas en la operación.

El responsable del mantenimiento de la infraestructura deberá:

3. Integrar en el documento Mecanismo de operación y mantenimiento de TIC las acciones de carácter preventivo para evitar fallas a los componentes.
4. Aplicar los controles de mitigación de riesgos establecidos en el Proceso de Administración de la Seguridad de la Información (ASI), relativos a componentes de infraestructura.
5. Implementar los controles de seguridad del SGSI.
6. Registrar y dar seguimiento a los incidentes de mantenimiento, con el propósito de analizar y eliminar las vulnerabilidades dentro de la infraestructura tecnológica e informarlos.

AOP2 Mantener: Programar y ejecutar las tareas de la operación de los sistemas, aplicaciones y servicios de TIC.

El responsable de este proceso deberá:

1. Mantener un control en la ejecución de tareas para la operación de TIC, así como, los elementos de la configuración que se verán afectados y dar seguimiento.

2. Constatar que el personal a su cargo ejecute las tareas programadas, registre solicitudes derivadas de la ejecución o del trámite de solicitud de servicio con motivo de incidentes de operación, y de seguimiento a cada solicitud de manera administrada.
3. Constatar que las tareas ejecuta- das coinciden con las tareas programadas.

AOP3 Monitorear: Los dispositivos y servicios de TIC

El responsable de este proceso deberá:

1. Revisar que se registre cualquier tarea ejecutada como parte de la operación, así como confirmar la ejecución satisfactoria de las tareas de la operación.
2. Dar seguimiento a los eventos e incidentes que se presenten en la operación y registrar aquellos que aporten experiencia y conocimiento, con el propósito de apoyar el análisis para la solución de problemas o la prevención de incidentes.

AOP4 Mantener y actualizar: Implementar y verificar que se cumplan los controles de seguridad física en el centro de datos.

El responsable del proceso, con apoyo del responsable del Proceso de Administración de la Seguridad de la Información (ASI), deberá:

1. Mantener, actualizar e integrar el sistema de seguridad física en el centro de datos, en el que se incorporen, de acuerdo con el SGSI, los controles de seguridad para:
    a. Los riesgos de seguridad física.
    b. Limitar el acceso a la información sensible del centro de datos.
    c. Efectuar el retiro, transporte y almacenamiento de activos de TIC, de forma segura.

d. El borrado seguro de la información de los dispositivos de almacenamiento fijos, removibles y externos, que sean retirados del ambiente operativo, por daño o reemplazo.
e. El registro de incidentes sobre la seguridad del ambiente físico, mediante la solicitud de servicio respectiva.
f. Los controles de seguridad requeridos para el acceso físico a las áreas reservadas de la UTIC.

2. Difundir al interior de la UTIC los controles de seguridad implementados y verificar su cumplimiento.
3. Registrar los incidentes del ambiente físico que se presenten y administrarlos hasta su solución.

Control Interno Informático

1. Aspectos clave del control interno.

GESTIÓN (eficiencia y efectividad). CONTROL (Riesgo y Control).

Eficiencia = Buen Uso de Recursos.

Efectividad = Nivel en que se alcanza los resultados.

Riesgo = Evento que podría impedir el logro de un objetivo.

Control = Políticas y procedimientos para (enfoques):

(+) Alcanzar lo que SI se quiere.

(-) Evitar lo que NO se quiere.

Alerta: excesivo énfasis en la Gestión (eficiencia y efectividad) descuidando Controles incrementa el riesgo de errores e irregularidades.

Alerta: excesivo énfasis en el Control descuidando la Gestión incrementa el riesgo de ineficiencia e inefectividad.

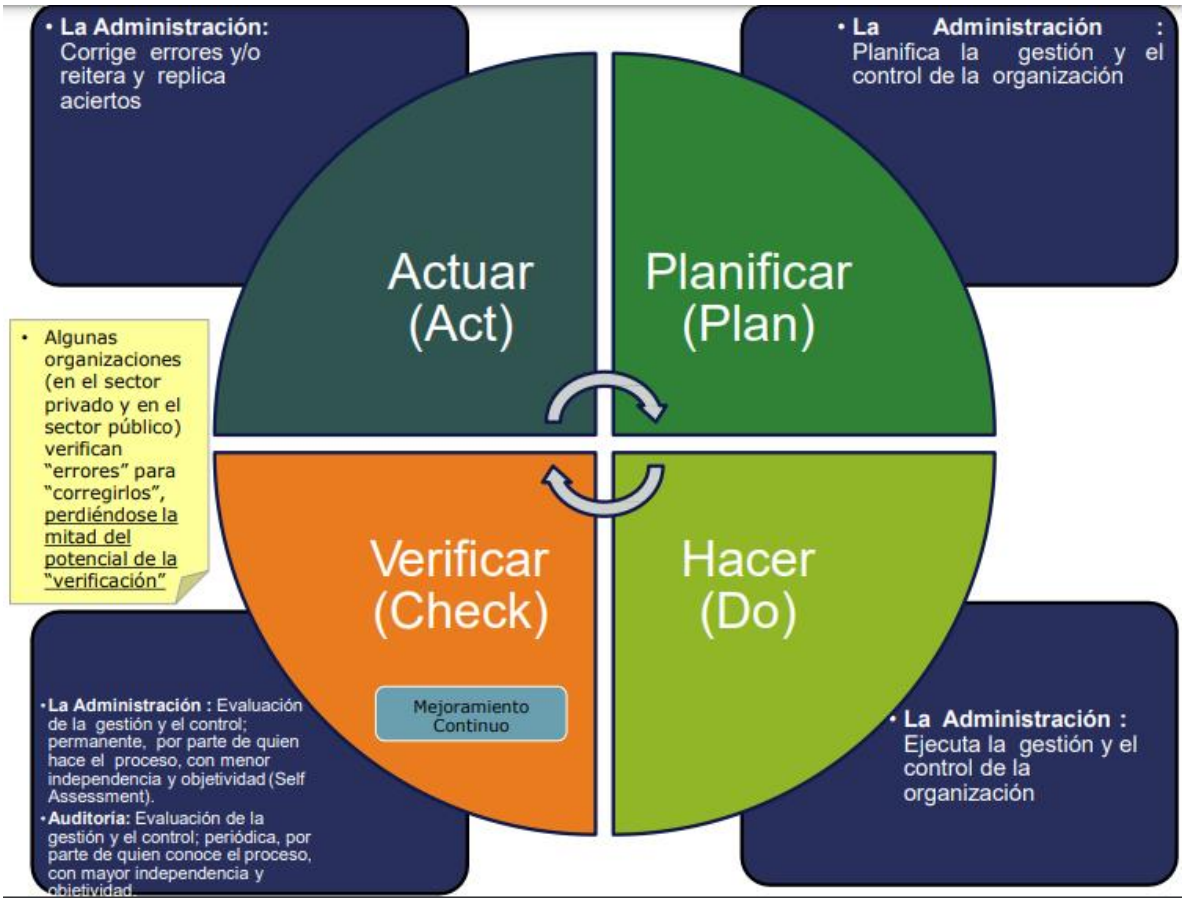
Gestión (Eficiencia & Efectividad): Cuando la balanza está desbalanceada hacia el lado de la gestión se afecta el control, cuando esto pasa es usualmente en el sector privado (por ejemplo: lo único importante es vender, mejores y más rápidas ventas, alcanzar los resultados, el precio de la acción, etc.)

Control (Riesgo & Control): Cuando la balanza está desbalanceada hacia el lado del control se afecta la gestión, cuando esto pasa es usualmente en el sector público (por ejemplo: muchas aprobaciones, muchas firmas, revisiones excesivas, burocracia, etc.). Y lo que es peor es que algunas veces son falsos controles, creando una falsa seguridad, “cuando todos revisan todo, en realidad nadie revisa nada”

Administración y auditoría deberían trabajar de acuerdo a sus roles in los dos lados de la balanza, sin embargo a veces ellos prefieren/deciden trabajar solo en un lado, y cunado esto pasa es usualmente de esta manera:

- ADMINISTRACIÓN.- extremadamente enfocado en gestión sin considerar controles.
- AUDITORÍA.- extremadamente enfocado en controles sin considerar gestión.

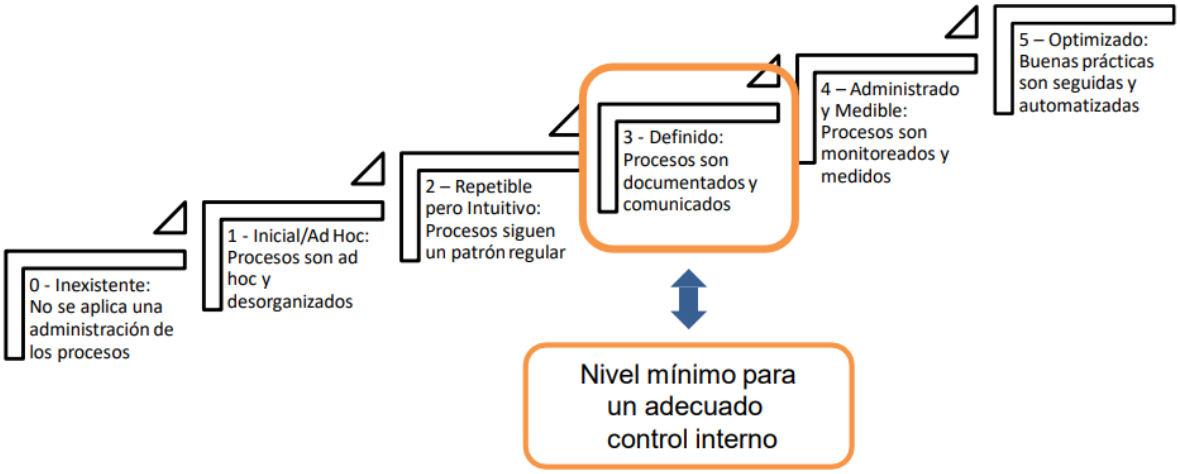
Equilibrio entre riesgos y controles.	
Los componentes de la aceptación de riesgos excesivos:	Consecuencias de la implementación de controles excesivos:
• Pérdida potencial de activos • Toma de decisiones de negocios incorrecta o ineficaz • Incumplimiento potencial con las leyes y regulaciones • Posibilidad de que se cometan fraudes	• Aumento de la burocracia • Exceso del costo de producción • Complejidad innecesaria de los controles • Incremento del tiempo de ciclo • Actividades que no agregan valor



EVALUACIONES COMPLEMENTARIAS

- LA ADMINISTRACIÓN
    - Permanente
    - Por quien hace y conoce el proceso
    - Menos independiente y objetiva
        - Monitoreo continuo
- AUDITORÍA
    - Periódica
    - Por quien conoce el proceso
    - Más independiente y objetiva
        - Auditoría continua

Niveles de Madurez en los Procesos.



CONTROL INTERNO.

Proceso que lleva a cabo el control diario de todas las actividades de la operación sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la dirección de la organización, así como los requerimientos legales.

Objetivos del control interno.

Responsabilidades frente al sistema de control interno.

En resumen:

- Es un proceso que hace parte de los demás sistemas y procesos de la empresa.
- Proporciona una seguridad razonable, más que absoluta, de que se lograran los objetivos definidos.
- Es concebido y ejecutado por personas de todos los niveles de la organización a través de sus acciones y palabras.

- ✓ "El control no es para ir mas lento, es para poder ir rápido pero seguro".
- ✓ "La confianza no es un control".
- ✓ Un buen control no garantiza el éxito… pero un mal control si garantiza el fracaso"
- ✓ "Hay que balancear la gestión y el control"
- ✓ "EL control interno es responsabilidad de todos"
- ✓ "Si no está documentado no existe"

CONTROL INTERNO INFORMÁTICO

Se refiere a realizar en los diferentes sistemas (centrales, departamentales, redes locales, PC's, etc.) y entornos informáticos (producción, desarrollo o pruebas) el control de las diferentes actividades operativas.

Objetivos principales:

1. Controlar que todas las actividades en los sistemas que se realizan cumplan los procedimientos y normas establecidos, evaluar sus beneficios y asegurarse del cumplimiento de normas legales.
2. Asesorar sobre el conocimiento de las normas.
3. Colaborar y apoyar el trabajo de Auditoria informática, así como de las auditorías externas al grupo.
4. Definir, implantar y ejecutar mecanismos y controles para comprobar el logro del servicio informático.

Tipos de control interno:

En el ambiente informático, el control interno se materializa fundamentalmente en controles de dos tipos:

- Controles manuales: Aquellos que son ejecutados por el personal del área usuaria o de informática sin la utilización de herramientas computacionales.
- Controles automáticos: Son generalmente los incorporados en el software, llámense estos de operación, de comunicación, de gestión de base de datos, programas de aplicación, etc.

Categorías de control interno.

De acuerdo a su finalidad se clasifican en:

- Controles preventivos: Para tratar de evitar un hecho, como un software de seguridad que impida los accesos no autorizados al sistema.
- Controles detectivos: Cuando fallan los preventivos para tratar de conocer cuanto antes el evento.
- Controles correctivos: Facilitan la vuelta a la normalidad cuando se ha producido incidencias.

Auditoría informática y control interno (diferencias).

	CONTROL INTERNO INFORMATICO	AUDITOR INFORMÁTICO
Diferencias:	1.- Análisis de los controles en el día a día. 2.- Informa a la Dirección del Departamento de Informática (Gobierno TI). 3.- Realizada por la administración de TI.	1.- Análisis en un momento determinado 2.- Informa a la Dirección General de la Organización. 3.- Realizada por auditores internos o externos.

Aspectos de implantación en un sistema de control informático.

Para la implantación de un sistema de controles internos habría que definir:

1. Gestión de sistema de información
2. Administración de sistemas.
3. Seguridad
4. Gestión del cambio

Gestión de sistema de información: Políticas, pautas y normas técnicas que sirvan de base para el diseño y la implantación de los sistemas de información y de los controles correspondientes.

Administración de sistemas: Controles sobre la actividad de los centros de datos y otras funciones de apoyo al sistema, incluyendo la administración de las redes.

Seguridad: Incluye las tres clases de controles fundamentales implantados en el software del sistema, integridad del sistema, confidencialidad (control de acceso) y disponibilidad.

Gestión del cambio: Separación de las pruebas y la producción a nivel del software y controles de procedimientos para la migración de programas software aprobados y probados.

Áreas de Aplicación del Control Interno Informático.

1. Controles generales organizativos
2. Controles de desarrollo, adquisición y mantenimiento de sistemas de información.
3. Controles sobre las aplicaciones
4. Controles sobre la administración de sistemas de información.
5. Controles sobre específicas tecnologías.

6. Controles de Calidad

Controles generales organizativos.

- Políticas.
- Reglamentos.
- Manuales e Instructivos.
- Formatos
- Estándares.
- Procedimientos.
- Descripción de funciones y responsabilidades
- Informes de Control.

Controles de desarrollo, adquisición y mantenimiento de sistemas de información.

- Metodología del ciclo de vida del desarrollo de sistemas
- Explotación y mantenimiento.

Controles sobre aplicaciones.

- Control de entrada: Datos completos, exactos, válidos y autorizados por única vez.
- Control de tratamiento de datos: procesamiento de las transacciones es completa, adecuado y autorizado.
- Control de salida de datos: Presentación completo de los resultados.

Controles sobre la administración de los sistemas de información.

- Planificación y gestión de los recursos informáticos.
- Controles para usar de manera efectiva los recursos en ordenadores
- Revisiones técnicas sobre equipos de infraestructura.
- Procedimientos y formatos de selección del software del sistema, de instalación, de mantenimiento, de seguridad y de control de cambios.
- Seguridad física y lógica.

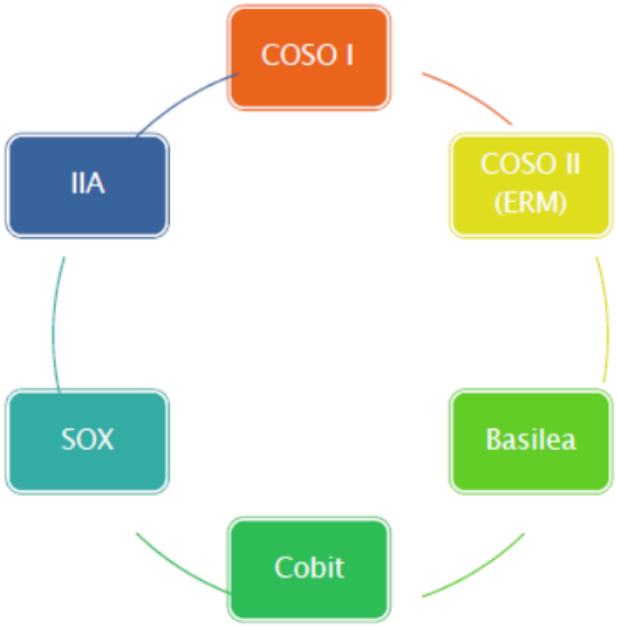
Controles específicos sobre tecnologías.

- Controles en servicios informáticos.
- Controles centralizados de ordenadores personales
- Controles conexiones con host y redes de área local.

Controles de calidad.

- Normas de documentación de programas
- Normas de pruebas de programas
- Normas con respecto a pruebas de sistemas
- Pruebas pilotos o en paralelo
- Evaluación del cumplimiento del software.

Control interno modelos internacionales.



Informe COSO.

- COSO I:
  - Se creó en 1992.
  - Evalúa y Mejora el sistema de control interno en las entidades
- COSO II**:**
  - Se creó en 2004.
  - Es un marco integrado sobre análisis de riesgo.
- COSO III:
  - Se creó en 2013.
  - Es una actualización y mejora de COSO I

Informe COSO III- Definición.

Es un marco de referencia o modelo común de control interno contra el cual las empresas y organizaciones pueden evaluar sus sistemas de control interno.

Objetivos:

- Establecer una definición común de control interno que responda a las necesidades de las distintas partes.
- Facilitar un modelo en base al cual las empresas y otras entidades, cualquiera sea su tamaño y naturaleza, puedan evaluar sus sistemas de control interno.

COSO:

- Ambiente de control:
    1. Demostrar compromiso con la integridad y los valores éticos.
    2. Ejercer la responsabilidad de supervisión.
    3. Establecer la estructura, la autoridad y la responsabilidad.
    4. Demostrar compromiso con las competencias.
    5. Aplicar la rendición de cuentas.

- Evaluación de pago:
    6. Especificar objetivos adecuados.
    7. Identificar y analizar los riesgos.
    8. Evaluar el riesgo de fraude.
    9. Identificar y analizar cambios significativos.

- Actividades de Control:
    10. Seleccionar y desarrollar actividades de control
    11. Seleccionar y desarrollar controles generales sobre la tecnología

12. Implementación a través de políticas y procedimientos

- Información & Comunicación:
    13. Utilizar información pertinente
    14. Comunicación interna
    15. Comunicación externa

- Actividades de Monitoreo:
    16. Realizar evaluaciones continuas y / o separadas
    17. Evaluar y comunicar las deficiencias

Estándar de Verificación de Seguridad en Aplicaciones 3.0.1 (ASVS).

El ASVS es un esfuerzo comunitario por establecer un marco de referencia para los requisitos de seguridad, controles funcionales y no funcionales necesarios al diseñar, desarrollar y testear aplicaciones web modernas.

ASVS v3.0 es la culminación de un esfuerzo comunitario y de retroalimentación por parte de la industria. En esta versión, nos pareció importante estudiar las experiencias de casos de uso del mundo real relacionados con la adopción de ASVS.

En la versión 3.0, se ha añadido varias secciones nuevas, incluyendo configuración, Web Services, aplicaciones cliente, para hacer la norma más aplicable a aplicaciones modernas, comúnmente responsive, con amplio uso de interfaces de usuario HTML5 o móvil, llamando a un conjunto común de Web Services REST, utilizando autenticación SAML.

Se ha reducido también las duplicaciones en la norma, por ejemplo, para asegurarnos de que un desarrollador móvil no necesite re-testear los mismos elementos varias veces.

Se ha proporcionado la correspondencia con el CWE. Esta correspondencia utilizarse para identificar información tal como la probabilidad de explotación, consecuencia de una explotación exitosa y en términos generales tener la visión de lo que podría salir mal si un control de seguridad no se utiliza o no se aplican eficazmente para mitigar la debilidad.

Por último, buscan ayuda en la comunidad con el fin de generar sesiones para la revisión por pares durante las conferencias de AppSec EU 2015 y una sesión final de trabajo en AppSec USA 2015 con el fin de incluir una enorme cantidad de comentarios de la comunidad. Durante la revisión, si el significado de un control fue cambió sustancialmente, se creó un nuevo control dejando el antiguo como obsoleto.

El Estándar de Verificación de Seguridad en Aplicaciones define tres niveles de verificación de seguridad, incrementando la profundidad con cada nivel.

- ASVS nivel 1 se encuentra dirigido a todo tipo de software.
- ASVS nivel 2 es para aplicaciones que contienen datos sensibles, que requieren protección.
- ASVS nivel 3 es para las aplicaciones más críticas - aplicaciones que realizan transacciones de alto valor, contienen datos médicos confidenciales, o cualquier aplicación que requiera el más alto nivel de confianza.

