

3.1 Controles en Aplicaciones en producción

Aldama Márquez Joel Jair.



1. Seguridad en aplicaciones



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.

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.



Seguridad en aplicaciones

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.

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

Seguridad en aplicaciones

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.



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

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.

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

Entorno UAT: User Acceptance Testing

En este entorno, usuarios reales realizan pruebas para asegurarse de que los requisitos de desarrollo de software se han cumplido

Entorno de pre-producción o staging

El entorno de pre-producción o staging es 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.

3. DevOps con controles



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.

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.

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.

Los playbooks de DevOps casi siempre incluyen mecanismos de reversión.

DevOps con controles

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.

Cuando se combina con la complejidad de las grandes empresas, unidades comerciales, equipos distribuidos y varios regímenes de conformidad

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.

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.

hay, por lo menos, diez controles exclusivos para implementar y configurar correctamente

¿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.

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.

4. 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 ejecutadas 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.



5. Control Interno Informático



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.

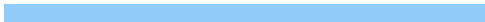
Riesgo = Evento que podría impedir el logro de un objetivo.

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 ineffectividad.



Aspectos clave del control interno.

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”



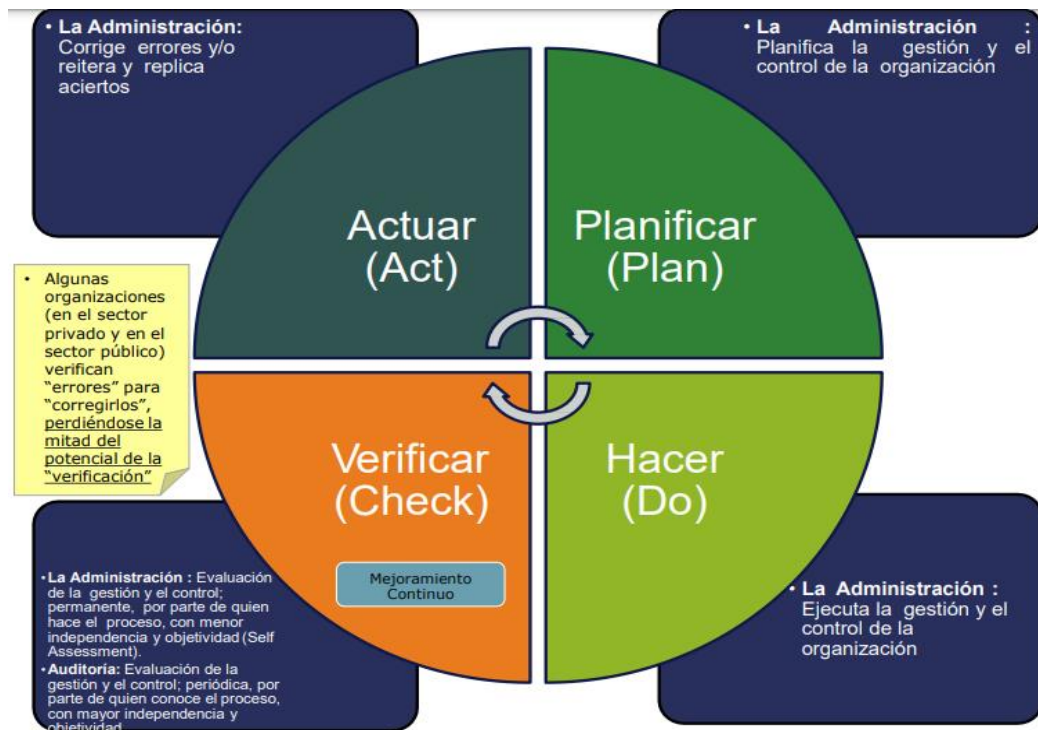
Aspectos clave del control interno.

