Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

# Memorias Científicas de

# Congreso Internacional de DESARROLLO DE SOFTWARE

ISBN: 978-9942-759-94-8

Instituto Superior Tecnológico del Azuay
**Cuenca, Ecuador**

24 - 25 - 26 octubre 2018

# MEMORIAS CIENTÍFICAS DEL CONGRESO INTERNACIONAL DE DESARROLLO DE SOFTWARE

# Memorias científicas del Congreso Internacional de Desarrollo de Software

Compiladores:

Ing. Daniela Fernanda Armijos Chillogallo Mgt.

Ing. Vinicio Estuardo Iñiguez Morán Mgt.

Ing. Jessica Priscila Herrera Urgilés Mgt.

Ing. María Gabriela Aguirre Vicuña Mgt.

ISBN: 978-9942-759-94-8

Edición con fines académicos no lucrativos.
Impreso y hecho en Ecuador

Diseño y Tipografía: Lic. Pedro Naranjo Bajaña



Centro de Investigación y Desarrollo Ecuador
Cdla. Martina Mz. 1 V. 4 Guayaquil, Ecuador
Tel.: 00593 4 2037524
http.:/www.cidecuador.com

# CONTENIDO

# PRESENTACIÓN DE LAS MEMORIAS CIENTÍFICAS DEL CONGRESO INTERNACIONAL DE DESARROLLO DE SOFTWARE

El Instituto Superior Tecnológico del Azuay en coordinación con el Centro de Investigación y Desarrollo Ecuador (CIDE) y el Centro de Estudios Transdisciplinarios (CET) Bolivia, convocaron a profesionales, profesores, estudiantes, e interesados en difundir y/o actualizarse en los avances de las diferentes líneas de investigación, a nivel nacional e internacional a participar en el CONGRESO INTERNACIONAL EN DESARROLLO DE SOFTWARE. Este Congreso fue un espacio de intercambio sobre las prácticas, metodologías, conocimientos e investigaciones en las diferentes áreas.

Con la participación de prestigiosos profesionales y expertos de diversas ramas y actividades, y mediante exposiciones, debates, sesiones plenarias y técnicas, los asistentes pudieron ampliar sus ya de por sí elevados conocimientos y obtener unas conclusiones que permitieron cumplir el objetivo pretendido por el Comité Organizador y el Científico, de ofrecer a los miembros de las instituciones y profesionales vinculados a las distintas temáticas a tratar. Fue un evento de especial interés y calidad para su desarrollo profesional.

Además de las actividades inherentes al Congreso, que contemplaron exposiciones orales y en modalidad de panel, se consideraron otras actividades adicionales sobre temas de relevancia y de actualidad, dentro de lo que se pueden mencionar: Ponencias Magistrales, Simposio, y eventos culturales, lo que brindó la oportunidad a los asistentes de complementar su visita a esta institución sobre otros temas de su interés. En cada una de sus especialidades, los conferencistas realizaron exposiciones del más alto nivel, de tal manera que sus intervenciones dirigidas a los diferentes sectores, sin duda alguna contribuyeron de manera importante al conocimiento de las diferentes temáticas tratadas.

# Conferencias:

# LA INTERFAZ DE SEGURIDAD EN MÉTRICA VERSIÓN 3 Y SU IMPLEMENTACIÓN A TRAVÉS DE LA FAMILIA DE NORMAS ISO/IEC 27000. UN CASO APLICADO EN UNA EMPRESA CERTIFICADA EN CMMI.

PhD. Francisco Javier Valencia Duque
**Universidad Nacional de Colombia**
fjvalenciad@gmail.com
fjvalenciad@unal.edu.co

**Resumen:**

Uno de los marcos de referencia más utilizados por las empresas de desarrollo de software para estandarizar sus procesos es Métrica, actualmente en su versión3, cuya alineación con estándares como la ISO 12207 – Information Technology Software life cycle processes- les ha permitido a diversas empresas su adopción y a partir de allí, obtener certificaciones tan importantes como CMMI. No obstante, el mercado exige además de contar con procesos estandarizados de software, la necesidad de garantizar adecuados niveles de seguridad de la información, no solo en los procesos de software, sino en los productos resultantes. En este sentido, Métrica establece como parte de sus interfaces, la Interfaz de Seguridad, la cual ante la exigencia del mercado a las empresas de desarrollo de software de certificar sus procesos y productos con la ISO/IEC 27001:2013, requiere ser complementada para garantizar adecuados niveles de Confidencialidad, Integridad y Disponibilidad de la información. La conferencia permitirá mostrar la experiencia en la implementación de un Sistema de Gestión de Seguridad de la Información – SGSI- de una empresa de desarrollo de software certificada en CMMI, la cual utiliza Métrica como parte de sus procesos y requiere para dar cumplimiento a requerimientos del negocio, certificarse en la norma ISO/IEC 27001:2013, sin desconocer la Interfaz de Seguridad que hace parte de la metodología del ciclo de vida de software incorporada a través de Métrica. Para ello se presentarán las principales normas de la familia ISO/IEC 27000 utilizadas en el proceso y la metodología y resultados obtenidos para lograr los fines propuestos.