Cómo utilizar este estándar.

Una de las mejores maneras de emplear el Estándar de Verificación de Seguridad en Aplicaciones es utilizarlo como checklist de seguridad específica para su aplicación, plataforma u organización.

Nivel 1: Oportunista.

Una aplicación alcanza ASVS nivel 1 si se defiende adecuadamente contra vulnerabilidades de seguridad de aplicaciones que son fáciles de descubrir y se incluyen en el OWASP Top 10 u otras listas similares.

Este nivel es apropiado típicamente para aplicaciones donde se requiere escasa confianza en el uso correcto de los controles de seguridad, o para proporcionar un análisis rápido a un conjunto de aplicaciones de una organización, o asistir en la elaboración de una lista de requerimientos de seguridad con prioridades como parte de un esfuerzo de múltiples fases.

Los controles de nivel 1 pueden ser asegurados automáticamente por herramientas o manualmente sin acceso al código fuente.

Nivel 2: Estándar

Una aplicación alcanza ASVS nivel 2, si se defiende adecuadamente contra la mayoría de los riesgos asociados con el software de hoy en día.

El Nivel 2 asegura que controles de seguridad se encuentran en el lugar adecuado, son efectivos y son utilizados dentro de la aplicación. Este nivel es generalmente apropiado para aplicaciones que manejan transacciones business-to-business, información de salud, implementan funciones sensibles o críticas para el negocio o incluyen el proceso de otros activos sensibles.

Nivel 3: Avanzado

El nivel 3 en ASVS es el más alto nivel de verificación dentro de ASVS. Este nivel está reservado normalmente para aplicaciones que requieren niveles significativos de verificación de seguridad, como las que se encuentran dentro de áreas de militares, salud, seguridad, infraestructuras, etc.

Las organizaciones pueden requerir del nivel 3 para aplicaciones que realizan funciones críticas, donde una falla de seguridad podría afectar significativamente sus operaciones y hasta su supervivencia. Un ejemplo en la aplicación del nivel 3 de ASVS se proporciona a continuación. Una aplicación alcanza el nivel 3 si se defiende adecuadamente contra vulnerabilidades de seguridad avanzadas y también demuestra los principios de un buen diseño de seguridad.

Aplicando ASVS en la práctica

Diferentes amenazas poseen diferentes motivaciones. Algunas industrias tienen activos de información únicos y valiosos y deben cumplir regulaciones y normas específicas de dichas industrias.

A continuación, se proporcionan recomendaciones con respecto a los niveles de ASVS específicas para algunas industrias.

Aunque existen criterios únicos y diferencias en las amenazas para cada sector, una amenaza común a todos los segmentos o industrias, son los ataques oportunistas. Estos buscarán cualquier aplicación vulnerable fácilmente explotable. Por esta razón el nivel 1 se recomienda para toda aplicación. Se sugiere este punto de partida para manejar los riesgos más fáciles de encontrar.

Industria	Perfil de amenaza	L1 Recomendación	L2 Recomendación	L3 Recomendación
Financiera y Seguros	Aunque este segmento experimentará intentos de atacantes oportunistas, a menudo es visto como un objetivo de alto valor por atacantes motivados y los ataques se deben muy a menudo a motivos financieros. Comúnmente, los atacantes buscan datos o credenciales de la cuenta que pueden utilizar para cometer fraudes o beneficiarse directamente aprovechando la	Todas las aplicaciones accesibles desde la red.	Aplicaciones que contienen información sensible como números de tarjeta de crédito, información personal, que puede mover una cantidad limitada de dinero de manera limitada. Los ejemplos incluyen: (i) transferir dinero entre cuentas en la	Aplicaciones que contengan grandes cantidades de información sensible o que permiten que sea rápido la transferencia de grandes sumas de dinero (p. ej. transferencias) o transferencia de grandes sumas de dinero en forma de transacciones

	funcionalidad de flujo de dinero en aplicaciones. Las técnicas incluyen a menudo credenciales robadas, ataques a nivel de aplicación y la ingeniería social. Algunas consideraciones importantes de cumplimiento incluyen EL ESTÁNDAR PCI DSS (PCI DSS), Gramm Leech Bliley Act y Sarbanes-Oxley (SOX).		misma institución o (ii) una forma más lenta del movimiento de dinero (por ejemplo, ACH) con límites de transacción o (iii) transferencias en línea con límites de transferencia dentro de un período de tiempo.	individuales o como un lote de transferencias pequeñas.

Industria	Perfil de amenaza	L1 Recomendación	L2 Recomendación	L3 Recomendación
Manufactura, profesional, transporte, tecnología, utilidades, infraestructura y defensa	Estas industrias no parecen tener mucho en común, pero los agentes de amenaza que suelen atacar a las organizaciones en este segmento son más propensos a realizar ataques enfocados con más tiempo, habilidad y recursos. A menudo la información sensible o los sistemas no son fáciles de localizar y requieren utilizar o manipular individuos que	Todas las aplicaciones accesibles desde la red.	Aplicaciones que contienen información interna o información sobre empleados que pueden aprovecharse utilizando la ingeniería social. Aplicaciones que contiene información poco esencial, pero de	Aplicaciones que contiene valiosa propiedad intelectual, secretos comerciales o secretos del gobierno (p. ej. en los Estados Unidos esto puede ser cualquier cosa clasificados en secreto o superior) que es fundamental

	trabajen dentro de la organización, utilizando técnicas de ingeniería social. Los ataques pueden involucrar individuos que trabajan dentro de la organización, extraños a la organización, o una combinación de ambos. Sus objetivos pueden incluir acceso a la propiedad intelectual para obtener ventajas estratégicas o tecnológicas. Tampoco queremos pasar por alto a los atacantes que buscan abusar la funcionalidad de la aplicación para influenciar el comportamiento de la aplicación o alterar sistemas sensibles. La mayoría de los atacantes buscan información sensible que puede ser utilizada directa o indirectamente para beneficiarse al incluir datos personales a la información de pago. A menudo los datos pueden utilizarse para una variedad de esquemas de fraude, robo de identidad o pagos fraudulentos.		importante propiedad intelectual o secretos comerciales.	para la supervivencia o el éxito de la organización. Aplicaciones que controlan funcionalidad sensible (p. ej. transporte, fabricación de equipos, sistemas de control) o que tienen la posibilidad de amenazar la seguridad.

Industria	Perfil de amenaza	L1 Recomendación	L2 Recomendación	L3 Recomendación
Salud	La mayoría de los atacantes está buscando información sensible que puede ser utilizada directa o indirectamente para beneficiarse al incluir datos personales a la información de pago. A menudo los datos pueden utilizarse para una variedad de esquemas de fraude, robo de identidad y pagos fraudulentos. Para Los Estados Unidos existen el Health Insurance Portability and Accountability Act (HIPAA) http://www.hhs.gov/ocr/privacy/	Todas las aplicaciones accesibles desde la red	Aplicaciones con cantidades pequeñas o moderadas de información médica confidencial (información de salud protegida), información de identificación personal o datos de pago.	Aplicaciones utilizadas para el control de equipos médicos, dispositivos o registros que pueden poner en peligro la vida humana. Sistemas de pago de Punto de venta y (POS) que contienen grandes cantidades de datos de transacciones que podrían ser utilizados para cometer fraudes. Esto incluye las interfaces administrativas de estas aplicaciones
Venta por menor, alimento, hospitalidad	Muchos de los atacantes en este segmento utilizan tácticas oportunistas de "aplaste y agarre". Sin embargo, también existe una amenaza regular de ataques específicos en aplicaciones que contienen información de pagos, que realizan transacciones financieras o almacenan información personal que pueda ser identificable.	Todas las aplicaciones accesibles desde la red.	Adecuado para aplicaciones de negocios, Catálogo de la información del producto, información corporativa interna y aplicaciones con información limitada del	Sistemas de pago de Punto de venta y (POS) que contienen grandes cantidades de datos de transacciones que podrían ser utilizados para cometer fraudes. Esto incluye las interfaces administrativas de estas aplicaciones. Aplicaciones con un

	Aunque menos probable que las amenazas antes mencionadas, también existe la posibilidad de amenazas más avanzadas las cuales atacan a este segmento de la industria para robar propiedad intelectual, obtener inteligencia competitiva o ganar una ventaja con la organización la cual se ha atacado o de un socio en negociaciones		usuario (p. ej. información de contacto). Aplicaciones con cantidades pequeñas o moderadas de la funcionalidad de datos o de comprobación de pago	gran volumen de información sensible como números de tarjeta de crédito, nombres completos, documentos de indentidad, etc.

Caso de Estudio 1: ASVS como guía de prueba de seguridad

En una Universidad privada en Utah, Estados Unidos, el equipo rojo del campus utiliza el OWASP ASVS como guía al realizar tests de penetración a aplicaciones. Es utilizado a lo largo del proceso de pruebas, desde la planificación inicial, definiendo reuniones de orientación para las actividades de la prueba y como una manera de enmarcar las conclusiones del informe final entregado a los clientes. El equipo rojo también organiza capacitaciones para el equipo utilizando el ASVS.

El equipo rojo del Campus realiza tests de penetración de redes y aplicaciones para varios departamentos del campus como parte de la estrategia de seguridad de la información general de la Universidad. Durante las reuniones de planificación iniciales, los clientes suelen ser reticentes a dar autorización para que su aplicación sea puesta a prueba por un equipo de estudiantes. Al presentar el ASVS y explicando a los interesados que las actividades de pruebas son guiadas por esta estándar, y que el informe final incluirá cómo se comporta la aplicación en comparación con el estándar, muchas preocupaciones quedan inmediatamente aclaradas. Luego, el ASVS es utilizado durante la evaluación para ayudar a determinar cuánto tiempo y esfuerzo se utilizará en la prueba. Mediante el uso de los niveles de verificación predefinidas de la ASVS, el equipo rojo explica el enfoque basado en riesgo de las pruebas a realizar. Esto ayuda al cliente, los actores y el equipo para llegar a un acuerdo sobre un alcance apropiado para la aplicación en cuestión.

Una vez que el test comienza, el equipo rojo utiliza el ASVS para organizar actividades y dividir la carga de trabajo. Al realizar el seguimiento de los requisitos de verificación que han sido probados y que se encuentran pendientes, el gerente de proyecto para el equipo puede observar fácilmente el avance de las pruebas. Esto conduce a mejorar la comunicación con los clientes y permite al jefe de proyecto gestionar mejor los recursos. Dado que el equipo rojo está compuesto principalmente de estudiantes, la mayoría de los miembros del equipo tienen múltiples demandas de su tiempo proveniente de diferentes cursos. Las tareas bien definidas, basadas en los requisitos de verificación individual o categorías totales, ayudan a los miembros del equipo a saber exactamente qué debe

analizarse y que estos puedan proporcionar estimaciones precisas sobre cuánto tiempo tardarán para completar las tareas. La actividad de informar también se beneficia de la clara organización del ASVS, debido a que los miembros del equipo pueden reportar sus hallazgos antes de continuar con el siguiente punto del estándar, generando el informe de forma simultánea con la ejecución de las pruebas de penetración.

Estudio de caso 2: un SDLC seguro

Un emprendimiento «start-up» que busca proporcionar análisis de grandes datos a instituciones financieras reconoce que implementar seguridad durante el desarrollo de su aplicación es una de las prioridades más altas de la lista de requisitos para acceder y procesar meta-datos financieros. En este caso, la Compañía «start-up» ha optado por utilizar el ASVS como base de su ciclo de desarrollo ágil.

La compañía «start-up» utiliza el ASVS para generar casos de uso e historias para cuestiones de seguridad funcional, tales como la mejor manera de implementar la funcionalidad para iniciar la sesión en la aplicación. La compañía «start-up» usa ASVS de forma diferente en comparación a la mayoría - ellos tratan de ver a través de ASVS, recogiendo los requisitos que se adhieren al sprint actual, y lo agregan directamente a la acumulación del sprint si es un requisito funcional, o como una limitación a casos de uso existentes si no son funcionales. Por ejemplo, la adición de la autenticación TOTP, junto con las políticas de contraseñas y servicio web que de detección de ataques de fuerza bruta. En los sprints futuros, los requisitos adicionales se seleccionarán basados en el criterio «justo a tiempo», o que «no se va a necesitar».

Evaluando que el software ha alcanzado un nivel de verificación

Postura de OWASP en certificaciones de ASVS y las marcas de confianza

OWASP, como organización independiente sin fines de lucro, no certifica proveedores, verificadores ni software.

Tales afirmaciones de aseguramiento, sellos de confianza o certificaciones no son oficialmente validadas, registradas o certificadas por OWASP, por lo tanto, una organización que cuenta con ese punto de vista debe ser cautelosa en depositar su confianza en cualquier tercero o sello de confianza que clame que tiene una certificación de ASVS.

Esto no debe inhibir organizaciones para ofrecer dichos servicios de garantía, con tal de que no pretendan proveer una certificación oficial de OWASP.

Guía para las organizaciones certificadoras

El estándar de verificación de seguridad en aplicaciones puede ser utilizado como un libro abierto de verificación para la aplicación, en conjunto con el acceso abierto y sin restricciones a arquitectos y desarrolladores, documentación de proyectos, código fuente, acceso autenticado al sistema (incluyendo por lo menos una cuenta en cada rol), particularmente para las verificaciones de nivel 2 y 3.

Una práctica estándar en la industria es mantener papeles de trabajo detallados, imágenes o videos, registros electrónicos de las pruebas, registros proxy y notas asociadas como un script de limpieza. Pueden ser realmente útiles como pruebas de los hallazgos para la mayoría de los desarrolladores que tengan dudas. No es suficiente con ejecutar una herramienta e informar sobre de las fallas; En caso de controversia, debe existir prueba suficiente que garantice demostrar que cada requisito verificado de hecho ha sido probado.

El papel de las herramientas automáticas de pruebas de penetración

Las herramientas automatizadas buscan brindar la mayor cobertura posible y ejecutar tantos parámetros como sea posible con varias formas de entradas maliciosas.

No es posible completar totalmente la verificación ASVS utilizando solamente herramientas automáticas. Mientras que una gran mayoría de los requisitos en el nivel 1 se pueden verificar por medio de pruebas automatizadas, la mayoría no lo son.

El rol del test de penetración

Es posible realizar una prueba de penetración manual y verificar todos los puntos del nivel L1 sin necesidad de acceso al código fuente, aunque esta no es una práctica muy utilizada. Para el nivel L2 se requiere al menos algún acceso a los desarrolladores, documentación, código y acceso autenticado al sistema. Una cobertura completa de pruebas de penetración del nivel 3 no es posible, como la mayoría de los problemas adicionales incluyen revisión de configuración del sistema, revisión de código malicioso, modelado de amenazas y otros artefactos de prueba de penetración.

Como una guía de arquitectura de seguridad detallada.

Uno de los usos más comunes para el estándar de verificación de seguridad en aplicaciones es su utilización como un recurso para arquitectos de seguridad. Los dos marcos de la arquitectura de seguridad, SABSA o TOGAF, carecen de una gran cantidad de información necesaria para completar por medio de una revisión de arquitectura aspectos de seguridad de la aplicación. ASVS puede utilizarse mitigar esas carencias permitiendo a los arquitectos de seguridad elegir controles adecuados para problemas comunes, tales como patrones de protección de datos y estrategias de validación de entradas de datos.

Como reemplazo para checklist de verificación generadas por terceros

Muchas organizaciones pueden beneficiarse de la adopción del ASVS, eligiendo uno de los tres niveles, o utilizar ASVS y refinar únicamente lo que se requiere para cada nivel de riesgo de la aplicación en un dominio específico. Recomendamos este tipo de combinación o adaptación del ASVS original mientras se mantiene la trazabilidad, por lo que si una aplicación ha pasado requisito 4.1, esto significa lo mismo tanto para el refinamiento como para el estándar a medida que éste evolucione.

Como una guía para pruebas unitarias y de integración automatizadas

El ASVS está diseñado para ser altamente verificable, con la sola excepción de requisitos de arquitectónicos y de código malicioso. A través de la generación de pruebas unitarias y de integración (tanto específicas como de fuzzing), la aplicación se aproxima a auto verificase y validarse con cada construcción.

Asimismo, se deben incluir pruebas al parámetro de contraseña para las más comunes, su longitud, inyección de byte nulo, eliminación del parámetro, XSS, enumeración de cuentas y mucho más.

Como capacitación para el desarrollo seguro

ASVS también puede utilizarse para definir características de software seguro. Muchos cursos de “codificación segura” son simplemente cursos éticos de hacking con un ligero toque de consejos sobre codificación. Esto no ayuda a los desarrolladores de sistemas. En cambio, cursos de desarrollo seguro pueden usar la guía ASVS con un fuerte enfoque en los controles pro-activos en esta, en lugar de cosas negativas del OWASP Top 10.

Proyectos OWASP que utilizan ASVS

Security Knowledge Framework

https://www.owasp.org/index.php/OWASP_Security_Knowledge_Framework

Para entrenar desarrolladores en la escritura de código seguro - El proyecto SKF es una aplicación completamente gratis escrita en Python-Flask que utiliza el estándar de verificación de seguridad OWASP para aplicaciones, pensada para entrenar en la escritura de código seguro desde su diseño.

OWASP Zed ataque Proxy (ZAP)

https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

OWASP Zed (ZAP) es una herramienta de fácil uso e integrada para la búsqueda de vulnerabilidades en aplicaciones web. Está diseñada tanto para ser utilizado por personas con amplia experiencia en seguridad, así como desarrolladores y testers funcionales que son nuevos en pruebas de penetración. ZAP ofrece escaneos automatizados e integra un conjunto de herramientas que permiten encontrar vulnerabilidades de seguridad manualmente.

OWASP Cornucopia

https://www.owasp.org/index.php/OWASP_Cornucopia

Cornucopia de OWASP es un mecanismo en forma de un juego de cartas que ayudar a equipos de desarrollo de software a identificar requisitos de seguridad utilizado metodologías ágiles y procesos de desarrollo formales. Es un lenguaje agnótico de la tecnología y la plataforma. El contenido de Cornucopia fue seleccionado en base a la

estructura de la Guía Práctica de Codificación Segura de OWASP - guía de referencia rápida

(SCP), considerando adicionalmente el estándar de verificación de seguridad de OWASP para aplicaciones, la guía de pruebas de OWASP y los principios de programación segura de David Rook.

Requisitos de verificación detallada

V1. Arquitectura, diseño y modelado de amenazas

V2. Autenticación

V3. Gestión de sesiones

V4. Control de acceso

V5. Manejo de entrada de datos maliciosos

V7. Criptografía en el almacenamiento

V8. Gestión y registro de errores

V9. Protección de datos

V10. Comunicaciones

V11. Configuración de seguridad HTTP

V13. Controles Maliciosos

V15. Lógica de negocio

V16. Archivos y recursos

V17. Móvil

V18. Servicios Web (Nuevo en 3.0)

V19. Configuración (nuevo en 3.0)

V1: Arquitectura, diseño y modelado de amenazas

Objetivo de control

Asegurar que una aplicación verificada satisfaga los siguientes requisitos de alto nivel:

• Nivel 1, los componentes de la aplicación son identificados y tienen una razón de ser.

• Nivel 2, se ha definido la arquitectura y el código se adecúa a ésta.

• Nivel 3, la arquitectura y el diseño son los indicados, se utilizan y resultan eficaces.

Nota: Esta sección se ha introducido nuevamente en la versión 3.0, pero se utilizan en esencia los mismos controles arquitectónicos de la versión 1.0 del ASVS.

Requisitos

#	Descripción	1	2	3	Desde
1.1	Verificar que todos los componentes de la aplicación se encuentran identificados y asegurar que son necesarios.	✓	✓	✓	1.0
1.2	Verificar todos los componentes, tales como bibliotecas, módulos y sistemas externos, que no son parte de la aplicación pero que la misma los necesita para funcionar se han identificado.		✓	✓	1.0
1.3	Verificar que se ha definido una arquitectura de alto nivel para la aplicación.		✓	✓	1.0
1.4	Verificar que todos los componentes de la aplicación se definen de acuerdo a las funciones de negocio o de seguridad que proporcionan.			✓	1.0
1.5	Verificar que todos los componentes que no son parte de la aplicación pero que son necesarios para su funcionamiento, sean definidos de acuerdo a las funciones de negocio o de seguridad que proporcionan.			✓	1.0
1.6	Verificar que se ha realizado un modelo de amenazas para la aplicación en cuestión y que éste cubre riesgos asociados con la suplantación de identidad, manipulación, repudio, revelación de información y elevación de privilegios (STRIDE).			✓	1.0
1.7	Verificar que todos los controles de seguridad (incluyendo las bibliotecas que llaman a servicios de seguridad externos) tienen una implementación centralizada.		✓	✓	3.0
1.8	Verificar que los componentes están separados unos de		✓	✓	3.0

#	Descripción	1	2	3	Desde
	otros mediante controles de seguridad, tales como segmentación de la red, reglas de firewall, o grupos de seguridad basados en la nube.				
1.9	Verificar que la aplicación tiene una clara separación entre la capa de datos, la capa de control y la capa de presentación, tal que las decisiones de seguridad pueden aplicarse en sistemas confiables.		✓	✓	3.0
1.10	Verificar que no hay ninguna lógica de negocio sensible, claves secretas u otra información propietaria en el código del lado del cliente.		✓	✓	3.0
1.11	Verificar que todos los componentes de la aplicación, bibliotecas, módulos, frameworks, plataformas y sistemas operativos se encuentran libres de vulnerabilidades conocidas		✓	✓	3.0.1

V2: Requisitos de verificación de autenticación

Objetivo de control

Autenticación es el acto de establecer o confirmar, algo (o alguien) como auténtico, esto es, que lo que reclama sobre aquello es verdadero. Se debe asegurar que la aplicación satisface los siguientes requisitos de alto nivel:

• Verifica la identidad digital del remitente de una comunicación.