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 cuando 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:
<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Aumento de la burocracia• Exceso del costo de producción• Complejidad innecesaria de los controles• Incremento del tiempo de ciclo• Actividades que no agregan valor

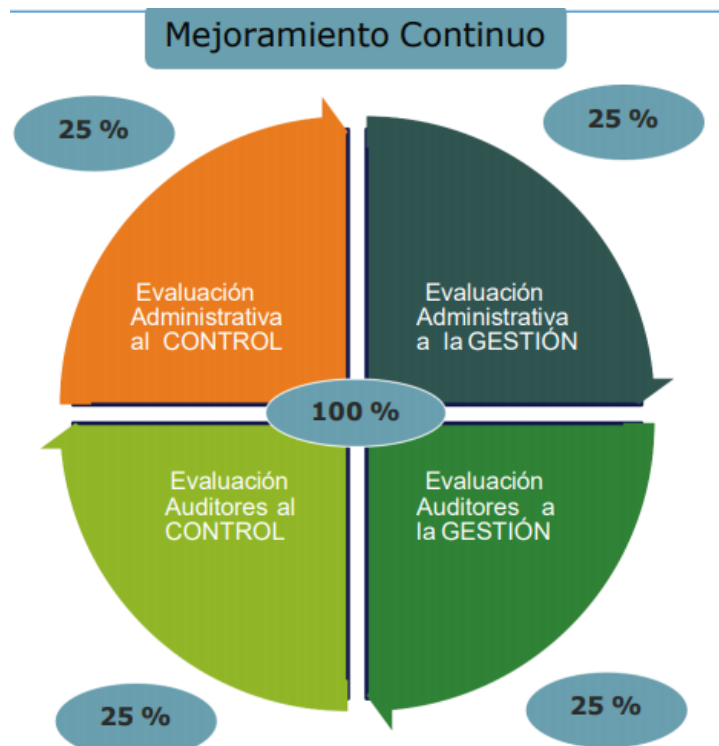
Aspectos clave del control interno.



Aspectos clave del control interno.