**Descriptores claves**: Seguridad de la Información, Interfaz de Seguridad, Métrica, Seguridad en el ciclo de desarrollo de software, Aseguramiento de software.

# ASEGURAMIENTO DE TECNOLOGÍAS DE INFORMACIÓN. UNA PROPUESTA INTEGRADORA.

PhD. Francisco Javier Valencia Duque
**Universidad Nacional de Colombia**
fjvalenciad@gmail.com
fjvalenciad@unal.edu.co

**Resumen:**

El aseguramiento de las tecnologías de información y comunicaciones (TIC) es una disciplina que se construye a partir de la interrelación de la tríada riesgos-control-auditoría y que busca disminuir la incertidumbre que genera el uso de las TIC como recurso clave en la productividad y competitividad organizacional. Con tal perspectiva, se presenta un panorama general de los conceptos fundamentales del aseguramiento organizacional y tecnológico que sirven como insumo para la efectiva implementación de esta práctica en el ámbito empresarial. A partir de allí, se presenta la gestión de riesgos de tecnologías de información como el primer eslabón del aseguramiento, resumido en aquellos eventos adversos que bajo una probabilidad de ocurrencia pueden generar impactos en el cumplimiento de los objetivos de cualquier organización, para lo cual es necesaria la incorporación de controles en sus diferentes tipologías que permitan disminuir la probabilidad o el impacto y contar con niveles aceptables de riesgo, de acuerdo al apetito de riesgo definido por la organización. No obstante, el simple hecho de incorporar controles no es suficiente, se requiere desarrollar procesos de auditoria a dichos controles, para garantizar que se encuentren adecuadamente diseñados y que cumplan con los objetivos previstos, y por ende el nivel de vulnerabilidad de la organización frente a los riesgos estén bajo control.

**Descriptores claves**: Aseguramiento tecnológico, Riesgos, Control, Auditoria.

# CLOUD COMPUTING, MONITORIZACIÓN Y CALIDAD DE SERVICIOS.

Dra. Irene Priscilla Cedillo Orellana
**Universidad de Cuenca**
iprisy@hotmail.com
Priscila.cedillo@ucuenca.edu.ec

**Resumen:**

La computación en la nube permite proveer servicios atractivos a las organizaciones, éstos se derivan de sus características particulares (autoservicio bajo demanda, elasticidad, modelo multi-huésped, pago por uso, escalabilidad, entre otras); sin embargo, existen muchos desafíos relacionados al aprovisionamiento de los servicios, específicamente centrados en la calidad de servicio, la misma que debe ser pactada entre clientes y proveedores. Por medio de los acuerdos de nivel de servicio (SLA), las características tanto funcionales como no funcionales son especificadas, pero muchas veces éstas no son provistas de manera adecuada, dejando al cliente la ardua tarea de comprobar el cumplimiento de la oferta, a fin de realizar los reclamos respectivos. De ahí, nace la necesidad de conocer el estado actual de los servicios provistos a fin de proveer herramientas de control y monitoreo, que retroalimenten al proveedor y sean un instrumento de verificación y cumplimiento para el cliente.

**Descriptores claves:** Nuevas tecnologías, Servicios, Service Level Agreenments, Niveles de servicio, Tendencias Cloud Computing.