• Asegura que sólo los usuarios autorizados son capaces de autenticarse y que las credenciales sean transportadas de forma segura.

Requisitos

#	Descripción	1	2	3	Desde
2.1	Verificar que todas las páginas y recursos requieran autenticación excepto aquellos que sean específicamente destinados a ser públicos (Principio de mediación completa).	✓	✓	✓	1.0
2.2	Verificar que todos los campos de credenciales no reflejen las contraseñas del usuario. Cargar la credencial por parte de la aplicación implica que la misma fue almacenada de forma reversible o en texto plano, lo que se encuentra explícitamente prohibido.	✓	✓	✓	3.0.1
2.4	Verificar que todos los controles de autenticación se realicen del lado del servidor.	✓	✓	✓	1.0
2.6	Verificar que los controles de autenticación fallan de forma segura para evitar que los atacantes no puedan iniciar sesión.	✓	✓	✓	1.0
2.7	Verificar que los campos de contraseñas permiten o fomentan el uso de frases como contraseñas (passphrases) y no impiden el uso de gestores de contraseñas, contraseñas largas o altamente complejas.	✓	✓	✓	3.0.1
2.8	Verificar que toda función relacionada con la autenticación (como registro, actualización del perfil, olvido de nombre de usuario, recuperación de la contraseña, token perdido / deshabilitado, funciones de help desk o IVR) que pueda ser utilizada de forma indirecta como mecanismo de autenticación, sea al menos tan resistente a ataques como el mecanismo primario.	✓	✓	✓	2.0

#	Descripción	1	2	3	Desde
2.9	Verificar que la funcionalidad de cambio de contraseña solicite la contraseña anterior, la nueva contraseña y una confirmación de la contraseña.	✓	✓	✓	1.0
2.12	Verificar que todas las decisiones de autenticación son registradas en la bitácora sin almacenar información sobre la contraseña o el identificador de la sesión. Esto debería incluir los metadatos necesarios para investigaciones de seguridad.		✓	✓	3.01
2.13	Verificar que las contraseñas de las cuentas se encuentren almacenadas utilizando una rutina de hashing con una sal, y que requiera un factor de trabajo lo suficientemente alto para evitar un ataque de fuerza bruta.		✓	✓	3.0.1
2.16	Verificar que las credenciales son transportadas mediante un enlace cifrado adecuadamente y que todas las páginas/funciones que requieren que el usuario introduzca credenciales se realicen utilizando enlaces cifrados.	✓	✓	✓	3.0
2.17	Verificar que las funciones de recuperar contraseña y acceso no revelen la contraseña actual y que la nueva contraseña no se envíe en texto plano al usuario.	✓	✓	✓	2.0
2.18	Verificar que no es posible enumerar información mediante las funcionalidades de: inicio de sesión, reinicio o recuperación contraseñas.	✓	✓	✓	2.0
2.19	Verificar que no se utilizan contraseñas por defecto en la aplicación o cualquiera de los componentes utilizados por la misma (como "admin/password").	✓	✓	✓	2.0
2.20	Verificar que existen mecanismos de anti-automatización que previenen la verificación de credenciales obtenidas de forma masiva, ataques de fuerza bruta y ataques de bloqueos de cuentas.	✓	✓	✓	3.0.1
2.21	Verificar que todas las credenciales de autenticación para acceder a servicios externos a la aplicación se encuentran cifradas y almacenadas en un lugar protegido.		✓	✓	2.0
2.22	Verificar que las funcionalidades de recuperar contraseña y otras formas de recuperar la cuenta utilizan mecanismos de TOTP (Time-Based One-Time Password) u otro tipo de soft token, push a dispositivo móvil u otro tipo de mecanismo de recuperación offline. El uso de un valor aleatorio en un correo electrónico o SMS debe ser la última opción ya que son conocidas sus debilidades.	✓	✓	✓	3.0.1

#	Descripción	1	2	3	Desde
2.23	Verificar que el bloqueo de la cuenta se divida en estado de bloqueo suave y duro, y éstas no son mutuamente excluyentes. Si una cuenta está temporalmente bloqueada de forma suave debido a un ataque de fuerza bruta, esto no debe restablecer el bloqueo de estado duro.		✓	✓	3.0
2.24	Verificar que si la aplicación hace uso de conocimiento basado en preguntas (también conocido como "secreto"), las preguntas no violan leyes de privacidad y son lo suficientemente fuertes para proteger la cuenta de recuperaciones maliciosas.	✓	✓	✓	3.0.1
2.25	Verificar que el sistema puede configurarse para no permitir el uso de un número de contraseñas utilizadas anteriormente.		✓	✓	2.0
2.26	Verificar que la re-autenticación basada en riesgo, autenticación de dos factores o firma de transacciones se encuentra implementada en los lugares adecuados.		✓	✓	3.0.1
2.27	Verificar que existen medidas para bloquear el uso de contraseñas comúnmente utilizadas y contraseñas débiles.	✓	✓	✓	3.0
2.28	Verificar que todos los desafíos de autenticación, ya sea exitosa o fallida, responden en el mismo tiempo promedio.			✓	3.0
2.29	Verificar que secretos, llaves de API y contraseñas no se incluyen en el código fuente o en los repositorios en línea de código fuente.			✓	3.0
2.31	Verificar que, si una aplicación permite a los usuarios autenticarse, puedan hacerlo mediante autenticación de dos factores u otra autenticación fuerte, o cualquier esquema similar que proporcione protección contra la divulgación de nombres de usuario y contraseñas.		✓	✓	3.0
2.32	Verificar que las interfaces administrativas de la aplicación no sean accesibles a intrusos.	✓	✓	✓	3.0
2.33	Autocompletar de navegadores e integración con gestores de contraseñas deben estar permitidos a no ser que se encuentren prohibidos por políticas de riesgos.	✓	✓	✓	3.0.1

Referencias

• Guía de pruebas OWASP 4.0: Prueba de autenticación

https://www.owasp.org/index.php/Testing_for_authentication

• Cheat Sheet - Almacenamiento de Contraseña

https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet

• Cheat sheet - Olvido de Contraseña

https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet

• Escoger y usar preguntas de seguridad

https://www.owasp.org/index.php/Choosing_and_Using_Security_Questions_Cheat_Sheet

V3: Requisitos de verificación de gestión de sesiones

Objetivo de control

Uno de los componentes básicos de cualquier aplicación web es el mecanismo por el cual controla y mantiene el estado de un usuario al interactuar con ésta. Esto se refiere a manejo de sesiones y se define como el conjunto de todos los controles que rigen el estado completo de interacción entre un usuario y la aplicación basada en la web.

Se debe asegurar que la aplicación verificada satisface los siguientes requerimientos de manejo de sesiones de alto nivel:

• Las sesiones son únicas para cada individuo y no conjeturadas o compartidas

• Las sesiones son invalidadas cuando ya no son necesarias y el tiempo es limitado durante los períodos de inactividad.

Requisitos.

#	Descripción	1	2	3	Desde
3.1	Verificar que no se utiliza un gestor de sesiones personalizado, o que, si el gestor de sesiones es personalizado, éste sea resistente contra los ataques más comunes.	✓	✓	✓	1.0
3.2	Verificar que las sesiones se invalidan cuando el usuario cierra la sesión.	✓	✓	✓	1.0
3.3	Verificar que las sesiones se invalidan luego de un período determinado de inactividad.	✓	✓	✓	1.0
3.4	Verificar que las sesiones se invalidan luego de un período determinado de tiempo, independientemente de que se esté registrando actividad (timeout absoluto).			✓	1.0
3.5	Verificar que todas las páginas que requieren autenticación poseen acceso fácil y visible a la funcionalidad de cierre de sesión.	✓	✓	✓	1.0
3.6	Verificar que el identificador de sesión nunca se revele en URLs, mensajes de error o registros de bitácora. Esto incluye verificar que la aplicación no es compatible con la re-escritura de URL incluyendo el identificador de sesión.	✓	✓	✓	1.0
3.7	Verificar que toda autenticación exitosa y re-autenticaciones generen un nuevo identificador de sesión.	✓	✓	✓	1.0

3.10	Verificar que sólo los identificadores de sesión generados por la aplicación son reconocidos como activos por ésta.		✓	✓	1.0
3.11	Verificar que los identificadores de sesión son suficientemente largos, aleatorios y únicos para las sesiones activas.	✓	✓	✓	1.0
3.12	Verificar que los identificadores de sesión almacenados en cookies poseen su atributo “path” establecido en un valor adecuadamente restrictivo y que además contenga los atributos "Secure" y "HttpOnly"	✓	✓	✓	3.0
3.16	Verificar que la aplicación limita el número de sesiones concurrentes activas.	✓	✓	✓	3.0
3.17	Verificar que una lista de sesiones activas esté disponible en el perfil de cuenta o similar para cada usuario. El usuario debe ser capaz de terminar cualquier sesión activa.	✓	✓	✓	3.0
3.18	Verificar que al usuario se le sugiera la opción de terminar todas las otras sesiones activas después de un proceso de cambio de contraseña exitoso.	✓	✓	✓	3.0

Referencias

Para obtener más información, consulte:

• Guía de pruebas OWASP 4.0: sesión de prueba de manejo

https://www.OWASP.org/index.php/Testing_for_Session_Management

• Cheat Sheet – Gestión de sesiones

https://www.OWASP.org/index.php/Session_Management_Cheat_Sheet

V4: Requisitos de verificación del Control de acceso

Objetivo de control

Autorización es el concepto de permitir acceso a los recursos únicamente a aquellos que les ha sido permitido utilizarlos. Se debe asegurar que la aplicación verificada satisface los siguientes requisitos de alto nivel:

• Personas que acceden a recursos poseen credenciales válidas para hacerlo.

• Los usuarios se encuentran asociados con un conjunto bien definido de roles y privilegios.

• Los metadatos de Roles y permisos se encuentran protegidos de ataques de reutilización o manipulación.

Requisitos.

#	Descripción	1	2	3	Desde
4.1	Verificar que existe el principio de privilegio mínimo - los usuarios sólo deben ser capaces de acceder a las funciones, archivos de datos, URL, controladores, servicios y otros recursos, para los cuales poseen una autorización específica. Esto implica protección contra suplantación de identidad y elevación de privilegios.	✓	✓	✓	1.0
4.4	Verificar que el acceso a registros sensibles esté protegido, tal que sólo objetos autorizados o datos sean accesibles por cada usuario (por ejemplo, proteger contra la posible manipulación hecha por usuarios sobre un parámetro para ver o modificar la cuenta de otro usuario).	✓	✓	✓	1.0
4.5	Verificar que la navegación del directorio esté deshabilitada a menos que esto sea deliberadamente deseado. Además, las aplicaciones no deben permitir el descubrimiento o divulgación de metadatos de archivos o directorios, como carpetas que contengan Thumbs.db, DS_Store, o directorios .git o SVN.	✓	✓	✓	1.0
4.8	Verificar que los controles de acceso fallen de forma segura.	✓	✓	✓	1.0
4.9	Verificar que las mismas reglas de control de acceso implícitas en la capa de presentación son aplicadas en el servidor.	✓	✓	✓	1.0

#	Descripción	1	2	3	Desde
4.10	Verificar que todos los atributos de usuario, datos e información de las políticas utilizadas por los controles de acceso no puedan ser manipulados por usuarios finales a menos que sean específicamente autorizados.		✓	✓	1.0
4.11	Verificar que existe un mecanismo centralizado (incluyendo las bibliotecas que requieren servicios de autorización externa) para proteger el acceso a cada tipo de recursos protegidos.			✓	1.0
4.12	Verificar que todas las acciones de control de acceso pueden ser registradas y que todas las acciones fallidas son registradas.		✓	✓	2.0
4.13	Verificar que la aplicación o su infraestructura emite tokens anti-CSFR aleatorios existe otro mecanismo de protección de la transacción.	✓	✓	✓	2.0
4.14	Verificar que el sistema se pueda proteger contra el acceso permanente a funciones aseguradas, recursos o datos. Por ejemplo, que el sistema utilice un recurso gobernante que limite el número de ediciones por hora o para prevenir que la base de datos sea sobre-utilizada por un único usuario.		✓	✓	2.0
4.15	Verificar que la aplicación disponga de autorización adicional (como autenticación aumentada o adaptación de autenticación) para sistemas de valores bajos, y/o segregación de funciones para aplicaciones de alto valor para cumplir con los controles anti fraude según el análisis de riesgo de la aplicación y fraudes cometidos en el pasado.		✓	✓	3.0
4.16	Verificar que la aplicación aplique correctamente la autorización contextual para no permitir la manipulación de parámetros de la URL.	✓	✓	✓	3.0

Referencias

Para obtener más información, consulte:

• Guía de pruebas OWASP 4.0: Autorización

https://www.OWASP.org/index.php/Testing_for_Authorization

• Cheat Sheet – Control de acceso

https://www.OWASP.org/index.php/Access_Control_Cheat_Sheet

V5: Requisitos de verificación para Manejo de entrada de datos maliciosos

Objetivo de control

La debilidad más común de seguridad de las aplicaciones web es la falla en validar apropiadamente el ingreso de datos que provienen del cliente o del ambiente antes de ser utilizada. Esta debilidad conduce a casi todas las vulnerabilidades encontradas en aplicaciones web, tales como cross site scripting (XSS), inyecciones SQL, inyección de intérprete, ataques locale/Unicode, ataques a sistemas de archivos y desbordamientos de búfers.

Se debe asegurar que la aplicación verificada satisface los siguientes requisitos de alto nivel:

• Todas las entradas son correctamente validadas y adecuadas para el propósito previsto.

• No debe confiarse en datos de una entidad externa o del cliente y deben ser tratados como tales.

Requisitos

#	Descripción	1	2	3	Desde
5.1	Verificar que el entorno de ejecución no es susceptible a desbordamientos de búfer, o que los controles de seguridad previenen desbordamientos de búfer.	✓	✓	✓	1.0
5.3	Verificar que las fallas de validación de entradas de datos del lado del servidor sean rechazadas y registradas.	✓	✓	✓	1.0
5.5	Verificar que se aplican las rutinas de validación de entradas de datos del lado del servidor.	✓	✓	✓	1.0
5.6	Verificar que un único control de validación de entrada es utilizado por la aplicación para cada tipo de datos que es aceptado.			✓	1.0
5.10	Verificar que todas las consultas de SQL, HQL, OSQL, NOSQL y procedimientos almacenados, llamadas de procedimientos almacenados están protegidos por la utilización de declaraciones preparadas o parametrización de consultas, y por lo tanto no sean susceptibles a la inyección de SQL	✓	✓	✓	2.0

#	Descripción	1	2	3	Desde
5.11	Verificar que la aplicación no es susceptible a la inyección LDAP, o que los controles de seguridad previenen inyección LDAP.	✓	✓	✓	2.0
5.12	Verificar que la aplicación no es susceptible a la inyección de comandos del sistema operativo, o que los controles de seguridad previenen la inyección de comandos del sistema operativo.	✓	✓	✓	2.0
5.13	Verificar que la aplicación no es susceptible a la inclusión de archivo remoto (RFI) o inclusión de archivo Local (LFI) cuando el contenido es utilizado como una ruta a un archivo.	✓	✓	✓	3.0
5.14	Verificar que la aplicación no es susceptible a ataques comunes de XML, como manipulación de consultas XPath, ataques de entidad externa XML, y ataques de inyección XML.	✓	✓	✓	2.0
5.15	Asegurar que todas las variables string utilizadas dentro de HTML u otro lenguaje web interpretado en cliente se encuentra apropiadamente codificada manualmente o se utiliza plantillas que automáticamente codifican contextualmente para asegurar que la aplicación no sea susceptible a ataques DOM Cross-Site Scripting (XSS).	✓	✓	✓	2.0
5.16	Si el framework de la aplicación permite asignación automática de parámetros en masa (también llamada enlace automático de variables o variable biding) desde la petición entrante a un modelo, verificar que campos sensibles de seguridad como "*accountBalance*", "*role*" o "password" sean protegidos de enlaces automáticos maliciosos.		✓	✓	2.0
5.17	Verificar que la aplicación contenga defensas contra los ataques de contaminación de parámetros HTTP (agregar parámetros a la URL), particularmente si el framework de la aplicación no hace distinción sobre el origen de los parámetros de la petición (GET, POST, cookies, cabeceras, ambiente, etc.)		✓	✓	2.0
5.18	Verificar que las validaciones del lado del cliente se utilizan como una segunda línea de defensa, en adición a la validación del lado del servidor.		✓	✓	3.0
5.19	Verificar que todos los datos de entrada sean validados, no solamente los campos de formularios HTML sino también todos los orígenes de entrada como las llamadas REST, parámetros de consulta, encabezados HTTP, cookies, archivos por lotes, fuentes RSS, etc.; mediante validación positiva (lista blanca), o utilizando otras formas de validación menos eficaces tales como listas de rechazo transitorio (eliminando símbolos defectuosos), o rechazando malas entradas (listas negras).		✓	✓	3.0

#	Descripción	1	2	3	Desde
5.20	Verificar que datos estructurados fuertemente tipados son validados un esquema definido incluyendo; caracteres permitidos, longitud y patrones (p. ej. tarjeta de crédito o teléfono o validando que dos campos relacionados son razonables, tales como validación de coincidencia entre localidad y código postal).		✓	✓	3.0
5.21	Verificar que los datos no estructurados sean sanitizados cumpliendo medidas genéricas de seguridad tales como caracteres permitidos, longitud y que caracteres potencialmente dañinos en cierto contexto sean anulados (p. ej. nombres naturales con Unicode o apóstrofos, como ねこ o O'Hara)		✓	✓	3.0
5.22	Verificar que HTML no confiable proveniente de editores WYSIWYG o similares sean debidamente sanitizados con un sanitizador de HTML y se manejen apropiadamente según la validación de entrada y codificación.	✓	✓	✓	3.0
5.23	Para tecnologías de plantilla de codificación automática, si ésta se ha deshabilitado, asegurar que la sanitización de HTML esté habilitada en su lugar.		✓	✓	3.0
5.24	Verificar que los datos transferidos desde un contexto DOM a otro, utilice métodos de JavaScript seguro, como pueden ser .innerText y .val		✓	✓	3.0
5.25	Verificar que cuando se interprete JSON en navegadores, que JSON.parse sea el utilizado para interpretarlo y no eval().		✓	✓	3.0
5.26	Verificar que los datos de autenticación se eliminen del almacenamiento del cliente, tales como el DOM del navegador, después de terminada la sesión.		✓	✓	3.0

Referencias

Para obtener más información, consulte:

• Guía de pruebas OWASP 4.0: Validación de entradas de datos

https://www.OWASP.org/index.php/Testing_for_Input_Validation

• Cheat Sheet: Validación de entradas de datos

https://www.OWASP.org/index.php/Input_Validation_Cheat_Sheet

• Guía de pruebas OWASP 4.0: pruebas de contaminación de parámetro HTTP

https://www.OWASP.org/index.php/Testing_for_HTTP_Parameter_pollution_%28O

TG-INPVAL-004%29

• Cheat Sheet: Inyección LDAP

https://www.OWASP.org/index.php/LDAP_Injection_Prevention_Cheat_Sheet

• Guía de pruebas OWASP 4.0: Pruebas en el Cliente

https://www.OWASP.org/index.php/Client_Side_Testing

• Cheat Sheet: Prevención de Cross Site Scripting

https://www.OWASP.org/index.php/XSS_%28Cross_Site_Scripting%29_Prevention_Cheat_Sheet

• OWASP: Proyecto codificación de Java

https://www.OWASP.org/index.php/OWASP_Java_Encoder_Project

V6: Codificación / escape de salidas de datos

Esta sección se incorporó en V5 en el Estándar de Verificación de Seguridad en Aplicaciones 2.0. Requisitos de ASVS 5.16 tratan la codificación contextual de salida para ayudar a prevenir Cross Site Scripting.

V7: Requisitos de verificación para la criptografía en el almacenamiento

Objetivo de control

Asegure que una aplicación verificada satisfaga los siguientes requisitos de alto nivel:

• Que todos los módulos criptográficos fallen de forma segura y que los errores sean gestionados correctamente.

• Que se utilice un generador de números aleatorios adecuado cuando se requiere la aleatoriedad.

• Que el acceso a claves se gestiona de forma segura.