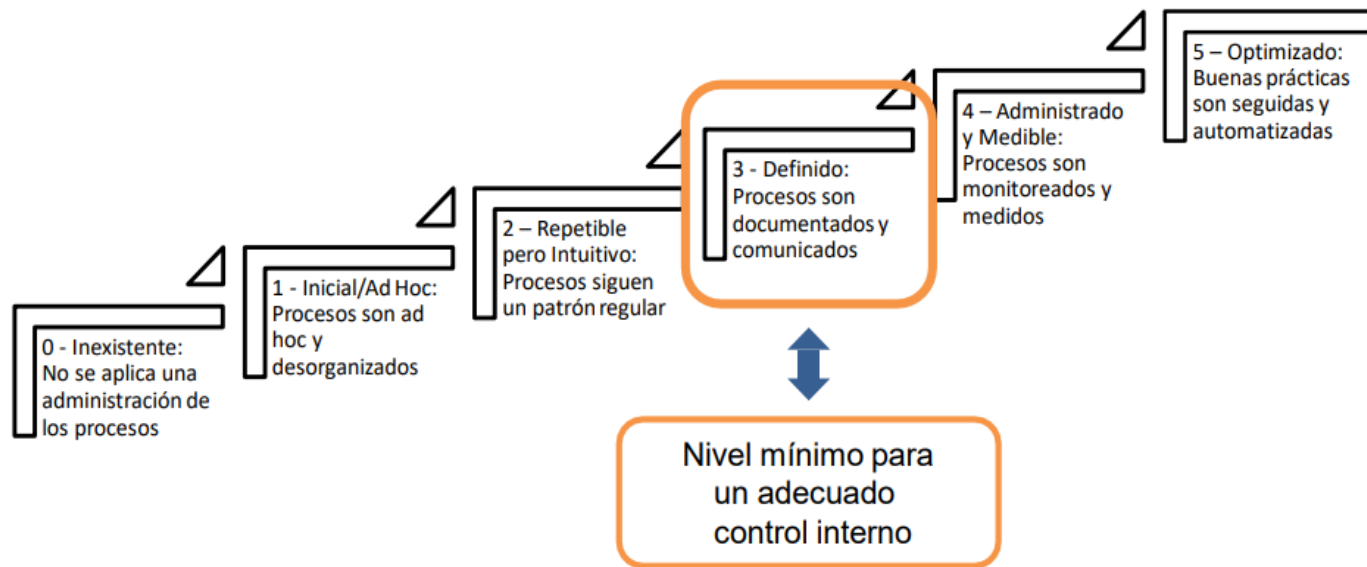
EVALUACIONES COMPLEMENTARIAS

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



Aspectos clave del control interno.

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.




Control interno.

Responsabilidades frente al sistema de control interno.



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 logran 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.

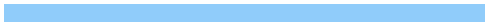


Categorías de control interno

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



Aspectos de implantación en un sistema de control informático.

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

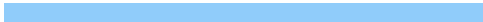
1. Gestión de sistema de información
2. Administración de sistemas.
3. Seguridad
4. Gestión del cambio

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 generales organizativos.

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 enti

COSO II:

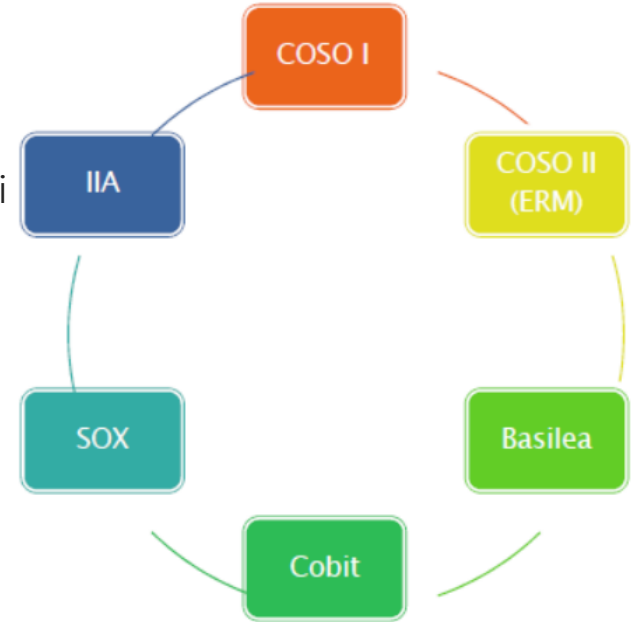
- Se creó en 2004.

- Es un marco integrado sobre análisis de riesgo.

COSO III:

- Se creó en 2013.

- Es una actualización y mejora de COSO I

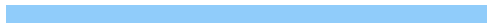


Informe COSO III- Definición.


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
- 

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



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.

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

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.



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

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.



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

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.



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


Nivel 1: Oportunista.

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




Nivel 2: Estándar

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

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.



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

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.

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.

Por esta razón el nivel 1 se recomienda para toda aplicación.



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

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 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).	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 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.	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 individuales o como un lote de transferencias pequeñas.

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

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 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.	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 contienen información poco esencial, pero de importante propiedad intelectual o secretos comerciales.	Aplicaciones que contienen valiosa propiedad intelectual, secretos comerciales o secretos del gobierno (p. ej. en los Estados Unidos esto puede ser cualquier cosa clasificada en secreto o superior) que es fundamental 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.

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

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. 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	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 usuario (p. ej. información de contacto). Aplicaciones con cantidades pequeñas o moderadas de la funcionalidad de datos o de comprobación de pago	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 gran volumen de información sensible como números de tarjeta de crédito, nombres completos, documentos de identidad, etc.

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

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

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.

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.



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

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 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.

ASVS puede utilizarse mitigar esas carencias permitiendo a los arquitectos de seguridad elegir controles adecuados para problemas comunes



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

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

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.

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.



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

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)



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



SERIES DE LIDERAZGO DE SEGURIDAD:

Estrategias de seguridad para el éxito.

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.