# APLICAR EXITOSAMENTE UN CICLO DE DESARROLLO SEGURO DE APLICACIONES.

Ing. Carlos Alcides Gonzales Fung
**INTELINTECH**
cagofu@gmail.com
cgonzales@intelitech.com.pe

**Resumen:**

A lo largo de la historia de la evolución de las tecnologías de información, la seguridad casi siempre ha sido un aspecto rezagado. Es habitual que primero pensemos en la funcionalidad y luego, cuando alguna tecnología ya fue desplegada y tengamos evidencias de que hay vulnerabilidades, nos preocupemos de la seguridad. En el desarrollo de aplicaciones también ocurre: algo sucede en el desarrollo del software o aplicaciones, que termina finalmente en una vulnerabilidad y personas mal intencionadas (como algunos hackers) están al acecho para aprovecharse. Objetivo: Presentar las principales prácticas, metodologías y estrategias que permitan producir aplicaciones seguras a través de la ejecución de un ciclo de desarrollo seguro. De esta manera, lograr que toda nueva aplicación o software desarrollado tenga un adecuado nivel de seguridad. Metodología: Se abordará los temas siguientes presentando en cada uno de ellos su base de conocimiento, ejemplos y recomendaciones:
1) Principales Casos
2) La resistencia a aplicar la seguridad
3) Metodologías y prácticas aplicables al Ciclo de Desarrollo
4) Estrategias para aplicar las metodologías y prácticas. Factores de éxito.
Conclusiones: Sí es posible desarrollar aplicaciones seguras. Sin embargo, debemos estar dispuestos a cambiar e incluir actividades en nuestro ciclo de desarrollo para lograr un producto seguro. Hay que romper paradigmas y vencer la resistencia en las personas. En un futuro, podríamos decir, si nos proponemos, que toda nueva solución tecnológica este a la par con su seguridad.

**Descriptores claves**: Seguridad, Aplicaciones, Ciclo

# PRINCIPALES VULNERABILIDADES EN APLICACIONES Y CÓMO EVITARLAS.

Ing. Carlos Alcides Gonzales Fung
**INTELINTECH**
cagofu@gmail.com
cgonzales@intelitech.com.pe

**Resumen:**

A lo Aplicar malas prácticas de desarrollo seguro conlleva la aparición de vulnerabilidades en aplicaciones. Asimismo, a lo largo del tiempo, van apareciendo nuevas vulnerabilidades que genera oportunidades a los atacantes para afectar nuestras aplicaciones y como consecuencia, el activo más valorado: la información. Objetivo: Presentar las principales vulnerabilidades que se presentan en aplicaciones, cómo se producen, cómo se detectan, qué consecuencias pueden generar, y finalmente cómo podemos evitarlas o remediarlas. Metodología: Se abordará los temas siguientes presentando en cada uno de ellos su base de conocimiento, ejemplos y recomendaciones: Conclusiones: El desarrollo de aplicaciones va evolucionando con el trascurrir del tiempo, por ello hay que estar siempre alertas a los nuevos casos y formas cómo se producen vulnerabilidades en nuestras aplicaciones. De esta manera podemos, en forma preventiva, evitarlas y hacer que nuestras aplicaciones sean seguras.

**Descriptores claves**: Seguridad, Aplicaciones, Vulnerabilidades.

# PROCEDIMIENTO PARA LA EVALUACIÓN DE LA CONFORMIDAD DE LOS PRODUCTOS INFORMÁTICOS. CASO DE ESTUDIO FACULTAD DE INFORMÁTICA Y MATEMÁTICA DE LA UNIVERSIDAD DE HOLGUÍN.

MSc. Yasnalla Rivero Peña
**Universidad de Holguín**
yasnidf@gmail.com
yasnalla@uho.edu.cu

**Resumen:**

En la actualidad, el desarrollo de software en la Facultad de Informática y Matemática de la Universidad de Holguín, presenta dificultades para evaluar la calidad y conformidad de los productos informáticos elaborados para el correcto funcionamiento. En este sentido solo se realizan acciones aisladas, debido a que se prioriza el cumplimiento de los plazos pactados con el cliente. Esto provoca que se aparte la atención de la realización de un conjunto de pruebas para detectar las no conformidades y que no sean evaluados utilizando métricas de calidad con objetividad, generando problemas en cuanto a la utilidad del software y por ende la satisfacción del cliente. Con el objetivo de lograr el aseguramiento de una calidad adecuada en este proceso, se propone un procedimiento para la evaluación de la conformidad a partir de la medición de las características de calidad en iteraciones de pruebas tempranas. Para ello se toman como referencias normativas la norma internacional para evaluar la conformidad (NC-ISO/IEC: 17000 2005), evaluación de software (ISO/IEC: 14598) y el modelo de calidad (NC-ISO/IEC: 9126). El procedimiento se sustenta en una herramienta informática que sirve de apoyo a los evaluadores en el cálculo de las métricas asociadas a las características evaluadas. La propuesta realizada fue valorada a partir de la aplicación del criterio de expertos y la aplicación práctica, en el Grupo de Procesamiento de Datos Biomédicos (GPDB) y en la Empresa Nacional de Proyectos e Ingeniería (ENPA). Con el primero de los métodos valorativos empleados todos los aspectos fueron evaluados de muy relevantes y la aplicación práctica también arrojó buenos resultados lo que permite asegurar el cumplimiento del objetivo propuesto en la investigación.