Requisitos

#	Descripción	1	2	3	Desde
7.2	Verificar que todos los módulos criptográficos fallen de forma segura, y que los errores sean manejados de tal manera que no permitan ataques Oracle padding.	✓	✓	✓	1.0
7.6	Verificar que todos los números aleatorios, nombres aleatorios de archivo, GUIDs aleatorios y cadenas aleatorias sean generados usando un módulo criptográfico aprobado del generador de números aleatorios cuando se pretende que estos valores no puedan ser adivinados o predecibles para un atacante.		✓	✓	1.0
7.7	Verificar que los algoritmos criptográficos utilizados por la aplicación hayan sido validados contra FIPS 140-2 o un estándar equivalente.	✓	✓	✓	1.0
7.8	Verificar que los módulos criptográficos operen en su modo aprobado según sus políticas de seguridad publicadas.			✓	1.0
7.9	Verificar que existe una política explícita para el manejo de las claves criptográficas (por ejemplo, generadas, distribuidas, revocadas y vencidas). Verificar que el ciclo de vida de las clave se aplique correctamente.		✓	✓	1.0

#	Descripción	1	2	3	Desde
7.11	Verificar que los consumidores de servicios criptográficos no poseen acceso directo a los datos de la clave. Aislar procesos criptográficos, incluyendo secretos maestros y considerar el uso de un módulo de seguridad de hardware (HSM).			✓	3.0.1
7.12	*La información de identificación personal* debe almacenarse de forma cifrada y verificar que la comunicación se lleve a cabo utilizando de canales protegidos.		✓	✓	3.0
7.13	Verificar que contraseñas y claves criptográficas sean sobreescritas con ceros en memoria tan pronto no sean necesarias, con el fin de mitigar ataques de volcado de memoria.		✓	✓	3.0.1
7.14	Verificar que todas las claves y contraseñas sean reemplazables, y sean generadas o reemplazadas durante la instalación.		✓	✓	3.0
7.15	Verificar que los números aleatorios sean creados con adecuada entropía, incluso cuando la aplicación se encuentre bajo carga intensa, o que la aplicación se degrade armoniosamente en tales circunstancias.			✓	3.0

Referencias

Para obtener más información, consulte:

● Guía de pruebas OWASP 4.0: Pruebas para criptografía débil

https://www.owasp.org/index.php/Testing_for_weak_Cryptography

● Cheat Sheet: Almacenamiento criptográfico

https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet

V8: Requisitos de verificación de gestión y registro de errores

Objetivo de control

El objetivo principal de la gestión y registro de errores es proporcionar una reacción útil para los usuarios, administradores y equipos de respuesta a incidentes. El objetivo no es crear cantidades masivas de registros, sino crear registros de alta calidad, con información útil y desechando ruido.

Los registros de bitácora de alta calidad a menudo contienen datos confidenciales y también deben ser protegidos según las leyes de privacidad de datos o directivas. Esto debe incluir:

• No recoger o registrar información confidencial si no es necesaria.

• Garantizar que toda la información registrada se gestiona de forma segura y es protegida según su clasificación de datos.

• Asegurar que los registros de bitácora no sean almacenados indeterminadamente, sino que posean un ciclo de vida útil lo más corta posible.

Si los registros contienen datos privados o confidenciales, cuya definición varía de país a país, éstos se convierten en parte de la información sensible y por lo tanto resulta muy atractiva para los atacantes.

Requisitos

#	Descripción	1	2	3	Desde
8.1	Verificar que la aplicación no emita mensajes de error o rastros de pilas que contengan datos sensibles que podrían ayudar a un atacante, incluyendo el identificador de sesión, versiones de software/entorno y datos personales.	✓	✓	✓	1.0
8.2	Verificar que la lógica de manejo de errores en controles de seguridad niegue el acceso por defecto.		✓	✓	1.0
8.3	Verificar que los controles del registro de seguridad proporcionen la capacidad para registrar los eventos de éxito y sobre todo los eventos de falla que son identificados como relevantes para la seguridad.		✓	✓	1.0
8.4	Verificar que cada registro de evento incluya la información necesaria para permitir una eventual investigación y correlación con otros eventos.		✓	✓	1.0

8.5	Verificar que todos los eventos que incluyen datos no confiables no se ejecuten como código en el software destinado a la visualización del registro.			✓	1.0
8.6	Verificar que los registros de seguridad estén protegidos contra modificación y acceso no autorizado.		✓	✓	1.0
8.7	Verificar que la aplicación no registre datos sensibles definidos en las leyes o regulaciones de privacidad local, datos organizacionales sensibles definidos por una evaluación de riesgos, o datos de autenticación sensible que podrían ayudar a un atacante, incluyendo identificadores de sesión del usuario, contraseñas, hashes o tokens de APIs.		✓	✓	3.0
8.8	Verificar que todos los símbolos no imprimibles y separadores de campos estén codificados correctamente en las entradas del registro, para evitar la inyección del registro que no permita seguir las pistas de un acto malicioso.			✓	2.0
8.9	Verificar que los campos del registro de fuentes confiables y no confiables sean identificables en las entradas del registro.			✓	2.0
8.10	Verificar que un registro de auditoría o similar permita la no repudiación de transacciones claves.		✓	✓	3.0
8.11	Verificar que los registros de seguridad poseen alguna forma de verificación o control de integridad para prevenir modificaciones no autorizadas.			✓	3.0
8.12	Verificar que los registros estén almacenados en una partición diferente a donde ejectua la aplicación con una rotación de registros adecuada.			✓	3.0

Referencias

Para obtener más información, consulte:

● OWASP Testing Guide 4.0: Pruebas de gestión de Errores

https://www.owasp.org/index.php/Testing_for_Error_Handling

V9: Requisitos de Verificación de Protección de Datos

Objetivo de control

Hay tres elementos clave para la protección de datos: Confidencialidad, Integridad y

Disponibilidad (CIA por sus siglas en inglés). Este estándar asume que la protección de datos se aplica en un sistema de confianza, como un servidor, que ha sido protegido debidamente y dispone de protecciones suficientes.

Las aplicaciones web deben asumir que todos los dispositivos de un usuario puedan ser comprometidos de alguna manera. Cuando una aplicación transmite o almacena información sensible dentro de dispositivos inseguros, como equipos compartidos, teléfonos y tabletas, la aplicación es responsable de que los datos almacenados en estos dispositivos sean cifrados y no pueden ser fácilmente o ilícitamente obtenidos, alterados o divulgados.

Se debe asegurar que la aplicación verificada satisface los siguientes requisitos de protección de datos de alto nivel:

• Confidencialidad: los datos deben ser protegidos de observación no autorizada o la divulgación tanto en tránsito como cuando están almacenados.

• Integridad: los datos deben protegerse siendo creados maliciosamente, alterados o eliminados por los intrusos no autorizados.

• Disponibilidad: los datos deben estar disponibles para usuarios autorizados cuando sea necesario

Requisitos

#	Descripción	1	2	3	Desde
9.1	Verificar que todos los formularios que contengan información sensible se les haya desactivado el almacenamiento de caché en el cliente, incluyendo funciones de autocompletar.	✓	✓	✓	1.0
9.2	Verificar que la lista de datos sensibles procesados por la aplicación se encuentra identificada, y que existe una política explícita de cómo debe controlarse el acceso a estos datos, cifrarse y reforzarse bajo las directivas de protección de datos pertinentes.			✓	1.0

#	Descripción	1	2	3	Desde
9.3	Verificar que toda información sensible es enviada al servidor en el cuerpo o cabeceras del mensaje HTTP (por ejemplo, los parámetros de la URL nunca se deben utilizar para enviar datos sensibles).	✓	✓	✓	1.0

9.4	Verificar que la aplicación establece encabezados anti-caché adecuados según el riesgo de la aplicación, tales como las siguientes:
	`Expires: Tue, 03 Jul 2001 06:00:00 GMTT`
	`Last-Modified: {now} GMT`
	`Cache-Control: no-store, no-cache, must-revalidate, max-age=0`
	`Cache-Control: post-check = 0, pre-check = 0`
	`Pragma: no-cache`
		✓	✓	✓	1.0

9.5	Verificar que, en el servidor, todas las copias almacenadas en caché o temporales de datos sensibles estén protegidos de accesos no autorizados o son purgados/invalidados después del acceso por parte del usuario autorizado.		✓	✓	1.0
9.6	Verificar que existe un mecanismo para eliminar de la aplicación todo tipo de dato sensible luego de transcurrido el tiempo definido por la política de retención.			✓	1.0
9.7	Verificar que la aplicación reduce al mínimo el número de parámetros en una solicitud, como campos ocultos, variables de Ajax, cookies y valores en encabezados.		✓	✓	2.0
9.8	Verificar que la aplicación tenga la capacidad para detectar y alertar sobre un número anormal de solicitudes para la recolección de datos por medio de extracción de pantalla (screen scrapping).			✓	2.0
9.9	Verificar que datos almacenados en el cliente (como almacenamiento local de HTML5, almacenamiento de la sesión, IndexedDB, cookies normales o las cookies de Flash) no contengan información sensible o información personal identificable.	✓	✓	✓	3.0.1
9.10	Verificar que el acceso a datos sensibles es registrado en bitácora, los datos son registrados acorde a las directivas de protección de datos o cuando el registro de los accesos es requerido.		✓	✓	3.0
9.11	Verificar que la información sensible mantenida en memoria es sobre escrita con ceros tan pronto como no es requerida, para mitigar ataques de volcado de memoria.		✓	✓	3.0.1

Referencias

Para obtener más información, consulte:

● Cheat Sheet - Protección de la privacidad del usuario

https://www.owasp.org/index.php/User_Privacy_Protection_Cheat_Sheet

V10: Requisitos de Verificación de Seguridad de las Comunicaciones

Objetivo de control

Se debe asegurar que la aplicación verificada satisfaga los siguientes requisitos de alto nivel:

• Que se utilice TLS donde se transmite información sensible

• Que se utilicen algoritmos y cifradores fuertes en todo momento.

Requisitos

#	Descripción	1	2	3	Desde
10.1	Verificar que puede construirse la cadena de confianza desde una CA (Autoridad de Certificación) para cada certificado TLS (Transport Layer Security) del servidor, y que cada certificado del servidor sea válido.	✓	✓	✓	1.0
10.3	Verificar que se utiliza TLS para todas las conexiones (incluyendo conexiones back-end y externas) autenticadas o que involucran funciones o información sensible, y no recaigan en protocolos inseguros o sin cifrado. Asegúrese de que la alternativa más fuerte es el algoritmo preferido.	✓	✓	✓	3.0
10.4	Verificar que se registran los fallos de conexiones TLS en el backend.			✓	1.0
10.5	Verificar que se construyen las cadenas de confianza para todos los certificados de clientes mediante anclajes de confianza e información de revocación de certificados.			✓	1.0
10.6	Verificar que todas las conexiones a sistemas externos que involucran acciones o información sensible sean autenticadas.		✓	✓	1.0
10.8	Verificar que haya una sola implementación estándar de TLS utilizada por la aplicación la cual esté configurada para operar en un modo aprobado de operación.			✓	1.0
10.10	Verificar que el certificado de clave pública se encuentre fijado (Certificate Pinning) con la clave de producción y la clave pública de respaldo. Para obtener más información, vea las referencias abajo.			✓	3.0.1
10.11	Verificar que los encabezados HTTP Strict Transport Security sean incluidos en todas las peticiones y para todos los subdominios, como Strict-Transport-Security: max-age = 15724800; includeSubdomains	✓	✓	✓	3.0

#	Descripción	1	2	3	Desde
10.12	Verificar que la URL del sitio web de producción haya sido enviada a una lista precargada de dominios de Strict Transport Security(STS) mantenidos por proveedores de navegadores web. Para obtener más información, vea las referencias abajo.			✓	3.0
10.13	Asegurar que *foward secrecy* se esté utilizando para mitigar que atacantes pasivos puedan grabar el tráfico.	✓	✓	✓	3.0
V10.14	Verificar que una adecuada revocación de certificados, tal como el protocolo de estatus de certificado en línea (OSCP), está habilitado y configurado para determinar el estado de vigencia del certificado.	✓	✓	✓	3.0
V10.15	Verificar que se utilicen únicamente algoritmos, cifradores y protocolos fuertes, a través de toda la cadena de confianza, incluyendo certificados raíz y certificados intermediarios de la autoridad certificadora seleccionada.	✓	✓	✓	3.0
V10.16	Verificar que la configuración de TLS esté en línea con las mejores prácticas actuales, particularmente debido a que configuraciones comunes se convierten en inseguras a medida que transcurre el tiempo.	✓	✓	✓	3.0

Referencias

Para obtener más información, consulte:

• Cheat Sheet: TLS

https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet

• Notas sobre "Modos aprobados de TLS": En el pasado, el ASVS hizo referencia al estándar estadounidense FIPS 140-2, pero como es un estándar global, la aplicación de estándares americanos puede resultar difícil, contradictorio o confuso de aplicar.

Un mejor método de cumplimiento para el punto 10.8 es revisar guías tales como

(https://wiki.mozilla.org/Security/Server_Side_TLS), generar configuraciones bien conocidas (https://mozilla.github.io/server-side-tls/ssl-config-generator/) y utilizar herramientas de evaluación de TLS conocidas, como sslyze, diversos escáneres de vulnerabilidades o servicios confiables de evaluación en línea de TLS para obtener un nivel de seguridad deseado. En general, vemos el incumplimiento de esta sección debido al uso de cifradores anticuados, algoritmos inseguros, la falta de perfect secret fowarcy, protocolos de SSL obsoletos o inseguros, algoritmos de Cifrado débiles y así sucesivamente.

• Fijación de Certificado: Por más información consulte

https://tools.ietf.org/html/rfc7469. La razón de ser tras el fijado de certificados para producción y copia de claves es la continuidad del negocio - vea

https://noncombatant.org/2015/05/01/about-http-public-key-pinning/

• Pre-Cargamiento de HTTP Transporte de Seguridad Estricto:

https://www.Chromium.org/hsts

V11: Requisitos de verificación de configuración de seguridad HTTP

Objetivo de control

Asegure que la aplicación verificada satisfaga los siguientes requisitos de alto nivel:

• El servidor de aplicaciones está convenientemente endurecido de una configuración preestablecida

• Toda respuesta HTTP contiene su tipo de contenido establecido utilizando un conjunto de caracteres seguro.

Requisitos

#	Descripción	1	2	3	Desde
11.1	Verificar que la aplicación acepte solo un conjunto definido de métodos de solicitud HTTP y que son necesarios, como GET y POST, y métodos no utilizados (por ejemplo: TRACE, PUT y DELETE) se encuentran explícitamente bloqueados.	✓	✓	✓	1.0
11.2	Verificar que cada respuesta HTTP contenga una cabecera content-type en la que se especifique un conjunto utilizando un conjunto de caracteres seguros (Ejemplo: UTF-8, ISO 8859-1).	✓	✓	✓	1.0
11.3	Verificar que los encabezados HTTP agregados por un proxy confiable o dispositivos SSO, tales como un token de portador (bearer), son autenticados por la aplicación.		✓	✓	2.0
11.4	Verificar que el cabezal X-FRAME-OPTIONS se encuentra especificado para los sitios que no deben ser embebidos en X-Frame en sitios de terceros		✓	✓	3.0.1
11.5	Verificar que los encabezados HTTP o cualquier parte de la respuesta HTTP no expongan información detallada de la versión de los componentes del sistema.	✓	✓	✓	2.0
11.6	Verificar que todas las respuestas del API contienen opciones X-Content-Type: nosniff y Content-Disposition: attachment; filename="api.json" (u otro nombre de archivo apropiado para el tipo de contenido).	✓	✓	✓	3.0

11.7	Verificar que la política de seguridad de contenido (CSPv2) está en uso de tal manera que ayude a mitigar vulnerabilidades de inyección comunes de DOM, XSS, JSON y Javascript	✓	✓	✓	3.0.1
11.8	Verificar que el encabezado "X-XSS-Protection: 1; mode=block" esté presente para habilitar a los navegadores a filtrar XSS reflejados	✓	✓	✓	3.0

Referencias

Para obtener más información, consulte:

• Guía de pruebas OWASP 4.0: Testeo para la manipulación de verbos HTTP

https://www.owasp.org/index.php/Testing_for_HTTP_Verb_Tampering_%28OTGINPVAL-003%29

• Adición de Content-Disposition a las respuestas API ayuda a prevenir muchos de los ataques basados en errores o malinterpretaciones en el tipo MIME entre cliente y servidor, y la opción de "nombre de archivo" específicamente ayuda a prevenir ataques de tipo Descarga de Archivos Reflejada.

https://www.blackhat.com/docs/eu-14/materials/eu-14-Hafif-Reflected-FileDownload-A-New-Web-Attack-Vector.pdf

V12: Requisitos de verificación de configuración de seguridad

Esta sección se incorporó en V11 en la versión 2.0 del Estándar de Verificación de Seguridad en Aplicaciones.

V13: Requisitos de verificación para Controles Malicioso

Objetivo de control

Asegure que la aplicación verificada satisfaga los siguientes requisitos de alto nivel:

• La actividad maliciosa se debe manejar con seguridad y adecuadamente para no afectar el resto de la aplicación.

• No posee bombas de tiempo ni otros ataques basados en tiempo

• No realiza "phone home" a destinos malintencionados o no autorizados

• La aplicación no posee puertas traseras, huevos de Pascua, ataques salami o fallos de lógica que pueden ser controlados por un atacante

El código malicioso es extremadamente raro difícil de detectar. La revisión manual línea por línea del código puede ayudar a encontrar bombas lógicas, pero incluso el más experimentado revisor de código tendrá que esforzarse para encontrar código malicioso aunque sepa que existe.

Requisitos

#	Descripción	1	2	3	Desde
13.1	Verificar que toda actividad maliciosa sea adecuadamente aislada o encajonada para retrasar y disuadir a los atacantes de atacar a otras aplicaciones.			✓	2.0
13.2	Verificar que el código fuente de la aplicación y tantas bibliotecas de terceros como sean posibles, no poseen puertas traseras, huevos de pascua, o fallas de lógica en la autenticación, control de acceso, validaciones de entrada y lógica de negocio en transacciones de alto valor.			✓	3.0.1

Referencias

Para obtener más información, consulte:

• http://www.dwheeler.com/essays/apple-goto-fail.html

V14: Requisitos de verificación de seguridad interna

Esta sección se incorporó en V13 en la versión 2.0 del Estándar de Verificación de Seguridad en Aplicaciones.

V15: Requisitos de verificación para lógica de negocios

Objetivo de control

Asegure que la aplicación verificada satisfaga los siguientes requisitos de alto nivel:

• El flujo de la lógica de negocio es secuencial y en orden

• La Lógica de negocios incluye límites para detectar y evitar ataques automatizados, como las continuas transferencias de fondos pequeños, agregando 1 millón amigos uno a uno y así sucesivamente.

• Flujos de lógica de negocios de alto valor han considerado casos de abuso y agentes maliciosos y poseen protecciones contra la falsificación, alteración, repudio, revelación de información y ataques a la elevación de privilegios.

Requisitos.

#	Descripción	1	2	3	Desde
V15.1	Verificar que la aplicación sólo procese flujos lógicos de negocios en orden secuencial, con todos los pasos procesados en tiempo humano realista, y no procesados fuera de orden, con pasos salteados, con pasos del proceso de otro usuario, o de transacciones muy rápidamente enviadas.		✓	✓	2.0
V15.2	Verificar que la aplicación tiene límites de negocio y los aplique correctamente por cada usuario, con alertas configurables y reacciones automatizadas ante ataques inusuales o automáticos.		✓	✓	2.0

Referencias

Para obtener más información, consulte:

• Guía de pruebas OWASP 4.0: Pruebas de lógica de negocios

https://www.OWASP.org/index.php/Testing_for_business_logic

• Cheat Sheet: Lógica de Negocio

https://www.OWASP.org/index.php/Business_Logic_Security_Cheat_Sheet

V16: Requisitos de verificación de archivos y recursos

Objetivo de control

Asegure que la aplicación verificada satisfaga los siguientes requisitos de alto nivel:

• Datos no confiables deben ser gestionados como tales y de forma segura

• Datos Obtenidos de fuentes no confiables sean almacenan fuera del webroot y posean permisos limitados.