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



SERIES DE LIDERAZGO DE SEGURIDAD:

Estrategias de seguridad para el éxito.

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.

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.

1. Centrarse en el equilibrio entre las necesidades de seguridad y de la experiencia de usuario.
2. Habilitar opciones flexibles de almacenamiento de datos, acceso y gestión.
3. Ofrezca un poderoso motor de políticas para controles contextuales.
4. Permitir una eficiente gestión del cumplimiento normativo y presentación de informes.
5. Reducir la superficie de ataque mientras bajan los costes de TI.



SERIES DE LIDERAZGO DE SEGURIDAD:

Estrategias de seguridad para el éxito.

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.

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.
2. Compromiso con las líneas de negocio de las organizaciones.
3. Vea las políticas de seguridad de forma moderna y móvil.
4. Aplique las políticas de forma apropiada y constantemente.
5. Automatizar la seguridad correctamente.



SERIES DE LIDERAZGO DE SEGURIDAD:

Estrategias de seguridad para el éxito.

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.

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.

Cada vez más auditores, reguladores, partners, y clientes están exigiendo pruebas defendibles de ese hecho.

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.
2. Controlar la información confidencial
3. Auditar, medir y demostrar el cumplimiento de la normativa.



8. 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.

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.

¿En que momento debemos considerar estos 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.

9. 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

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

10. 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.

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.

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

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.



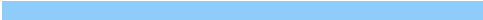
11. Procedimiento para el desarrollo de aplicaciones informáticas.



Procedimiento para el desarrollo de aplicaciones informáticas.

IDENTIFICACIÓN DEL PROCEDIMIENTO:

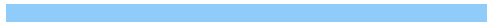
MACROPROCESO	PROCESO	SUBPROCESO
GESTIÓN DE DESARROLLO INSTITUCIONAL	GESTIÓN INFORMÁTICA	DESARROLLO DE APLICACIONES
PROCEDIMIENTO PARA EL DESARROLLO DE APLICACIONES		
AREA RESPONSABLE		DIRECCIÓN DE DESARROLLO DE TECNOLOGÍA
VERSION DEL DOCUMENTO		1.0
CÓDIGO		PRO-DDT-001



Procedimiento para el desarrollo de aplicaciones informáticas.


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.




Procedimiento para el desarrollo de aplicaciones informáticas.

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.
 - **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.
 - **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.
- 


Procedimiento para el desarrollo de aplicaciones informáticas.

DEFINICIONES:

- **BASE TÉCNICA:** Es la documentación técnica, definitiva y actualizada, a ser incluida en los pliegos de contratación.
 - **COMPLEJIDAD TÉCNICA:** Es el grado de dificultad técnica para la ejecución de una tarea específica.
 - **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.
 - **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.
- 

Procedimiento para el desarrollo de aplicaciones informáticas.

DEFINICIONES:

- **MANUAL TÉCNICO:** Es un documento que contiene información técnica del aplicativo informático.
 - **PROCESOS INSTITUCIONALES ESTANDARIZADOS:** Un proceso constituye un conjunto de actividades con entradas (insumos) y salidas (entregables, resultados) que permiten obtener un producto o servicio.
 - **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.
- 