Requisitos

#	Descripción	1	2	3	Desde
16.1	Verificar que las URL de redireccionen y reenvíen sólo a destinos clasificados en la lista blanca, o mostrar una advertencia cuando se redirija a contenido potencialmente no confiable.	✓	✓	✓	2.0
16.2	Verificar que archivos no confiables enviados a la aplicación no sean utilizados directamente por comandos de I/O (Entrada/Salida) de archivos, especialmente para proteger contra manipulaciones de rutas, archivo local incluido, manipulación de tipo mime y vulnerabilidades de inyección de comandos de sistema operativo.	✓	✓	✓	2.0
16.3	Verificar que los archivos procedentes de fuentes no confiables sean validados para ser del tipo del cual se espera y sean analizados por escáneres antivirus para evitar la carga de contenido malicioso conocido.	✓	✓	✓	2.0
16.4	Verificar que datos no confiables no se utilicen en funcionalidades de reflexión, cargado de clases o inserción para prevenir vulnerabilidades de inclusión de archivos remotos/locales.	✓	✓	✓	2.0
16.5	Verificar que datos no confiables no se utilicen en recursos de dominios compartidos (CORS) para proteger contra el contenido remoto arbitrario.	✓	✓	✓	2.0
16.6	Verificar que los archivos obtenidos de fuentes no confiables se almacenen fuera del webroot, con permisos limitados, preferiblemente con una fuerte validación.		✓	✓	3.0

#	Descripción	1	2	3	Desde
16.7	Verificar que el servidor web o de aplicación se encuentra configurado por defecto para negar el acceso a recursos remotos o sistemas fuera del servidor web o de aplicación.		✓	✓	2.0
16.8	Verificar que el código de la aplicación no ejecuta datos cargados obtenidos de fuentes no confiables.	✓	✓	✓	3.0
16.9	Verificar que no utiliza Flash, Active-X, Silverlight, NACL, Java del lado del cliente u otras tecnologías del lado del cliente que no sean soportadas de forma nativa a través de los estándares de navegador W3C.	✓	✓	✓	2.0

Referencias

Para obtener más información, consulte:

• Manejo de Extensión de Archivo para información confidencial:

https://www.owasp.org/index.php/Unrestricted_File_Upload

V17: Requisitos de verificación Móvil

Objetivo de control

Esta sección contiene controles específicos para aplicaciones móviles. Estos controles han sido de-duplicados de la versión 2.0, por lo que deben tomarse en conjunto con el resto de las secciones de los niveles correspondientes de Verificación ASVS.

Las aplicaciones móviles deben:

• Deben tener el mismo nivel de controles de seguridad tanto en el cliente móvil como en el servidor, mediante la aplicación de controles de seguridad en un entorno de confianza.

• Activos de Información sensible almacenados en el dispositivo debe realizarse de un modo seguro.

• Todos los datos sensibles transmitidos desde el dispositivo deben ser hechos teniendo en mente la seguridad en la capa de transporte.

Requisitos

#	Descripción	1	2	3	Desde
17.1	Verificar que los valores de identificadores almacenados en el dispositivo y recuperables por otras aplicaciones, como el número de UDID o IMEI no se utilicen como tokens de autenticación.	✓	✓	✓	2.0
17.2	Verificar que la aplicación móvil no almacene datos sensibles en recursos compartidos potencialmente no cifrados en el dispositivo (tarjeta SD o carpetas compartidas).	✓	✓	✓	2.0
17.3	Verificar que los datos sensibles no se almacenen sin protección en el dispositivo, incluso en áreas protegidas del sistema como llaveros.	✓	✓	✓	2.0
17.4	Verificar que las contraseñas, claves secretas y tokens de APIs se generan dinámicamente en la aplicación móvil.		✓	✓	2.0

#	Descripción	1	2	3	Desde
17.5	Verificar que la aplicación móvil evite fugas de información sensible (por ejemplo, capturas de pantalla de la aplicación actual sean guardadas mientras la aplicación está en segundo plano o escribiendo información sensible en consola).		✓	✓	2.0
17.6	Verificar que la aplicación solicita permisos mínimos para la funcionalidad y recursos requeridos.		✓	✓	2.0
17.7	Verificar que el código sensible de la aplicación sea cargado de forma no predecible en memoria (utilizando ASLR por ejemplo).	✓	✓	✓	2.0
17.8	Verificar que se encuentren presentes técnicas anti depuración suficientes para impedir o retrasar a posibles atacantes de inyectar depuradores en la aplicación móvil (GDB, por ejemplo).			✓	2.0
17.9	Verificar que la aplicación no exporte actividades intents, o proveedores de contenido con información sensible a otras aplicaciones móviles posibles de ser explotados por otras aplicaciones en el mismo dispositivo.	✓	✓	✓	2.0
17.10	Verificar que la información sensible almacenada en memoria es sobreescrita con ceros tan pronto como no deje de ser requerida, con el fin de mitigar ataques de volcado de memoria.			✓	3.0.1
17.11	Verificar que las actividades expuestas, intents, proveedores de contenido realicen validaciones de los datos de entrada.	✓	✓	✓	3.0.1

Referencias

Para obtener más información, consulte:

• Proyecto OWASP de Seguridad Móvil:

https://www.OWASP.org/index.php/OWASP_Mobile_Security_Project

• iOS Developer Cheat Sheet:

https://www.OWASP.org/index.php/IOS_Developer_Cheat_Sheet

V18: Requisitos de verificación de servicios Web

Objetivo de control

Asegúrese de que la aplicación verificada, de utilizar servicios web REST o SOAP posean:

• Autenticación adecuada, gestión de sesión y autorización de todos los servicios web

• Validación de entrada de datos de todos los parámetros que transiten de zonas de menor a mayor confianza

• Interoperabilidad básica de la capa de servicios web SOAP para promover el uso de la API.

Requisitos

#	Descripción	1	2	3	Desde
18.1	Verificar que el mismo estilo de codificación se utiliza tanto en el cliente como el servidor.	✓	✓	✓	3.0
18.2	Verificar que el acceso a las funciones de administración y gestión de la aplicación proveedora de servicios web sea limitado a los administradores.	✓	✓	✓	3.0
18.3	Verificar que existen esquemas XML o JSON y que éstos son verificados por la aplicación antes de aceptar datos de entrada.	✓	✓	✓	3.0
18.4	Verificar que todos los datos de entrada se encuentren limitados a un tamaño adecuado.	✓	✓	✓	3.0
18.5	Verificar que los servicios web basados en SOAP son compatibles con el perfil básico de interoperabilidad de servicios Web (WS-I) como mínimo. Esencialmente, eso implica compatibilidad con cifrado TLS.	✓	✓	✓	3.0.1
18.6	Verificar el uso de autenticación y autorización basada en sesiones. Por favor refiérase a las secciones 2, 3 y 4 para mayor orientación. Evite el uso de "claves de API" estáticas y enfoques similares.	✓	✓	✓	3.0

#	Descripción	1	2	3	Desde
18.7	Verificar que los servicios REST se encuentren protegidos de Falsificación de Peticiones en Sitos Cruzados (CSRF), mediante el uso de al menos uno o mas de los siguientes mecanismos: Verificaciones de ORIGIN, CSRF nonces, verificaciones de referrer o el envío doble de valores en cookie y en el servicio (double submit cookie pattern)	✓	✓	✓	3.0.1
18.8	Verificar que los servicios REST comprueben explícitamente que el Content-Type entrante sea el que se espera, como aplicación/xml o aplicación/json.		✓	✓	3.0
18.9	Verificar que el contenido de los mensajes se encuentra firmado para asegurar el transporte confiable entre el cliente y el servicio, utilizando JSON Web Signing o WS-Security para servicios SOAP.		✓	✓	3.0.1
18.10	Verificar que no existen rutas de acceso alternativas y menos seguras.		✓	✓	3.0

Referencias

Para obtener más información, consulte:

• Guía de pruebas de OWASP 4.0: Configuración y Despliegue

https://www.owasp.org/index.php/Testing_for_configuration_management

• Cheat Sheet: Falsificación de Peticiones en Sitos Cruzados

https://www.owasp.org/index.php/CrossSite_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet

• JSON Web Tokens (y su firma)

https://jwt.io/

V 19. Requisitos de Configuración

Objetivo de control

Asegúrese de que la aplicación verificada:

• Utilice bibliotecas y una plataforma actualizada.

• Una configuración segura por omisión.

• Un Hardening suficiente de tal forma que los cambios realizados por un usuario no resulten en exposiciones innecesarias o creen debilidades de seguridad o fallas a los sistemas subyacentes.

Requisitos

#	Descripción	1	2	3	Desde
19.1	Todos los componentes deben estar actualizados a las configuraciones y versiones de seguridad adecuadas. Esto debería incluir la eliminación de configuraciones y carpetas innecesarias como aplicaciones de ejemplo, documentación de plataforma y usuarios pre-establecidos o de ejemplo.	✓	✓	✓	3.0
19.2	Las comunicaciones entre componentes, tales como entre el servidor de aplicaciones y el servidor de base de datos, deberían ser cifradas, particularmente cuando los componentes están en diferentes contenedores o en sistemas diferentes.		✓	✓	3.0
19.3	Las comunicaciones entre componentes, tales como entre el servidor de aplicaciones y el servidor de base de datos deberían autenticarse utilizando una cuenta con los mínimos privilegios necesarios.		✓	✓	3.0
19.4	Verificar que los despliegues de la aplicación se encuentren dentro de Sandboxes, en contenedores o aislados para retrasar y disuadir a los atacantes de atacar a otras aplicaciones.		✓	✓	3.0
19.5	Verificar que los procesos de compilación y despliegue de la aplicación se realizan de forma segura.		✓	✓	3.0

#	Descripción	1	2	3	Desde
19.6	Verificar que los administradores autorizados posean la capacidad de verificar la integridad de todas las configuraciones de seguridad pertinentes para garantizar que no hayan sido manipuladas.			✓	3.0
19.7	Verificar que todos los componentes de aplicación se encuentren firmados.			✓	3.0
19.8	Verificar que los componentes de terceros proceden de repositorios de confianza.			✓	3.0
19.9	Verificar que los procesos de compilación para los lenguajes de nivel de sistema operativo tengan todas las banderas de seguridad activas, tales como controles de seguridad, DEP y ASLR.			✓	3.0
19.10	Verificar que todos los recursos de la aplicación se encuentran alojados en la aplicación en vez de confiar en un CDN o proveedores externos, tales como bibliotecas JavaScript, estilos CSS o web fonts			✓	3.0.1

Referencias

Para obtener más información, consulte:

• Guía de pruebas de OWASP 4.0: Configuración y Despliegue

https://www.owasp.org/index.php/Testing_for_configuration_management

SERIES DE LIDERAZGO DE SEGURIDAD: Estrategias de seguridad para el éxito.

LA SEGURIDAD NUNCA HA SIDO TAN DESAFIANTE. Tendencias como la movilidad, BYOD y la informática en la nube significa que más gente accede a la información empresarial confidencial desde más lugares y de más formas que nunca.

Para TI, el reto es proteger esta información de su pérdida, robo y de amenazas cada vez más sofisticadas mientras cumple con los requisitos de privacidad, cumplimiento normativo y mandatos en cuanto a la gestión de riesgos. Las estrategias de seguridad sólidas deben incluir políticas inteligentes, su aplicación rigurosa y un profundo seguimiento y presentación de informes, además de proporcionar a la gente el nivel de acceso a los recursos de la empresa que necesitan para ser productivos y hacer su trabajo.

Citrix, líder reconocido por sus contribuciones al avance de la seguridad de la información, puede ayudarle a proteger proactivamente la información, gestionar el riesgo y lograr el cumplimiento normativo y simplifica la capacidad de TI para administrar entornos cada vez más complejos, híbridos y de múltiples nubes.

Complementado por socios de seguridad líderes del sector, Citrix ofrece soluciones de seguridad holísticas para ayudarle a enfrentarse a las crecientes amenazas contra la seguridad informática de hoy, mientras le prepara para futuras necesidades.

Para los responsables de TI y seguridad es imprescindible leer estas estrategias de seguridad para el éxito. Empiece hoy mismo.

5 PASOS PARA CONTROLAR APLICACIONES Y DATOS.

Su reto es asegurar un entorno empresarial transformado por las complejidades de la informática en la nube y los nuevos requisitos de movilidad de la plantilla. Cómo hacerlo.

La revolución digital ha transformado las operaciones y modelos empresariales en muchas maneras positivas, y está ofreciendo beneficios que van desde un servicio de atención al cliente mejorado para una mayor productividad hasta nuevas fuentes de ingresos. Pero la transformación del negocio digital también ha presentado nuevas oportunidades para hackers, cibercriminales, y otras malas personas. Los modelos cambiantes de la informática y las redes lo complican aún más.

En el pasado, las corporaciones rutinariamente mantenían sus sistemas y datos más confidenciales asegurados en sus centros de datos centrales y los portátiles administrados por la empresa. Sin embargo, hoy en día, los datos y aplicaciones suelen residir en dispositivos móviles dentro de soluciones establecidas en el departamento, o en servidores basados en la nube. Las herramientas y métodos tradicionales para asegurar las aplicaciones y los datos han demostrado ser insuficientes para abordar adecuadamente las complejidades inherentes a los diversos negocios actuales y el panorama de amenazas. Las organizaciones, en particular las de sectores altamente regulados, necesitan administrar y mitigar los riesgos cibernéticos de forma que protejan los datos en reposo, en uso y en tránsito. Además, deben cumplir estos objetivos incluso cuando su comunidad de “usuarios” incluye a los empleados móviles, remotos; consultores de terceros; externalización; y otros socios comerciales.

1. Centrarse en el equilibrio entre las necesidades de seguridad y de la experiencia de usuario.

   Cuando las aplicaciones y los datos sensibles están amenazados, la seguridad debe prevalecer sobre la facilidad de acceso y facilidad de uso. Dicho esto, las organizaciones de éxito toman una visión holística de la seguridad que se esfuerza en implementar controles de seguridad no obstructiva y práctica que no frustrarán

innecesariamente a los usuarios ni dificultarán su productividad. Afortunadamente, algunas de las defensas de seguridad más efectivas son transparentes y fluidas para los usuarios finales.

2. Habilitar opciones flexibles de almacenamiento de datos, acceso y gestión.

Las empresas pueden beneficiarse considerablemente de tener una plantilla que es móvil o ampliamente dispersa.

Inevitablemente, sin embargo, usuarios, dispositivos y sistemas dispersos e interconectados proporcionan más objetivos a los atacantes cibernéticos. Las empresas necesitan diseñar e implementar estrategias de gestión de datos en consonancia con el valor y la confidencialidad de los datos en riesgo.

3. Ofrezca un poderoso motor de políticas para controles contextuales.

En lugar de dar a los usuarios pases de acceso total a sus datos, aplicaciones y redes, debe implementar controles que puedan considerar el contexto de cada solicitud de acceso. Con estos controles, los administradores de TI pueden establecer políticas que determinen los títulos y departamentos de la gente, sus ubicaciones, la seguridad de las redes que están usando, las capacidades de sus terminales, e incluso variables tales como la hora del día en que intentan acceder a los datos.

4. Permitir una eficiente gestión del cumplimiento normativo y presentación de informes.

A nivel mundial, las organizaciones se enfrentan a más de 300 regulaciones y leyes relacionadas con los niveles mínimos de privacidad y seguridad, con más de 3500 controles específicos en la actualidad. Para garantizar el cumplimiento y satisfacer las

demandas de auditoría, las soluciones de seguridad deben proporcionar una supervisión completa y automatizada, registro e informes de acceso a datos, movimiento de datos y actividades a nivel de red. Es importante que las soluciones sean lo suficientemente flexibles para adaptarse fácilmente a las nuevas regulaciones y estándares a medida que emergen.

5. Reducir la superficie de ataque mientras bajan los costes de TI**.**

Controlando la distribución de datos y proporcionando acceso contextual, las organizaciones pueden reducir significativamente sus superficies de ataque. Estas protecciones deben incluir el uso rutinario del cifrado de las aplicaciones y datos en reposo, en uso, o en tránsito. A su vez, con menos objetivos expuestos a proteger, las empresas pueden reducir sus costes operativos ahorrándose compras de tecnologías de seguridad centradas en dispositivos individuales.

5 MEJORES PRÁCTICAS PARA HACER DE LA SEGURIDAD UN ASUNTO DE TODOS.

Los empleados son uno de los mayores riesgos de la seguridad de la información. Utilice estas cinco técnicas probadas para fortalecer su estrategia de seguridad y proteger su negocio.

Amenazadas por una variedad cada vez mayor de potentes amenazas, los empleados móviles de hoy son los participantes de primera línea en la lucha por asegurar la empresa. Así que mientras que las sólidas estrategias de seguridad deben incluir políticas inteligentes, la aplicación rigurosa y un profundo seguimiento/creación de informes, también deben reflejar las necesidades y los hábitos de los usuarios de la empresa.

Los usuarios finales son en última instancia, donde la seguridad tiene éxito o fracasados, dice Kurdo Remero, estratega jefe de seguridad de Citrix.

Por desgracia, mantener a los empleados seguros y satisfechos no es fácil. Los empleados quieren acceso a la información en cualquier lugar, en cualquier momento y desde cualquier dispositivo sin engorrosas protecciones de seguridad que les retrasen. Los responsables de negocio quieren salvaguardar la información importante sin inhibir el crecimiento, la innovación y la competitividad. Los departamentos de TI quieren mantener productivos a todos aunque reconocen que los empleados y sus dispositivos son a menudo los eslabones débiles en la cadena de seguridad.

1. Educar a los usuarios.

   Una plantilla laboral informada, consciente de la seguridad es la primera línea de defensa de cada empresa contra amenazas a la seguridad, por lo tanto enseñar a la gente cómo trabajar de forma segura desde cualquier lugar en cualquier dispositivo debe ser una prioridad.

   Enseñar las mejores prácticas es una buena receta contra el fracaso. Luego explíqueles las políticas de seguridad de su empresa en términos que sean fácilmente comprensibles y relevantes a su rol.

   “La relevancia es clave”, dice Roemer. También debería ser personal, añade Stan Black, director de seguridad de Citrix. Por ejemplo, además de la formación relacionada con la seguridad en el trabajo, Citrix proporciona a sus empleados asesoramiento sobre temas tales como asegurar una red inalámbrica doméstica y ayudar a sus hijos a utilizar Internet de forma segura.

   “Tratamos de unir todos los esfuerzos de formación para el ciclo de vida completo de la seguridad, no solo para lo que la gente hace en la oficina”, dice Black.

2. Compromiso con las líneas de negocio de las organizaciones.

Las estrechas relaciones laborales entre los ejecutivos de TI y los responsables de las líneas de negocio son un ingrediente esencial para una seguridad efectiva. Reunirse regularmente con los responsables de la toma de decisiones empresariales permite a los responsables de seguridad incorporar salvaguardias adecuadas a nuevas iniciativas empresariales desde el principio. También les da una perspectiva cercana e indispensable sobre los riesgos y los requisitos únicos de un grupo empresarial.

"Usted aprenderá más acerca de los procesos operativos y los peligros potenciales de los que nunca sabría de lo contrario", dice Black. "Después de eso, puede incorporar estos conocimientos a su planes de seguridad y hacerlos aún más ricos"

3. Vea las políticas de seguridad de forma moderna y móvil.

Tan importante como es, la formación por si sola no garantiza una seguridad fuerte. Muchos de los dispositivos, redes y sistemas de almacenamiento en los que los empleados confían hoy en día están fuera del control de TI.

"TI tiene que actualizar las políticas de seguridad tradicionales a la nueva realidad móvil y de servicios en la nube", observa Roemer.

La mayoría de las empresas adopta políticas graduales que protegen la información confidencial con más cuidado que la información pública y proporcionan menos acceso desde dispositivos BYOD de consumo que desde dispositivos intencionadamente "bloqueados" de tipo empresarial.

4. Aplique las políticas de forma apropiada y constantemente.

Las políticas de seguridad pueden perder valor con el tiempo si los usuarios no creen que el violarlas tiene consecuencias, o peor aún, si creen que saltándoselas mejora la productividad. Las políticas deben ser mantenidas y actualizadas con el negocio. Los responsables de seguridad por lo tanto deben hacer cumplir las políticas de manera apropiada y consistentemente.

“Cuando las políticas se desarrollan en colaboración a través de la compañía, y la conciencia de la seguridad está tejida en la cultura, las violaciones de seguridad no son frecuentes”, dice Black.

5. Automatizar la seguridad correctamente.

Para reducir aún más las violaciones de las políticas, utilice el software de seguridad para automatizar la aplicación de las mismas. Por ejemplo, muchas soluciones de seguridad pueden implementar comportamientos deseados tales como cifrado de datos del negocio en los dispositivos móviles de forma predeterminada. Pueden también construir una seguridad más estricta en los elementos fundamentales de la experiencia del usuario evitando automáticamente que los empleados utilicen aplicaciones no autorizadas sobre la red de la empresa o limitando qué aplicaciones pueden utilizar para archivos adjuntos de correo electrónico, por ejemplo.

Aun así, el software es solo una pieza del rompecabezas de la seguridad.

“Para proteger realmente la empresa tiene que conocer sus grupos de líneas de negocio y a sus usuarios finales”, dice Roemer.

En definitiva, las mejores estrategias de seguridad son tanto la gente como la tecnología.

3 ESTRATEGIAS PARA ADMINISTRAR LOS MANDATOS DEL CUMPLIMIENTO NORMATIVO.

Cumplir con los requisitos del cumplimiento normativo relacionados con la seguridad es un trabajo cada vez más complejo. Céntrese en estas tres estrategias para gestionar fácilmente el cumplimiento normativo.

He aquí una buena noticia para los responsables de seguridad: Si ha establecido sólidas políticas, hágalas cumplir rigurosamente, y haga un seguimiento a fondo y un informe de la eficacia de la seguridad, y estará en el buen camino de proteger a su empresa de la cantidad creciente de potentes amenazas. Ahora la mala noticia: Cada vez más auditores, reguladores, partners, y clientes están exigiendo pruebas defendibles de ese hecho. "A nivel mundial, hay más de 300 estándares de seguridad relacionados con las normas de la privacidad, reglamentos y leyes con más de 3500 controles específicos, y muchos más que vienen", dice Stan Black, director de seguridad en Citrix.

"La gente responsable de esas reglas quiere pruebas de que está cumpliendo las normas". Las consecuencias por decepcionar a auditores y reguladores pueden ser graves. No cumplir con la constante expansión de requisitos relacionados con la seguridad puede resultar en multas y sanciones, clientes indignados, pérdida de datos confidenciales, creciente indagación por parte de los reguladores y costosos daños a la marca y reputación de su organización.

No es de extrañar, entonces, que el cumplimiento normativo se haya convertido en un tema de intenso interés para altos ejecutivos y miembros del comité de dirección.

1. Permita el acceso al mismo tiempo que protege la información.

   Adoptar un planteamiento integral para la gestión de la identidad y el acceso, combinado con un profundo enfoque en los datos confidenciales e informes relevantes y métricas es un importante equilibrio. Las políticas deberían especificar los privilegios del acceso elemental a los datos dependiendo de dónde se encuentran los empleados, en

qué red están y qué dispositivo están usando, con controles adicionales acordes con el riesgo. La función es una variable importante. «Se debe conceder acceso solo a las personas que tienen necesidad debido a su función», recomienda Kurt Roemer, director de estrategia de seguridad de Citrix. La formación específica según la función y el control de acceso automatizado según la función asegurará que los empleados entiendan las políticas y las sigan.

Usted debe hacer cumplir sus políticas diligentemente con la ayuda de una arquitectura de seguridad robusta. Por ejemplo, las medidas de seguridad enfocadas a los datos ayudan a proteger los datos «en tránsito» a través de redes privadas y públicas, y «en reposo» en almacenes basados en la nube o en la oficina, y «en uso» en los dispositivos del usuario final.

2. Controlar la información confidencial

La mayor parte de mandatos de seguridad se aplican principalmente a información personalmente identificable, archivos médicos, transacciones de pago y otros datos secretos. Para cumplir con estos mandatos, debe identificar primero los datos confidenciales creando un modelo de clasificación para las distintas clases de información que su la compañía crea, transmite, y almacena.

Después, analice la clasificación de datos y asigne prioridades. Para asegurar que los datos correctos terminan en las categorías correctas, implique una amplia representación de accionistas en este proceso, incluso representantes de sus grupos de negocio, departamento legal y funciones operacionales.

Por ejemplo, usted puede elegir un control mínimo de datos públicos independientemente del usuario, red y dispositivo, pero limitar el acceso a la información confidencial en hardware «BYO» y de consumo. Aplique siempre los controles más estrictos a sus datos más confidenciales.

«Tiene sentido negar el acceso a los datos confidenciales en los dispositivos y redes que no pueden ser verificados y asegurados adecuadamente», dice Roemer.

3. Auditar, medir y demostrar el cumplimiento de la normativa.

   Los informes de seguridad integral son siempre importantes, pero son cruciales cuando se trata del cumplimiento normativo.

   “Los auditores y otros quieren ver pruebas claras de que se hizo lo que usted dijo que haría”, dice Black

   Satisfacer esas demandas lleva un registro de conexión sistemático, informes y rigurosos procesos de auditoría suficientes para seguir cuando determinados usuarios acceden a aplicaciones y datos específicos, y son lo suficientemente flexibles para abordar nuevas regulaciones y estándares según aparecen. «De lo contrario usted podrá sumergirse entre hojas de cálculo desfasadas antes de que nadie las vea», apunta Black.

   Si una auditoría descubre deficiencias en sus medidas de cumplimiento normativo, lleve a cabo un planteamiento integral para su resolución haciendo un seguimiento centralizado de los problemas desde su detección hasta el cierre. Trate a la gente que descubrió esos problemas como colegas mejor que como adversarios. Los auditores externos pueden proporcionar una reacción valiosa, imparcial en su régimen de cumplimiento normativo.

   Consultar con colegas es a menudo igualmente provechoso.

   Los ejecutivos en su campo pueden estar poco dispuestos a hablar libremente, pero los responsables de seguridad en otros sectores a menudo están dispuestos a intercambiar opiniones útiles si todo el mundo está de acuerdo de antemano en la no divulgación de las mismas.

La planeación y evaluación de los procesos productivos.

Dos conceptos son importantes en la planeación y evaluación de los procesos productivos: el COSTO de los insumos y materia prima al realizar el producto y el BENEFICIO que se obtendrá al vender este producto. Por ello es necesario comprar insumos de buena calidad para que nuestro producto sea adquirido por la gente y así obtengamos un beneficio que en nuestro caso serán las ganancias generadas por las ventas. Si compro insumos de regular o mala calidad, tendremos que vender nuestros productos a un bajo costo y por lo tanto el beneficio que obtendremos será poco .¿En que momento debemos considerar estoé conceptos?, pues en la PLANEACIÓN ya que en este momento se determinan los objetivos que pretendemos alcanzar, se diseña el proceso, se eligen los insumos, se definen las técnicas para la elaboración del producto y se genera la documentación necesaria.

La evaluación como parte de la resolución de problemas técnicos y el trabajo por proyectos en los procesos productivos.

La evaluación como parte de la resolución de problemas técnicos y el trabajo por proyectos en los procesos productivos

Cuando se requiere desarrollar una solución técnica para un problema, hay que organizar las acciones que deben efectuarse a partir de la información que se tiene del problema o la necesidad, con el propósito de evaluar las distintas soluciones técnicas que pueden aplicarse.

De esta manera, los elementos de entrada pasan a ser elementos de salida, tras un proceso en el que se incrementa su valor.

Los productos, en cambio, están destinados a la venta al consumidor o mayorista.

La evaluación en el desarrollo de los procesos de producción para mayor eficiencia.

Cuando el ciclo de desarrollo de un producto se acerca a su fin, el coste de los cambios que se hagan se incrementa. Los cambios en el diseño deberían hacerse en el principio del proceso con el fin de producir el mayor impacto y teniendo un menor efecto en la financiación. Por tanto, el proyecto debe ser sometido a evaluación tan pronto como sea sensato en el proceso de diseño. Es entonces fácil alterar los diseños del proyecto sobre la base de las pruebas.

El primer evaluador del proyecto es el diseñador mismo.

Presentar el esbozo y hacer un prototipo

El método de presentación es importante cuando los diseñadores demuestran sus propuestas para que sean evaluadas por personas que no están habituadas a las convenciones de dibujo que los diseñadores usan normalmente.

Probar los prototipos

Al lado del método de presentación, usted tendrá que considerar el ambiente donde ocurre la presentación, el método de observar el comportamiento de las personas de prueba, y el método de recolectar sus opiniones. Las pruebas pertenecientes al campo de la física se suelen hacer en laboratorios, porque tienen un equipo de medición adecuado

Puntos de vista en la evaluación

Los partes que contribuyen a menudo a la evaluación de una propuesta para producto incluyen:

1. Los usuarios futuros del producto.
2. La gente en el taller de la fabricación.
3. La división de la comercialización.
4. Los implicados y el ambiente.
5. La escuela o la asociación de diseñadores profesionales, donde el diseñador es un miembro.

Prueba de comercialización

Si el producto deberá ser producido en cantidades grandes puede ser recomendable primero probar la respuesta de los consumidores de modo que la gente tenga la opción de elegir el producto entre los rivales, pagando con su propio dinero.

Respuesta y crítica

Toda organización duradera comete a veces errores. Los errores se repetirán si no hay respuesta o reacciones sobre ellos. A largo plazo irán mejor las empresas que reconocen y satisfacen las necesidades y deseos de los clientes mejor que la competencia.

Procedimiento para el desarrollo de aplicaciones informáticas.

IDENTIFICACIÓN DEL PROCEDIMIENTO:

MACROPROCESO	PROCESO	SUBPROCESO
GESTIÓN DE DESARROLLO INSTITUCIONAL	GESTIÓN INFORMÁTICA	DESARROLLO DE APLICACIONES
PROCEDIMIENTO PARA EL DESARROLLO DE APLICACIONES		
AREA RESPONSABLE	DIRECCIÓN DE DESARROLLO DE TECNOLOGÍA	
VERSION DEL DOCUMENTO	1.0	
CÓDIGO	PRO-DDT-001	

OBJETIVO: Establecer el marco de trabajo sobre el cual deben regirse las acciones a tomar para la Gestión de Desarrollo de Aplicaciones Informáticas, a fin de incrementar la productividad de la Dirección de Desarrollo Tecnológico, respondiendo efectiva y eficientemente a las necesidades del GAD Municipal de Portoviejo.

ALCANCE: Este procedimiento tiene como alcance el desarrollo de aplicativos informáticos nuevos que conforman el componente tecnológico de los proyectos a desarrollar o las modificaciones a aplicativos ya existentes, hasta su puesta en marcha e implementación.

DEFINICIONES:

REQUERIMIENTO: Un requisito es una necesidad documentada sobre el contenido, forma o funcionalidad de un producto o servicio. Se usa en un sentido formal en la ingeniería de sistemas, ingeniería de software e ingeniería de requisitos.

DELEGADO: Experto de la Unidad Requirente.

APLICATIVO INFORMÁTICO: Es un producto de software generado como un entregable de un proyecto con componente tecnológico. Corresponde a un programa informático diseñado con el fin de permitir a un usuario final la ejecución de una tarea específica, mediante la automatización de su proceso asociado; a través del tratamiento automático de la información.

DESARROLLO INTERNO: cuando la fase de Implementación es ejecutada con recursos del GAD Municipal de Portoviejo.

DESARROLLO EXTERNO: cuando todas o parte de las sub-fases de planeación, análisis y diseño, codificación y pruebas son ejecutadas por proveedores, posterior a su contratación. Los proveedores participan también en las fases de Certificación, Puesta en Producción y Estabilización conforme a lo establecido en los contratos suscritos. En el caso del Desarrollo Externo, las bases técnicas necesarias para la contratación de los proveedores se elaboran una vez finalizadas todas las iteraciones de la fase de implementación. Para este caso cada iteración comprende únicamente las sub-fases de planeación, análisis y diseño.

ATDD: Es una práctica en la cual todo el equipo colaborativamente discute criterios de aceptación de requerimientos, con ejemplos, y luego los configura en un conjunto de pruebas de aceptación antes de que la programación comience.

BASE DE CONOCIMIENTO TÉCNICO: Es el conjunto de recursos (preguntas y respuestas, soluciones a errores conocidos, manuales, documentos técnicos u otros) relacionados con el área de conocimiento del desarrollo de software. Su objetivo principal

es proporcionar medios que permitan descubrir soluciones a problemas ya resueltos, los cuales podrían ser aplicados como base a otros problemas.

BASE TÉCNICA: Es la documentación técnica, definitiva y actualizada, a ser incluida en los pliegos de contratación. Esta comprende los estudios, requerimientos, diseños y demás especificaciones técnicas que detallen el objeto de la contratación y permitan su ejecución.

COMPLEJIDAD TÉCNICA: Es el grado de dificultad técnica para la ejecución de una tarea específica. Considera factores como el uso de nuevas plataformas tecnológicas, múltiples plataformas tecnológicas, sistemas heredados, datos heredados, integraciones, etc.

CRITERIO DE ACEPTACIÓN: Criterios y normas que deben cumplirse para lograr la aceptación del cliente final por cada requerimiento.

DOCUMENTACIÓN FORMAL: Es toda aquella documentación emitida por una Unidad Administrativa de la Institución (Dirección, Departamento o Área), la cual ha seguido un proceso formal de revisión, aprobación y difusión con la participación de todos los interesados en la misma. Cuando esta documentación especifica responsabilidades, requisitos, compromisos o de manera general cualquier disposición que involucre la participación de una Unidad de la Institución diferente a quien la haya emitido; esta documentación se considera formal únicamente cuando exista la aprobación explícita de estas.

ESTÁNDARES VIGENTES RELACIONADOS: Se refiere a los estándares relacionados al desarrollo de software, los cuales pueden ser de programación, arquitectura, diseño, control de calidad, etc.

FASE: Etapas por las cuales atraviesa el proyecto durante su ejecución.

ITERACIÓN: Una iteración se considera al período fijo de tiempo, normalmente entre 2 y 4 semanas, durante el cual se ejecutan las sub-fases de planeación, análisis, diseño, codificación y pruebas de un conjunto de requerimientos.

MANUAL TÉCNICO: Es un documento que contiene información técnica del aplicativo informático. Incluye como mínimo el modelo de clases/diagrama entidad relación/diagrama de componentes, y otra información relevante para su mantenimiento.

PROCESOS INSTITUCIONALES ESTANDARIZADOS: Un proceso constituye un conjunto de actividades con entradas (insumos) y salidas (entregables, resultados) que permiten obtener un producto o servicio. Un proceso se lo considera estandarizado cuando cumple con todas las fases de intervención (diseño, construcción, implementación, cierre) y ha pasado por un proceso de evaluación del cumplimiento de las actividades establecidas en el mismo.

REQUERIMIENTO DE USUARIO: Conjunto de necesidades funcionales y no funcionales que un aplicativo informático debe cumplir.

RESOLUCIONES: Disposiciones legales emitidas por el SRI u otro organismo

REVISIÓN CRUZADA: Procedimiento mediante el cual se ejecuta la revisión de un entregable o del resultado de una actividad con el fin de comprobar que este cumpla ciertas características o especificaciones de calidad previamente definidas. Para ello, un revisor (un recurso diferente a quien elabora dicho entregable o actividad) identifica errores o carencias en el mismo y sugiere la inclusión de mejoras o cambios.

PROCEDIMIENTOS

Procedimiento para solicitud de cambios, mejoras o nuevo desarrollo de un aplicativo informático.

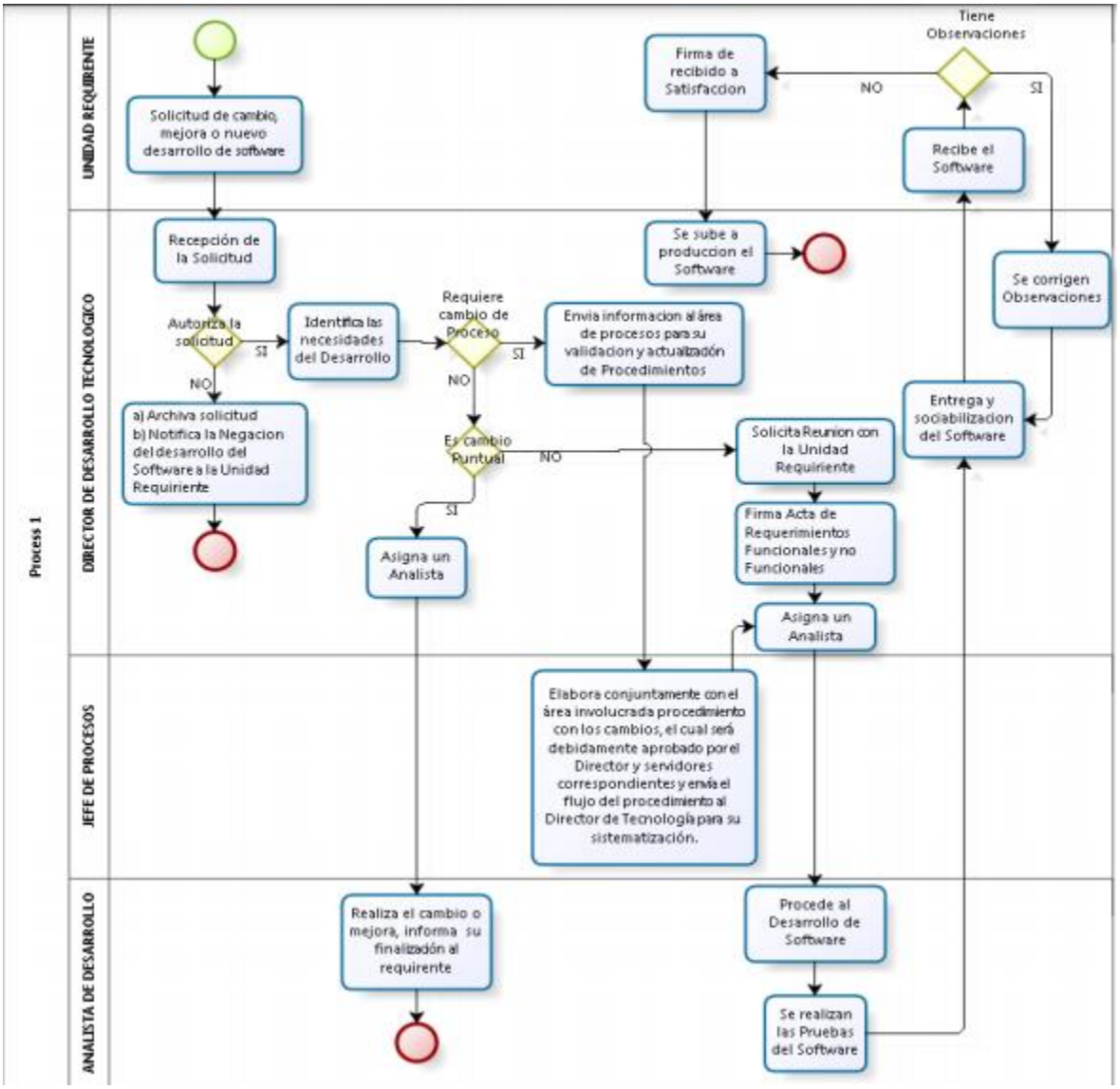
No.	Asigna un analista para el desarrollo del requerimiento	Documento	Responsable	Tiempo (días)
1	Ingresa vía sistema la "Solicitud de cambio, mejora o nuevo desarrollo de software", que se encuentra en la intranet institucional.	"Solicitud cambios en el desarrollo de un aplicativo informático"	Director/Usuario requirente del Proyecto	1 dia
2	Recepta la solicitud y analiza el impacto del cambio solicitado sobre un el aplicativo informático ¿Autoriza la Solicitud? SI: Identifica las necesidades del desarrollo. NO: Envía respuesta vía correo electrónico al director requirente indicando el motivo de la no viabilidad del proyecto.		Director de de Desarrollo Tecnológico.	10 min
2.1	¿Requiere cambio en proceso? NO: ¿Es cambio puntual? SI: Autoriza a realizar los cambios o mejoras puntuales sobre un aplicativo, que no incurra en cambios significativos en el proceso NO: Solicita reunión con el área requirente, genera un acta de requerimientos funcionales y no funcionales, y define el tiempo de entrega. Paso 4 SI: Envía información al área de procesos		Director de de Desarrollo Tecnológico	3 dias

	para su validación y actualización de procedimientos, de requerir solicita reunión con el área requirente para recopilar información, genera un acta de requerimientos funcionales y no funcionales, y define el tiempo de entrega. Paso 3			
3	Elabora conjuntamente con el área involucrada procedimiento con los cambios, el cual será debidamente aprobado por el Director y servidores correspondientes y envía el flujo del procedimiento al Director de Tecnología para su sistematización.		Jefe del área de procesos	
4	Asigna un analista para el desarrollo del requerimiento	Acta de requerimientos funcionales	Director de Desarrollo Tecnológico	2 dias
5	a) Procede con el desarrollo, previo la elaboración del Plan de Gestión cuando sea un aplicativo informático nuevo, en el cual se define: la arquitectura y código fuente del aplicativo (estándares, patrones de programación, documentación), modelo de entidad – relación, código fuente de los procedimientos de migración y carga inicial de datos. • Planeación. - Se efectúa la planificación de la iteración en función de los requerimientos seleccionados a ser implementados. Se planifican las tareas y recursos necesarios. • Análisis. - Se obtiene una especificación detallada del aplicativo informático que satisfaga las necesidades de información de los usuarios y sirva de base para el	Plan de Gestión	Analista de Desarrollo Tecnológico	

	posterior diseño del sistema. • Diseño. - Se define la arquitectura del aplicativo informático y del entorno tecnológico que le va a dar soporte, así como: componentes, interfaces y otras características del aplicativo informático, que pueden ser codificadas y probadas. • Codificación. - Se genera el código fuente del aplicativo informático por medio de la programación, verificación, pruebas unitarias, pruebas de integración y depuración. • Pruebas. - Se evalúa la calidad del aplicativo informático, para mejorarlo, mediante la identificación de defectos y problemas del mismo. Estas pruebas se ejecutan de acuerdo a lo establecido en el plan de pruebas. b) Realiza las pruebas del software, coordinando una reunión con el Usuario experto de la unidad requirente. c) Genera una social			
6	Recibe el aplicativo informático. ¿Tiene observaciones? SI: Envía las observaciones a la Dirección de Tecnología para que efectúen las correcciones del caso Mediante Correo Electrónico institucional. NO: Firma un Acta de Recepción a conformidad	Acta de recepción y conformidad (Que es parte del Acta de requerimientos funcionales)	Director requirente o su delegado	2 dias
7	• Coloca los entregables (documentación, código fuente, etc.) en los diferentes		Director de Desarrollo	15 días

	repositorios institucionales específicos de gestión, almacenamiento y versionamiento de información de software de aplicaciones. • Solicita al Procurador Síndico Municipal el registro del aplicativo informático desarrollado, conforme a lo establecido en el Reglamento a la Ley de Propiedad Intelectual. • Sube a producción la aplicación informática, envía un correo institucional al Director requirente e involucrados informando la puesta en producción y su uso obligatorio. • Informa a la Dirección de Comunicación el desarrollo de nuevo sistema para su publicación y marketing.		de Tecnología	
8	Realiza campaña de comunicación del nuevo sistema		Dirección de Comunicación	
	FIN PROCESO			

DIAGRAMAS DE FLUJO:



FORMATOS DE REGISTRO.