PROCEDIMIENTOS

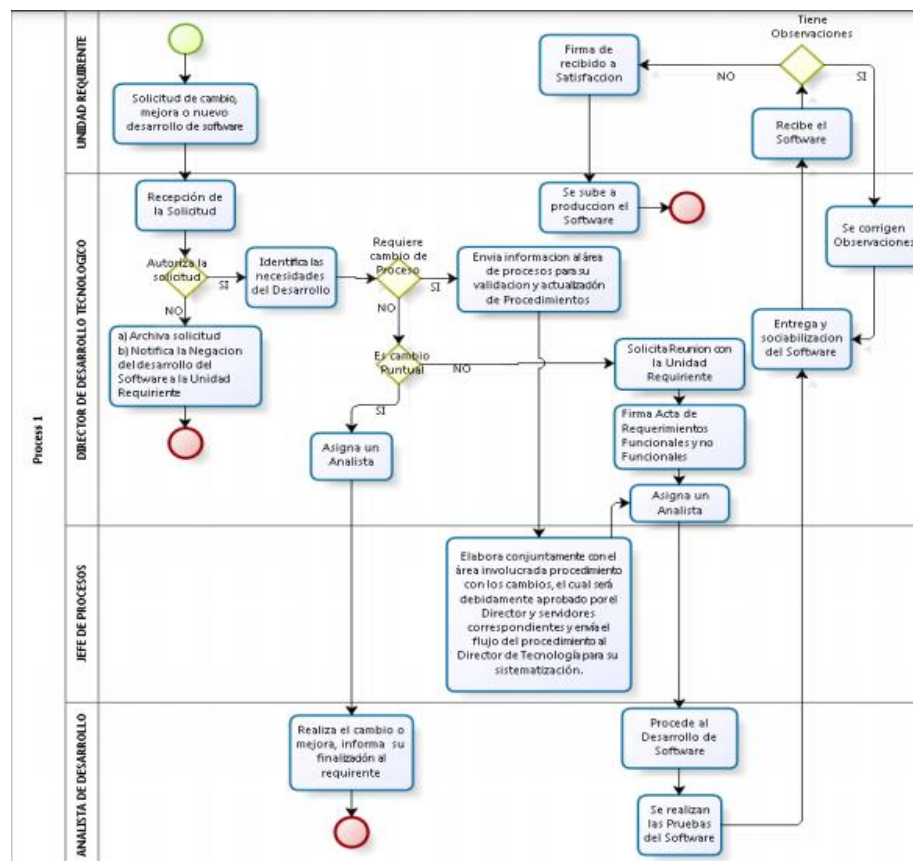
Procedimiento para solicitud de cambios, mejoras o nuevo desarrollo de un aplicativo informático.

No.	Asigna un analista para el desarrollo del requerimiento
1	Ingresa vía sistema la “Solicitud de cambio, mejora o nuevo desarrollo de software”, que se encuentra en la intranet institucional.
2	<p data-bbox="102 191 1222 223">Recepta la solicitud y analiza el impacto del cambio solicitado sobre un el aplicativo informático</p> <p data-bbox="102 289 363 322">¿Autoriza la Solicitud?</p> <p data-bbox="102 387 618 420">SI: Identifica las necesidades del desarrollo.</p> <p data-bbox="102 485 1477 518">NO: Envía respuesta vía correo electrónico al director requirente indicando el motivo de la no viabilidad del proyecto.</p>
2.1	<p data-bbox="102 521 469 554">¿Requiere cambio en proceso?</p> <p data-bbox="102 620 401 653">NO: ¿Es cambio puntual?</p> <p data-bbox="102 718 1636 751">SI: Autoriza a realizar los cambios o mejoras puntuales sobre un aplicativo, que no incurra en cambios significativos en el proceso</p> <p data-bbox="102 816 1812 849">NO: Solicita reunión con el área requirente, genera un acta de requerimientos funcionales y no funcionales, y define el tiempo de entrega. Paso 4</p> <p data-bbox="102 915 1889 975">SI: Envía información al área de procesos 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</p>

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 días
5	<p>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.</p> <ul style="list-style-type: none"> • 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 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. <p>b) Realiza las pruebas del software, coordinando una reunión con el Usuario experto de la unidad requirente.</p> <p>c) Genera una social</p>	Plan de Gestión	Analista de Desarrollo Tecnológico	

6	<p>Recibe el aplicativo informático.</p> <p>¿Tiene observaciones?</p> <p>SI: Envía las observaciones a la Dirección de Tecnología para que efectúen las correcciones del caso Mediante Correo Electrónico institucional.</p> <p>NO: Firma un Acta de Recepción a conformidad</p>	Acta de recepción y conformidad (Que es parte del Acta de requerimientos funcionales)	Director requirente o su delegado	2 días
7	<ul style="list-style-type: none"> Coloca los entregables (documentación, código fuente, etc.) en los diferentes 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. 		Director de Desarrollo de Tecnología	15 días
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

FORMATOS DE REGISTRO.