ESPECIFICACIÓN DE REQUERIMIENTOS

Descripción de la Funcionalidad de la Aplicación.

Descripción breve del sistema.

Nombre del sistema a Modificar / Mejorar

Descripción de la relación de la Aplicación con Sistemas e Interfaces Externas.

Validación de integración con otros sistemas

Objetivo del proceso

El objetivo principal del proceso de especificación es lograr definir de forma clara y precisa cada uno de los requerimientos del Sistema para el seguimiento de la gestión de proyectos de desarrollo de Software.

Responsables del Proceso

El proceso de especificación será desarrollado conjuntamente por todo el equipo de trabajo, realizando una distribución equitativa de cargas de trabajo. El proceso estará dirigido por el líder del proyecto y el aseguramiento de la calidad estará a cargo del Líder de Calidad.

Requerimientos funcionales: En este documento se especificarán los requerimientos funcionales del sistema

Requerimientos no funcionales: En este documento se especificarán los requerimientos no funcionales del sistema.

Tiempo aproximado de Entrega:

Verificaciones:

No. Verificación	Observación	Fecha	Usuario	Firma

Ingresar el Número de Módulos a Desarrollar:

Fecha del Acta:

Vinicio Bucheli	Gustavo Donoso	Usuario

ACTA DE RECEPCIÓN A CONFORMIDAD

Fecha de Recepción:

RECEPCIÓN A CONFORMIDAD:

Luego de revisar el aplicativo ACEPTO A CONFORMIDAD ya que cumple con lo solicitado y se ajusta a los requerimientos firmada en el Acta de requerimientos funcionales:

Observaciones:

Vinicio Bucheli	Gustavo Donoso	Usuario

PROTOCOLO – PASO A PRODUCCIÓN PARA LA ENTREGA DE PRODUCTO DE NUEVAS SOLUCIONES TECNOLÓGICAS

1. Introducción

El presente documento tiene como finalidad establecer los lineamientos y definir los artefactos para la entrega en producción de todos los nuevos servicios de tecnología o sus actualizaciones, que faciliten al Ministerio de Educación su gestión, administración y mantenimiento.

2. Objetivos

2.1. Objetivo General

Establecer y describir los lineamientos que se deben cumplir, para la entrega en productivo al Ministerio de Educación Nacional, de las nuevas soluciones de tecnología (infraestructura, sistemas de información y/o servicios tecnológicos) del Ministerio de Educación Nacional.

2.2. Objetivos Específicos.

- ✓ Asegurar la entrega de la totalidad de documentación de la solución implementada
- ✓ Asegurar el despliegue de las nuevas soluciones tanto de aplicaciones como de infraestructura, para los ambientes de (Certificación y Producción).
- ✓ Garantizar transferencia de conocimiento hacia los usuarios/clientes y personal técnico, que resguarde la operatividad de los servicios IT.
- ✓ Controlar los riesgos latentes generados al realizar los despliegues de nuevas soluciones tecnológicas.

3. Alcance

El alcance de este protocolo describe los lineamientos a cumplir para nuevas soluciones y actualizaciones y aplica desde el inicio de su implementación hasta la salida en productivo y entrega a la operación de la misma.

4. Funcionalidades

A continuación, se describen los roles que interactúan en el proceso, y las responsabilidades asociadas a cada uno.

Ítem	Rol	Responsabilidades
4.1	Coordinador de Aplicaciones y/o Coordinador de Infraestructura del MEN	a. Encargados de asegurar la aprobación de paso a producción de las soluciones tecnológicas adquiridas por el MEN.
4.2	Líder Técnico MEN	a. Encargado de coordinar con el proveedor de la solución la entrega acorde a los requisitos de este documento al Ministerio de Educación Nacional. b. Es el encargado de gestionar con el coordinador que corresponda (ítem 4.1), la aprobación para el paso a producción. c. Responsable de asegurar el envío y sustentación del RFC en los CAB. d. Encargado de gestionar y coordinar con el proveedor o área funcional del MEN, la realización de pruebas y entrega de información.
4.3	Change Manager	a. Responsable de verificar la solicitud de paso a producción, y evaluar la viabilidad por parte de los involucrados, de acuerdo al proceso de gestión de cambios. b. Responsable de garantizar el flujo y ejecución del RFC.

4.4	Líder Funcional MEN	a. Persona del área usuario, responsable de validar y dar conformidad al cumplimiento de los requerimientos funcionales.
4.5	Operador	Dentro de este rol, se encuentran asociados los siguientes perfiles: **4.5.1 Especialista Aplicaciones** b. Responsable de validar y dar conformidad a la aplicación que será puesta en producción y a la documentación entregada. c. Encargado de hacer el despliegue de la aplicación en el ambiente de producción. **4.5.2 Especialista Base de Datos** a. Responsable de validar y dar conformidad a la base de datos que será puesta en producción. b. Encargado de hacer el despliegue de base de datos en el ambiente de producción. **4.5.3 Especialista Seguridad** c. Responsable de verificar que la aplicación cumpla con las poliitcas de seguridad establecidas por el Ministerio de Educación Nacional.

5. Matriz

En el siguiente cuadro se lista la asignación de responsabilidades de los involucrados en este protocolo de paso a producción, donde: R – Responsable, A – Administrador, C – Consultado e I – Informado:

ITEM	ROL					
	Proveedor	Coordinadores MEN	Líder Técnico MEN	Change Manager	Operador	Usuario Final
1. **Entregra de la Solución Actulizado o Nueva**	R					
2. **Verifica Cumplimiento de Protocolo**		A	R	I	I	C
3. **Aprueba pase a producción**		R				

6. Requisitos para la entrega de nuevas aplicaciones en productivo.

A continuación, se indican los requisitos que se deben cumplir para entregar en productivo las nuevas aplicaciones

D: Pruebas – C: Certificación – P: Producción

Ítem	Ambiente			Entregable	Descripción
	D	C	P		
6.1		X	X	Pruebas funcionales y técnicas	Entrega resultados pruebas funcionales en ambiente de Certificación y Acta de aprobacion del area funcional.
6.2		X	X	Inventario de aplicaciones	Entregar el inventario de las aplicaciones que componen la solución con la respectiva CMDB actualizada.
6.3		X	X	Fuentes o medios de instalación de la aplicación.	Son los recursos, archivos con la carpeta o código fuente de la aplicación que son entregados por el MEN al Operador, para poder realizar el despliegue de la aplicación. (Deployment, Indicar Librerías y Dependencias, Scripts BD). **Para las aplicaciones comerciales:** entrega de medios en físico o indicar las rutas o el link para descargar los medios de instalación a última versión. **Para las aplicaciones IN HOUSE**: entrega del código fuente o su compilador a última versión, en forma física o en la ruta con los respectivos permisos para su descarga.
6.4			X	Manual Técnico.	Es un documento en el que se contemplan los aspectos técnicos de la aplicación, y en el que se definen los servicios y la forma de administrarlos, como mínimo este documento deberá contener: a) Contenido b) Introducción c) Objetivo d) Generalidades e) Administración Capa Media APP f) Administración Base de datos
6.5	X	X	X	Manual de Instalación.	Es un documento guía, que ayuda a entender el funcionamiento de la aplicación para los usuarios finales, como mínimo este documento deberá contener: a) Contenido b) Introducción c) Objetivo d) Pre-requisitos de Instalación e) Instalación Base de datos f) Configuración Base de datos g) Instalación Capa Media h) Configuración Capa Media i) Paso a paso despliegue de la APP j) Actualización archivos de configuración k) Verificación correcto despliegue

6.6			X	Arquitectura de la aplicación.	Documento y/o diagrama que define los componentes que hacen parte de la aplicación, y la comunicación entre los mismos, como mínimo este documento deberá contener: a) Contenido b) Introducción c) Objetivo d) Arquitectura del Negocio (Modelo conceptual cadena de valor, macro procesos, procesos, subprocesos). e) Arquitectura de la infraestructura f) Arquitectura de la solución (Diagramas caso de uso, diagramas de secuencia). g) Diagrama dependencias e interoperabilidad con los otros sistemas. h) Conclusiones i) Glosario j) Anexos Nota: Los diagramas deben estar en formato editable "Visio"
6.7			X	Manual de usuario	Es un documento en el que se relacionan las actividades que puede realizar el administrador o los usuarios de la aplicación, como mínimo este documento deberá contener: a) Contenido b) Introducción c) Objetivo d) Generalidades e) Pre requisitos de uso f) Funcionalidades g) Glosario h) Anexos
6.8			X	Diagrama entidad-relación	Documento y/o diagrama que permite ver las relaciones y atributos de los objetos de la base de datos, como mínimo este documento deberá contener: a) Diseño relacional de la BD. b) Dependencias de la aplicación sobre los esquemas de la BD. c) Diccionario de Datos. d) Usuario y privilegios de usuarios sobre los esquemas. e) Listado de procedimientos almacenados, índices, funciones, triggers, vistas, Jobs, sinónimos, dblinks. Nota: Los diagramas deben estar en formato editable "Visio"
6.9	X	X	X	Sizing	Cantidad de recursos proyectados, para soportar un número determinado de usuarios, como mínimo este documento deberá contener: a) Cantidad de usuarios a soportar b) Memoria c) CPU d) Storage

Ítem	Ambiente			Entregable	Descripción
	D	C	P		
					Nota: el plan de capacidad de la aplicación debe estar dimensionado mínimo a tres años.
6.10		X	X	Pruebas de carga y stress.	Son pruebas que debe realizar el proveedor de la aplicación, con el fin de determinar el rendimiento y respuesta de la misma, bajo una cantidad de peticiones esperada. a) Criterios de tiempos de respuesta y uso de recursos en carga. b) Cantidad de usuarios estimados en operación normal. c) Cantidad máxima de usuarios soportados con el criterio de tiempo de respuesta. d) Requerimientos mínimos de hardware y comunicaciones para cumplir con criterio de tiempo de respuesta.
6.11		X	X	Pruebas de Seguridad	Son pruebas que debe realizar el proveedor de la aplicación, las cuales permiten garantizar que la aplicación se encuentra libre de vulnerabilidades. La solicitud de paso a producción incluye certificación de pruebas de seguridad, donde se indique: La aplicación o su versión ha pasado pruebas basadas en OWASP sobre: a) Introducción b) Objetivos c) Alcance d) Fecha de realización e) Metodología utilizada f) Resumen ejecutivo g) Hallazgos detallados con recomendaciones. h) Configuración i) Gestión identidad j) Autenticación k) Autorización l) Manejo de sesiones m) Validación de entrada de datos n) Manejo de errores o) Lógica de negocio
6.12	X	X	X	Backups	Indicar cuales son las rutas que se deben respaldar dentro de las políticas de Backups, periodicidad y rotación del Backups.
6.13		X	X	Servicios Monitoreados	a. Indicar cuales son los servicios que se desean monitorear sobre la aplicación. (Puertos, servicios, url, etc). b. Indicar un usuario de consulta, con el cual se pueda realizar logueo sobre la aplicación.
6.14			X	Categorización de la Aplicación	Indicar cuál es la categoría a la que pertenece la aplicación de acuerdo a las siguientes características : **Aplicaciones Cat I:** a. Aplicaciones de gran impacto o misión crítica para el MEN y el Sector Educativo Colombiano. b. En este grupo de aplicaciones se encuentran las que registran mayor transaccionalidad especialmente desde las Secretarías de Educación Nacional. **Aplicaciones Cat II:** a. Aplicaciones de impacto medio para el MEN y para el Sector Educativo. b. En este grupo de aplicaciones se encuentran sistemas con poca cantidad de registros, y con una baja transaccionalidad para las bases de datos y para el canal de Internet.

Ítem	Ambiente			Entregable	Descripción
	D	C	P		
					Aplicaciones Cat III: a. Aplicaciones con impacto bajo para el MEN y el Sector. b. En este grupo de aplicaciones se encuentran sistemas de uso interno del MEN.
6.15			X	Licenciamiento	Entregar los acuerdos de licenciamiento suscritos con los proveedores e indicar las fechas de vigencia de los licenciamientos y tipo de soporte (7x24, 8x5). Entrega de la relación de todas las licencias utilizadas para el desarrollo, tanto en el sistema operativo, capa media y servidores, esto para licencias base como para los equipos a utilizar. Al respecto a las licencias de software comercial, se debe recibir del proveedor la respectiva certificacion del licenciameinto. Entregar certificado de cesión de derechos patrimoniales de autor.
6.16		X	X	Cuentas y contraseñas de Usuarios	Entregar los usuarios de ROOT y contraseñas, de consulta y de administración, con los cuales se pueda realizar logueo sobre cada aplicación; estas deben estar incluidas dentro del KeyPass.
6.17		X	X	Gestión de Vulnerabiliades	Entregar escaneo de vulnerabilidades y mitigacion de las mismas.
6.18		X	X	Gestión de Backlog	Gestionar y dar cierre al backlog para los procesos de: gestión de cambios, gestión de incidentes, gestión de problemas y gestión de solicitudes asociadas a la infraestructura a entregar.
6.18		X	X	Gestión de Backlog	Gestionar y dar cierre al backlog para los procesos de: gestión de cambios, gestión de incidentes, gestión de problemas y gestión de solicitudes asociadas a la infraestructura a entregar.
6.19		X	X	Plan de Recuperación Tecnológica (PRT)	Entregar documentaciòn con el plan de recuperación ante una indisponibildad y el procedimiento donde se describa cómo se debe realizar la recuperacion de esta, el cual debe contener como mínimo: a) Introducción b) Objetivos c) Alcance d) Fecha de realización e) Metodología utilizada f) Resumen ejecutivo g) Procedimiento de recuperación h) Tiempos de recuperación
6.20	X	X	X	IPV6	Entregar evidencia dentro de la aplicacion del protocolo IPV6.
6.21		X	X	Tiempos de Logueo para Aplicaciones Nuevas	Entregar definidos y documentados, los tiempos mínimos de logueo a corde a su respectiva categorización.
6.22	X	X	X	Diagrama DSI	Entrega de diagrama DSI, en formato visio.
6.23	X	X	X	Ingreso a Almacén	Entregar el certificado de ingreso a almacén
6.24		X	X	Actualización Linea Base APP	Entregar acta de de inclusión de la nueva solución en la liena base de de aplicaciones del Ministerio.
6.25		X	X	Actualizacion Archivos en la Intranet	Entregar evidencia del carga de la totalidad de documentación en el dosier de la solución.

7. Requisitos para la entrega de nueva Infraestructura tecnológica en productivo:

A continuación, se indican los requisitos que se deben cumplir para entrega a productivo de nueva infraestructura tecnológica.

Ítem	Entregable	Descripción
7.1	Inventario	Entregar el inventario o relación de la infraestructura con mínimo los siguientes ítems: a) Marca b) Modelo c) Cantidad d) Descripción e) Modelo f) Estado g) Fabricante h) Ubicación física i) # de placa, etc. j) Relación de VPNs existentes indicando usuario rol y permisos de acceso. k) CMDB actualizada a la fecha de entrega en la herramienta CA.
7.2	Manuales Técnicos.	Garantizar que en este documento estén contemplados como mínimo los aspectos técnicos de la infraestructura como: a) Tipos de garantía b) Niveles de escalamiento c) Instructivo del soporte técnico (forma de operar), si lo tiene, los servicios ofrecidos y en general la forma de administrar cada elemento.
7.3	Manuales Administración	El documento debe contener instructivos para la administración del elemento según su rol (Ej.: servidor base de datos, balanceador de carga, etc)
7.4	Ingeniería	En este documento debe contener la arquitectura detallada así: a) Arquitectura de la solución (esquema de red (fisico y

		logico, vlans, etc.), equipos de seguridad, balanceo. b) Descripción de capa media entre otros) de la solución a nivel donde se puede identificar cada componente. c) Direccionamiento IP, d) Tablas de rutas e) NAT público f) Mapeo de servicios g) Plan de capacidad proyectado a 3 años Nota: la arquitectura se debe entregar en formato editable "Visio".
7.5	Aseguramiento de infraestructura	Entregar inventario de los dispositivos de seguridad y la evidencia de las pruebas de seguridad realizadas por el área de seguridad, para garantizar que NO se tiene vulnerabilidad, en caso de que existiera, garantizar que estas se encuentren documentadas y argumentadas, de modo que avale que no hay riesgo para la información, infraestructura y los sistemas de información del Ministerio de Educación Nacional
7.6	Backups de configuración	Entregar los Backups en medio magnético, los archivos de configuración de cada uno de los elementos que componen la solución.
7.7	Backups	Entregar la política de Backups y sus tiempos de retención, manuales de administración de la herramienta de Backups (librería y aplicación), en la que se indica: a) Cuál es la frecuencia b) Tipos de Backups c) Tiempos de retención d) Rutas de almacenamiento e) Inventario de medios de almacenamiento. f) Lineamientos de custodia. g) Resultados de pruebas de recuperación de los últimos tres (3) meses.
7.8	Servicios Monitoreados	Definir cuáles son los elementos que deben ser monitoreados: a) Puertos de monitoreo

		b) Dispositivos y URLs. Por cada componente de la solución
7.9	Cuentas y contraseñas de Usuarios	Entregar los usuarios y contraseñas en sobre sellado de: ROOT, Administrador, y consulta, con los cuales se pueda realizar logueo sobre la solución; a su vez deben ser incluidos dentro del KeyPass del Ministerio
7.10	Capacity Planing	Análisis y estadísticas de uso de los recursos que componen la solución (memoria, almacenamiento, canal CPU, etc.) del último año de operación, Así como los indicadores de uso, disponibilidad y proyección a 3 años.
7.11	Licenciamiento	Entregar los acuerdos de licenciamiento suscritos con los proveedores de Hardware y software que compone la solución. Entregar esquema de soporte (ej. 7x24, 5x8) indicar las fechas de vigencia de los licenciamientos.
7.12	Garantía	Contratos de soporte y garantía de cada elemento de la solución
7.13	Gestión de Vulnerabilidades	Entregar informe de los últimos tres (3) meses del escaneo de vulnerabilidades y mitigación pertinente de la plataforma a entregar
7.14	Gestión de Backlog	Gestionar y dar cierre al backlog para los procesos de: gestión de cambios, gestión de incidentes, gestión de problemas y gestión de solicitudes asociadas a la infraestructura a entregar.
7.15	Plan de Recuperación Tecnológica (PRT)	Entregar documentación con el plan de recuperación ante una indisponibilidad en donde se evidencie el procedimiento de cómo se debe realizar su recuperación. a) Introducción b) Objetivos c) Alcance d) Fecha de realización e) Metodología utilizada f) Resumen ejecutivo g) Procedimiento de recuperación

		h) Tiempos de recuperación
7.16	IPV6	Configuración dentro de la infraestructura del protocolo IPV6. Nota: Se debe garantizar que cualquier infraestructura a entregar debe soportar el procolo IPV6
7.17	Arquitectura	Entrega de la arquitectura en donde se asegure un esquema de alta disponibilidad y full tolerancia, para que esta sea compatible con la actual arquitectura del Ministerio
7.18	Ingreso a Almacén	Entregar el certificado de ingreso a almacén del Ministerio

8. Requisitos para la entrega a la mesa de servicio de tecnología en productivo:

A continuación, se indican los requisitos que se deben cumplir para entregar el nuevo servicio a la mesa de ayuda.

Ítem	Entregable	Descripción
8.1	Capacitación	Realizar la capacitación y entregar evidencia (listados de asistencia) de la misma por parte del proveedor o del Ministerio (aplica para desarrollos in house). Lo anterior, con el fin de solucionar o tener la claridad necesaria para justificar ante el usuario final las respuestas a su necesidad. Dentro de esta capacitación es necesario asegurar que los capacitados cuenten con usuarios de prueba que permitan consultar dentro de la aplicación para orientar de una mejor manera a los usuarios finales ya que esto permite el desarrollo de una comunicación efectiva.
8.2	Matriz de escalamiento	Entrega de la matriz de escalabilidad por cada frente, en este debe estar detallado: la solución que soporta (ej. aplicación SIGSE, servidor 1), especialidad, nombre del especialista, correo electrónico y número telefónico.
8.3	Árbol de tipificación de la herramienta de gestión	Entrega de la tipificación por cada frente, indicando: a) Servicio b) Categoría c) Requerimiento d) Clasificación (incidente, evento requerimiento)
8.4	Catálogo de Servicios	Entrega de la información del servicio, para la inclusión en la matriz del catálogo de servicio del nuevo servicio o la actualización del mismo de ser requerido. Como mínimo deberá informar: • Categoría del Servicio de TI • Nombre del Servicio de TI • Descripción del Servicio

		• Solicitud del Servicio de TI • Descripción de la Solicitud de Servicio • Excepciones del Servicio • Condiciones del Servicio de TI • Impacto del Servicio • Tiempo de Atención • Tiempo de Solución • Documentos Asociados al Servicio • Clientes del Servicio • Estado
8.5	Tiempo de respuesta.	Hacer entrega de los ANS, OLA y SLAS, con la descripción de los tiempos de respuesta de acuerdo a su categorización en los diferentes niveles.
8.6	Base de Datos del conocimiento.	Entrega de la base de datos de conocimiento donde se describa los errores conocidos, sus síntomas, la causa raíz y su respectiva solución y gestión de problemas.