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

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



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

La finalidad es establecer los lineamientos y definir los artefactos para la entrega en producción de todos los nuevos servicios de tecnología o sus actualizaciones, que faciliten su gestión, administración y mantenimiento.

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

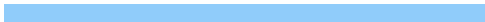
El protocolo describe los lineamientos a cumplir para nuevas soluciones y actualizaciones y aplica desde el inicio de su implementación hasta la salida en productivo y entrega a la operación de la misma.



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

Se describen los roles que interactúan en el proceso, y las responsabilidades asociadas a cada uno:

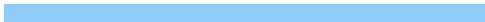
- El Coordinador de Aplicaciones y/o Coordinador de Infraestructura es el encargado de asegurar la aprobación de paso a producción de las soluciones tecnológicas adquiridas.
- El líder técnico se encarga de coordinar con el proveedor de la solución la entrega acorde a los requisitos de este documento, se encarga de gestionar con el coordinador que corresponda, la aprobación para el paso a producción y se encarga de gestionar y coordinar con el proveedor o área funcional
- El Change Manager es el responsable de verificar la solicitud de paso a producción, de garantizar el flujo y ejecución del RFC
- El líder Funcional es el responsable de validar y dar conformidad al cumplimiento de los requerimientos funcionales.



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

Se describen los roles que interactúan en el proceso, y las responsabilidades asociadas a cada uno:


- El operador se divide en 3 perfiles
 - El especialista de Aplicaciones es el responsable de validar y dar conformidad a la aplicación y el encargado de hacer el despliegue de la aplicación en el ambiente de producción
 - El especialista de Base de Datos es el responsable de validar y dar conformidad a la base de datos y se encargada de hacer el despliegue de base de datos en el ambiente de producción.
 - El especialista de Seguridad es el responsable de verificar que la aplicación cumpla con las políticas de seguridad.
- I. El proveedor es el responsable de la entrega de la solución actualizada o nueva.
- II. El coordinador es el responsable de aprobar el pase a producción y es el administrador de verificar el cumplimiento del protocolo.
- III. El líder técnico es el responsable de verificar el cumplimiento de protocolo
- IV. El change manager y el operador son los informados que se verifico el cumplimiento del protocolo.
- V. El usuario final es el que consulta la verificación del cumplimiento del protocolo.



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

Requisitos para la entrega de nuevas aplicaciones en productivo.

Se indican los requisitos que se deben cumplir para entregar en productivo las nuevas aplicaciones.

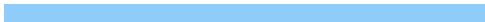
- ✓ Las pruebas funcionales y técnicas son de ambiente de certificación y producción.
 - ✓ El inventario de aplicaciones son de ambiente de certificación y producción.
 - ✓ Las fuentes o medios de instalación de la aplicación son de ambiente de certificación y producción.
 - ✓ El manual técnico es de ambiente de producción.
 - ✓ El manual de instalación tiene los 3 ambientes, que son de pruebas, certificación y producción.
 - ✓ La Arquitectura de la aplicación es de ambiente de producción.
 - ✓ El manual de usuario es de ambiente de producción.
 - ✓ El diagrama entidad-relación es de ambiente de producción.
 - ✓ El sizing es de ambiente de pruebas, certificación y producción.
 - ✓ Las pruebas de carga y stress es de ambiente de certificación y producción.
 - ✓ Las pruebas de seguridad es de ambiente de certificación y producción.
 - ✓ Los backups es de ambiente de pruebas, certificación y producción.
 - ✓ Los servicios monitoreados es de ambiente de certificación y producción.
 - ✓ La categorización de la aplicación es de ambiente de producción.
- 

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

Requisitos para la entrega de nuevas aplicaciones en productivo.

Se indican los requisitos que se deben cumplir para entregar en productivo las nuevas aplicaciones.

- ✓ El licenciamiento es de ambiente de producción.
- ✓ Las cuentas y contraseñas de usuarios son de ambiente de certificación y producción.
- ✓ La gestión de vulnerabilidades es de ambiente de certificación y producción.
- ✓ La gestión de blacklog es de ambiente de certificación y producción.
- ✓ El plan de recuperación tecnológica es de ambiente de certificación y producción.
- ✓ IPV6 es de ambiente de pruebas, certificación y producción.
- ✓ Los tiempos de logueo para aplicaciones nuevas son de ambiente de certificación y producción.
- ✓ Los Diagramas DSI son de ambiente de pruebas, certificación y producción.
- ✓ El ingreso al almacén es de ambiente de pruebas, certificación y producción.
- ✓ La actualización de línea base APP es de ambiente de certificación y producción.
- ✓ La actualización de archivos en la intranet es de ambiente de certificación y producción.

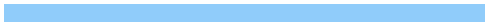


PROTOCOLO – PASO A PRODUCCIÓN PARA LA ENTREGA DE PRODUCTO DE NUEVAS SOLUCIONES TECNOLÓGICAS

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

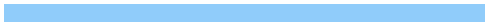
1. Inventario: Entregar el inventario o relación de la infraestructura con mínimo los siguientes ítems:

- 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



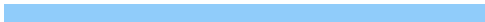
PROTOCOLO – PASO A PRODUCCIÓN PARA LA ENTREGA DE PRODUCTO DE NUEVAS SOLUCIONES TECNOLÓGICAS

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.
3. Manuales Administración: El documento debe contener instructivos para la administración del elemento según su rol.
4. Ingeniería: En este documento debe contener la arquitectura detallada así:
 - a) Arquitectura de la solución (esquema de red (físico y lógico, 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



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

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.
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. 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.
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



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

9. Cuentas y contraseñas de Usuarios: Entregar los usuarios y contraseñas en sobre sellado de: ROOT, Administrador, y consulta.
10. Capacity Planing; Análisis y estadísticas de uso de los recursos que componen la solución
11. Licenciamiento: Entregar los acuerdos de licenciamiento suscritos con los proveedores de Hardware y software que compone la solución.
12. Garantía: Contratos de soporte y garantía de cada elemento de la solución.
13. Gestión de Vulnerabilidades: Entregar informe de los últimos tres (3) meses del escaneo de vulnerabilidades y mitigación pertinente de la plataforma a entregar.
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.



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

15. Plan de Recuperación Tecnológica: 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 | e) Metodología utilizada |
| b) Objetivos | f) Resumen ejecutivo |
| c) Alcance | g) Procedimiento de recuperación |
| d) Fecha de realización | h) Tiempos de recuperación |

16. IPV6: Configuración dentro de la infraestructura del protocolo IPV6.

17. Arquitectura: Entrega de la arquitectura en donde se asegure un esquema de alta disponibilidad y full tolerancia.

18. Ingreso a Almacén: Entregar el certificado de ingreso a almacén del Ministerio.

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

- Capacitación
 - Matriz de escalamiento
 - Árbol de tipificación de la herramienta de gestión
 - Catálogo de Servicios
 - Tiempo de respuesta.
 - Base de Datos del conocimiento.
- 



Gracias!

TECNOLOGÍAS DE SEGURIDAD EN SOFTWARE.

DOCENTE: DÍAZ RINCÓN HILDA.

ALUMNO Y N° CONTROL:

ALDAMA MÁRQUEZ JOEL JAIR - 15251870.

GRUPO: T91.

ACTIVIDAD: 3.1 Controles en Aplicaciones en
producción

- 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*. Magazciturum. <https://www.magazciturum.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

Referencias.

- Pérez Estes, 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>

Referencias.