CASO DE ESTUDIO.

Objetivo general:

Analizar el control interno en el almacén de la Facultad de Ciencias Económicas y Sociales de la Universidad del Zulia

Objetivos Específicos

1. Describir el proceso de control interno en el almacén de la Facultad de Ciencias Económicas y Sociales de la Universidad del Zulia.
2. Identificar el Método de Inventario que adopta el almacén de la Facultad de Ciencias Económicas y Sociales de la Universidad del Zulia.
3. Determinar la efectividad de los procesos administrativos relacionaos con el pago a los proveedores del almacén de la Facultad de Ciencias: Económicas y Sociales de la Universidad del Zulia.

Justificación de la Investigación.

En el presente trabajo de investigación se analizó el control interno del almacén de la Facultad de Ciencias Económicas v Sociales de la Universidad del Zulia, con la finalidad de aprender cómo se están llevando los procesos de recepción, almacenamiento y despacho de los productos que demandan, de tal ll1anera que la información puede ser utilizada para optimizar el proceso de control de materiales, utilizando para ellos reglas y procedimientos más adecuados que le garanticen efectividad.

Todos los factores, reglas y procedimientos utilizados en esta investigación, pueden ser útiles a otras organizaciones pertenecientes al ramo, cuyo control sobre los materiales no sea eficiente y por ende no les permita operar de lila forma óptima. Así mismo, le permite al almacén mejorar la efectividad de los controles de inventarios de productos, ya que podrá

darse cuenta cual es la cantidad óptima de inventario a través de los tiempos de entrega y la disponibilidad y la disponibilidad de la mercancía, así como también detectar las necesidades que se tengan de estos para adecuar los niveles de stock a los requerimientos reales que el almacén tenga de los mismos.

Esto le permitió al personal del almacén darse cuenta de las fallas que su control interno está presentando y basándose en esta situación establecer los correctivos necesarios para disminuir los costos que se generan en ello, por otro lado, dicha investigación, es un aporte a las ciencias administrativas y contables ya que este trabajo sirve de base o incentivo a otros investigadores que quieran profW1dizar sobre el tema de los controles internos de inventarios del almacén.

Característica del Control Interno

Según (Cepeda, 1997)) el control interno se ejecuta dentro de la empresa tomando en consideración las siguientes características, las cuales son las siguientes:

1. Corresponde a la máxima autoridad de la organización la responsabilidad de establecer, mantener y perfeccionar el sistema de control interno, que debe adecuarse a la naturaleza, la estructura y la misión de la organización.
2. La auditoría interna, o quien funcione como tal, es la encargada de evaluar de forma independiente la eficacia, efectividad, aplicabilidad y actualidad del sistema de control interno de la organización y propone a la máxima autoridad de la respectiva organización las recomendaciones para mejorarlos.
3. El control interno debe diseñarse para prevenir errores y fraudes
4. Los mecanismos de control se deben encontrar en la redacción de todas las normas de la organización.
5. El control interno no tiene como objetivo medir desviaciones sino que permite identificarlas, considerando que su ausencia es una causa de las desviaciones.
6. El control interno es inherente al desarrollo de las actividades de la organización.

Estructura del Proceso de Control Interno.

Para (Poch, 1989), existen mecanismos propios de las organizaciones esenciales, ligados al control, los cuales son los procedimientos de autorización, los supervisores y la figura del contralar.

En referencia a los procedimientos de autorización, el autor expresa que en el án1bito de la responsabilidad y el de competencia se reparten la autoridad y el poder de delegación. Es así, corno la autoridad significa la competencia o facultad para realizar ciertos actos o para delegar tal autorización en otras personas subordinadas en la línea jerárquica. Es esencial que para la aplicación del control interno las competencias se hallen claramente específicas en los manuales de procedimientos, punto que viene a constituir el desarrollo de la organización. En tal sentido, se establece el poder de decisión al que, cómo y cuánto, respecto a las transacciones y demás actos de la empresa, los cuajes son acompañados por un amplio poder de delegación respecto a la ejecución propiamente dicha.

El supervisor adopta el control interno con el fin de buscar una amplia conexión con el sistema de relaciones que se da en la organización, teniendo que controlar su propio trabajo, haciendo control interno, que consiste que el trabajo de una persona sea sistemáticamente revisado por otro, y para la cual separa funciones y responsabilidades.

Por otra parte, el jefe de departamento controla el grupo que tiene bajo su mando asegurándose que todos cumplan con las actividades y entre departamentos también se harían chequeos para saber qué, cómo y cuánto se está haciendo en ellos para beneficio de la empresa.

Por otro lado, el control interno se estructura bajo algunas condiciones, las cuajes para (Cepeda, 1997), son las siguientes:

- **Un término de comparación:** Que puede ser un proceso, un programa, una norma, un estándar o un objetivo.

- **Un hecho real:** El cual se comprar con la condición o término de referencia del punto anterior.
- **Una desviación:** Que surge como resultado de la comparación de los dos puntos anteriores.
- **Un análisis de causa:** Los cuajes han dado origen a la desviación entre el hecho real y la condición ideal o término de referencia.
- **Toma de decisiones:** Son las decisiones que han de tomar y las acciones que se han de desarrollar para corregir la desviación.

Como se observa la estructura del proceso de control interno para la empresa., establece la forma, y como deberá llevarse esta) definiéndose como un hecho real que permita ver las fallas para analizar lo que está ocasionando y tomar decisiones que propicien el logro efectivo de los objetivos de la empresa.

Elementos del Sistema de Control Interno.

Goxcns y Goznes (1999), alegan que toda organización, bajo la responsabilidad de sus directivos, debe establecer aspectos que orienten la aplicación del control interno, entre las cuales tenemos las siguientes:

- Definición de los objetivos y las metas, tanto generales como específicas, además de la formulación de los planes operativos que sean necesarios.
- Definición de políticas como guía de acción y procedimientos para la ejecución de políticas.
- Adopción de un sistema de organización adecuado para ejecutar los planes.
- Delimitación precisa de la autoridad y los niveles de responsabilidad.
- Arunisión de normas de protección y utilización racional de los recursos.
- Dirección y administración del personal de acuerdo con un adecuado sistema de evaluación.

- Aplicación de las recomendaciones resultantes de las evaluaciones de control interno

Responsabilidad del Control Interno

El control interno es fundamentalmente una responsabilidad gerencial, desarrollada en forma autónoma que, para que rinda verdaderos frutos, debe ajustarse a las necesidades y requerimientos de cada organización. Además el control interno difiere entre organizaciones. Según (Goxens y Goznes, 1999), el control interno se lleva a cabo por personas de la empresa, encargados expresadamente por ello, por lo cual revisa y comprueba, en forma permanente los servicios contables, estadísticos, de inspección y similares de la empresa, sirviéndose de ellos para controlar la actuación dentro de ella.

La responsabilidad por las actuaciones recae en el gerente y sus funcionarios delegados, por lo cual es necesario establecer un sistema de control interno que les permita tener una seguridad razonable de que sus actuaciones administrativas se ajustan en todo a las normas legales y estatutarias aplicables a la organización.

Así que, el sistema de control interno debe ser un conjunto armónico conformado por el sistema de planeación, las normas, los métodos) los procedimientos utilizados para el desarrollo de las funciones de la organización y los mecanismos e instrumentos de seguimiento y evaluación que utilicen para realimentar su ciclo de operaciones.

Esta característica es fundamental, ya que es la que permite que todos los elementos de la organización participen activamente en el ejercicio de control donde la gerencia a través de la orientación general y la evolución global de los resultados junto con las áreas ejecutivas a través del establecimiento de norma y procedimientos para desarrollar actividades, y las dependencias de apoyo, mediante el uso adecuado de procesos administrativo.

Principios del Control Interno.

Según (Cepeda, 1997), el ejercicio del control interno implica que se debe hacer siguiendo los principios de igualdad, moralidad, eficiencia, celeridad, imparcialidad, publicidad y valoración de los costos ambientales.

Para una mayor comprensión se desarrolla a continuación:

1. El principio de igualdad, consiste en que el sistema de control interno debe velar porque las actividades de la organización estén orientadas efectivamente hacia el interés general, sin otorgar privilegios a grupos especiales.
2. Según el principio de la moralidad, todas las operaciones se deben realizar no solo aplicando las normas aplicables a la organización, sino los principios éticos y morales que rigen la sociedad.
3. El principio de eficiencia, vela porque en igualdad de condiciones de calidad y operatividad, la provisión de bienes y/o servicios se haga al mismo costo, con la máxima eficiencia y el mejor uso de los recursos disponibles.
4. El principio de economía, vigila que la asignación de recursos sea la más adecuada en función de los objetivos y las metas de la organización.

Inventarios del Almacén.

Para (Stoner, Freeman y Gilbcrt, 1996), son las existencias de materias primas, trabajo en proceso y bienes terminados que mantienen una organización para satisfacer sus necesidades. Los procedimientos utilizados para inventarios de productos en los almacenes de una organización son la recepción, el almacenamiento y el despacho.

Recepción de Productos: Según (Patón, 1987), las actividades de recepción es el procedimiento que se emplea al recibir la mercancía y materiales, varían considerando según las características del almacén o de la planta que se trate. Sin embargo algunas de estas características son de tipo general en establecimiento de importancia. Todas las

n1ercancÍas y los materiales que se reciben se concentrar en el departamento de recepción (que puede ser una sección separada del departamento del almacén). En esta sección o departamento se lleva un registro cronológico en forma de libro o archivo de entrada.

Así mismo (Cuesta) 1987), dice que la organización interna de este departamento es fundamental, dado que actúa como intermediario y catalizador de todos los productos adquiridos por la empresa y que posteriormente van hacer consun1ido en producción o gastados en algún departamentos no productivo. Para la recepción de todos los artículos del almacén se deberá recortar físicamente el producto recibido, cotejando dicha recepción con la copía del pedido enviado por el departamento de compras~ en dicha copia se informará del código, destino del gasto, fecha de recepción, etc.

Almacenamiento del Producto: Para (Cuesta, 1987), es una responsabilidad del encargado del mismo. Por lo tanto) deberá ejercer todas las actividades de conservación, vigilancia, limpieza, organización y control de los artículos. En el almacenamiento se deberá realizar conteos periódicos de materiales con el objeto de confirmar las existencias recogidas en libros. De esta forma resulta posible comparar las existencias teóricas con las reales, analizando posteriormente las diferencias y ajustando los mayores de almacenes

Despacho del Producto: Como lo acota (Narasirnhan, Me. Leavery y Billintong, 1996), es una función del control de la producción que está a cargo de un despachadores una persona que controla la producción coordinada con el departamento de manufactura, el cual mantiene un archivo de todas las órdenes abíertas relacionadas con su departamento, ya que estén liberadas o no. Este archivo se conoce corno archivo de carga muerta. Una vez que el trabajo se libera del departamento del despachador, la orden se pasa al archivo de carga viva

Valuación de los Inventarios: Sea cual fuese la empresa, es preciso la valuación del inventario, que según (Gómez, 1987), representa una importancia significativa, ya que el precio que se le asigne a cada producto determinará el monto del inventario, afectándose el costo de las ventas y, por lo tanto, la utilidad o pérdida neta. Para ponerle el precio a las

unidades que integran el inventario es decir, para valorar los mismos, suelen emplearse, muchos métodos.

Método de los últimos Costos (Método FIFO): Este método de valoración de los inventarios supone que las existencias están formadas por las últimas compras, ya que lo primero que se compró fue lo primero que se vendió. Este método ofrece la ventaja de ajustarse más a la realidad, en cuanto a la tendencia de los precios puesto que se adopta más a situaciones actuales del mercado. Utilizando este método de valoración se le da entrada a su precio de costo y las salidas se registran procurando agotar las primeras compras, a sus respectivos precios de costos, es decir, lo primero entrar será lo primero en salir.

Eficacia y Eficiencia en las Funciones Administrativas: La eficiencia es una parte fundamental y básica de la administración. Hace referencia a los recursos empleados ya los productos obtenidos. Si logramos incrementar la cantidad de productos obtenidos manteniendo constante el volumen de recursos empleados, podremos decir que se ha producido un aumento en la eficiencia. De igual modo, si mantenemos constantes la cantidad de productos obtenidos disminuyendo la cantidad de recursos empleados, también habremos logrado un aumento de la eficiencia. Todos los administradores se enfrentan con el reto de desempeñar sus funciones con recursos (humanos, financieros, físicos, tecnológicos, de comunicación, etc.) limitados, lo que les obliga al empleo eficiente de los mismos.

Aun siendo una características prioritaria la eficiencia en la administración y de los administradores, no es una cualidad eficiente. La administración y los administradores no solo deben buscar la eficiencia en sus acciones, sino que, además, tienen que alcanzar los objetivos propuestos, es decir, tienen que ser eficaces. Se es eficaz cuando se consiguen las metas que se habían definido. Podemos decir, por lo tanto, que la eficiencia está relacionada con los medios y la eficacia con los fines.

Tipo de Investigación.

Con el fin de analizar el control interno en el inventario del almacén de la Facultad de Ciencias Económicas y Sociales de la Universidad del Zulia, se describieron los hechos tal y como se plantearon para luego analizarlos y poder dar un juicio acerca de las fallas que presenta y poder hacer cambios pertinentes, lo cual ha permitido determinar que el tipo de investigación es descriptiva.

Al respecto (Chávez, 1994), expresa que la investigación descriptiva es aquella que se orienta a recolectar información relacionada con el estado real de los fenómenos, personas, objetos o situaciones, tal como se presentaron en el momento de su recolección.

Metodología.

En esta investigación la población estuvo representada por un total de 6 personas de edad comprendida entre los 25-40 años, sexo masculino y con un grado de instrucción de técnicos superiores universitarios y licenciados pertenecientes al almacén de la facultad a los cuales se les aplicó una entrevista estructurada.

Resultados.

Luego de terminar la investigación se destacarían los siguientes resultados:

1. Se pudo comprobar que existen procedimientos definidos y aprobados para el cumplimiento de las reglas de recepción de productos en el almacén de la Facultad de Ciencias Económicas y Sociales de la Universidad del Zulia.
2. Se logró demostrar que si existen reglas para controlar el almacenamiento de la mercancía que depende de la naturaleza de esta para que no se dañen o perezcan en el almacén de la Facultad de Ciencias Económicas y Sociales de la Universidad del Zulia.

3. En el almacén de la Facultad de Ciencias Económicas y Sociales de la Universidad del Zulia se evidenció que hay personal que se encarga de controlar el despacho de producto, ejerciendo el cargo de encargado, quién verifica que la mercancía que sale a las dependencias de la facultad tienen sus órdenes de entrega, así como también controla las fallas que puedan existir.
4. Se pudo confirmar que para el control del despacho~ el procedimiento que llevan las dependencias de la facultad es que éstas verifican sus fallas de mercancía, pasan la información al almacén donde se realizan las boletas de éstas fallas, luego se pasan al administrador para que autorice éstas y luego se la entrega al encargado del almacén para pedirlas a los proveedores.

Conclusiones.

Luego de haber efectuado el proceso de investigación y haber confrontado los objetivos del estudio se pudo llegar a las siguientes conclusiones:

1. El almacén de la Facultad de Ciencias Económicas y Sociales de la Universidad del Zulia no cuenta con un sistema de control interno integrado que le permita llevar con efectividad las actividades de recepción, almacenamiento y despacho de la mercancía.
2. Además, se pudo evidenciar que el método de valuación utilizado en el almacén es el FIFO o PEPS. Ello conlleva a que los costos que se expresan en el estado de ganancias y pérdidas no se ajustan a los precios del mercado.
3. Con respecto a los procesos administrativos relacionados con la cancelación a los proveedores del almacén, se pudo determinar que no existe efectividad, al comprobarse retardo en el proceso de pago sin considerar los factores tien1po, costo y calidad.

CONCLUSIONES

Los controles de aplicación en producción es un tema muy extenso y por ende de gran importancia para tener un gran manejo, desarrollo, producción de los recursos informáticos y gran seguridad en las aplicaciones.

Los temas proporcionados son de bastante uso y muy completo para lograr una buena seguridad en las aplicaciones, manteniendo un desarrollo seguro de los sistemas y seguridad en la arquitectura.

Se debe de trabajar con un buen ciclo de desarrollo de software, trabajando con los diferentes entornos existentes ya que servirá de gran ayuda en la seguridad de las aplicaciones y además incluir prácticas que combinen las operaciones de TI y el desarrollo de software para realizar más rápidamente el desarrollo de sistemas.

Debemos tener en cuenta cada uno de los procesos de administración de operación, ya que los cuatro procesos, llevados a cabo de manera correcta, serán de gran ayuda para lograr una correcta gestión de la producción de las empresas, y esto sirve para añadir crear valor.

Es de gran importancia tener un buen equilibrio entre riesgos y controles y tener un control interno para monitorear las actividades que se estén trabajando en los sistemas y lograr una buena estrategia de liderazgo en la seguridad informática para lograr más fácilmente la protección de las propiedades.

Es un tema muy bueno y es importante que las empresas y organizaciones deben de implementar en los sistemas para estar más protegidos y tener una correcta gestión y por ende que los objetivos planteados puedan ser más fácilmente alcanzados, con la seguridad correcta.

BIBLIOGRAFÍA

- Manico, J., Van Der Stock, A., & Cuthbert, D. (2017, abril). *Estándar de Verificación de Seguridad en Aplicaciones 3.0.1*. OWASP. https://owasp.org/www-pdf-archive/Est%C3%A1ndar_de_Verificaci%C3%B3n_de_Seguridad_en_Aplicaciones_3.0.1.pdf

- Polanco, M. (2010, 30 junio). *Seguridad en aplicaciones*. Magazcitum. https://www.magazcitum.com.mx/?p=537#.X878lGhKhPY

- CSO & Citrix. (2018). *SERIES DE LIDERAZGO DE SEGURIDAD: Estrategias de seguridad para el éxito*. https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/security-leadership-series-security-strategies-for-success-es.pdf

- Snyder, J. (2018, 8 febrero). *DevOps con controles*. IBM Developer. https://developer.ibm.com/es/articles/d-devops-cloud/

- Donoso, G. (2017, octubre). *Procedimiento para el desarrollo de aplicaciones informáticas*. PortoViejo. http://portoviejo.gob.ec/md-transparencia/2017/Noviembre/PROCEDIMIENTOS/procedimiento%20para%20el%20desarrollo%20de%20aplicaciones%20inform%C3%A1ticas%20pro-ddt-001-1.pdf

- Álvarez Mora., M. (2018). PROTOCOLO – PASO A PRODUCCIÓN PARA LA ENTREGA DE PRODUCTO DE NUEVAS SOLUCIONES TECNOLÓGICAS. *MINEDUCACIÓN*, 1–11.

https://sig.mineducacion.gov.co/files/mod_documentos/documentos/ST-PT-01/versiones/ST-PT-01_V3_copia_controlada.pdf

- Pérez Esteso, M. (2020). *Entornos existentes en el ciclo de desarrollo de software y despliegue de aplicaciones*. Geeky Theory. https://geekytheory.com/entornos-existentes-ciclo-desarrollo-software-despliegue-aplicaciones-testing-produccion

- Google Sites. (s. f.). *4.4 LA PLANEACION Y EVALUACION DE LOS PROCESOS PRODUCTIVOS - evaluación de los sistemas tecnologicos*. sites.google. Recuperado 26 de mayo de 2021, de https://sites.google.com/site/evaluaciondelossistemas/4-4-la-planeacion-y-evaluacion-de-los-procesos-productivos

- Google Sites. (s. f.). *4.4.2 LA EVALUACION EN EL DESARROLLO DE LOS PROCESOS DE PRODUCCION PARA MAYOR EFICIENCIA - evaluación de los sistemas tecnologicos*. Recuperado 26 de mayo de 2021, de https://sites.google.com/site/evaluaciondelossistemas/4-4-2-la-evaluacion-en-el-desarrollo-de-los-procesos-de-produccion-para-mayor-eficiencia

- Pirela, Alfonso (2005). Estudio de un caso de control interno. Telos, 7 (3), 483-495. [Fecha de Consulta 26 de Mayo de 2021]. ISSN: 1317-0570. Disponible en: https://www.redalyc.org/articulo.oa?id=99318837010