**Descriptores claves**: Calidad, evaluación de la conformidad, medición, métricas.

# SOFTWARE EDUCATIVO PARA LA ENSEÑANZA DEL PROCESO DE MEDICIÓN DE LA CALIDAD DE SOFTWARE. EXPERIENCIA PRÁCTICA CON EL USO DEL ASISTENTE METRIC_CAL.EXE PARA EL CÁLCULO DE LAS MÉTRICAS DE CALIDAD.

MSc. Yasnalla Rivero Peña
**Universidad de Holguín**
yasnidf@gmail.com
yasnalla@uho.edu.cu

**Resumen:**

La evaluación de la calidad es uno de los procesos en el ciclo de vida de desarrollo de software donde se deben planificar, organizar, dirigir y controlar una serie de actividades; con el objetivo de asegurar que el producto aporte la calidad requerida y satisfaga las necesidades del cliente. En este trabajo se aborda la descripción de la herramienta Metric_calc.exe como apoyo al proceso de enseñanza y aprendizaje de los temas de calidad en la Ingeniería de Software, imprescindible en el proceso de formación de los ingenieros informáticos. La guía de las prácticas probadas y la metodología de la realización de esta se realizaron siguiendo el modelo pedagógico del Aprendizaje Basado en Problemas, ABP, con adaptaciones especiales para la ingeniería.

**Descriptores claves**: Calidad, métricas, software educativo, aprendizaje basado en problemas.

# METODOLOGÍAS DE DESARROLLO DE ADD-ON PARA ERPS CORPORATIVOS.

Ing. Carlos Carrion R
**CIP GmbH**
CCarrion.Akrata@gmail.com
Ccarrion.CIP@CatedraLibre.org

**Resumen:**

Al ser ERP SAP líder mundial en desarrollar software aplicativo de negocios para la gestión operativa a nivel general y alcance mediano y multinacional de las empresas en casi todos los sectores económicos y en entornos diversos, por más de 35 años; ha conducido a la externa programación de módulos complementarios (Add-On) para cumplir características especiales de negocios particulares en sus clientes. Las normas de diseño, programación e implantación de soluciones de software en las organizaciones han ido evolucionando y los grandes centros de desarrollo (Software Factory) han dado las pautas con casos y situaciones acontecidas en las grandes y medianas corporaciones; a los niveles de innovación tecnológica y esfuerzos de instituciones normativas y particulares (Software Libre y OpenSource); que van desde el ciclo SDLC, OOD, RIMA. Según las vivencias de cada fabricante de software, las características particulares e innovadoras de los negocios, casos suscitados de problemas y el equipo de técnicos respectivos se han ido adaptando y aportando iniciativas para establecer la medición del nivel de confiabilidad, las mejores prácticas y seguimiento BSC aparte de esquemas gráficos de representación (datos DFD, procesos, entidades, relaciones, estados, modelos), mejoras de los manejadores de Bases de Datos DBMS, ampliación a accesos web/móvil, mejoras del hardware con virtualización e Hyperconvergencia, y nuevos lenguajes de programación que la comunidad de programadores y especialistas se van agrupando; produciendo resultados de su trabajo. Concluyendo que no solamente con la dotación de IDE adecuado para desarrollar módulos se puede programar o mejorar lo actualmente entregado, sino que adoptando renovadas metodologías del ciclo de desarrollo SDLC con herramientas de diagramación DFD, pruebas automáticas y modelamiento funcional, el futuro del desarrollo de software seguirá incorporando e innovando con el avance web/móvil; sea privado o software libre.

**Descriptores claves**: Add-On, ERP, IDE, DFD, SDLC.

# CATEGORIZACIÓN Y GESTIÓN DE FALLA, DEFECTO Y ERROR EN EL DESARROLLO DE SOFTWARE SEGÚN NORMAS SDLC Y MEJORES PRÁCTICAS DE FABRICANTES.

Ing. Carlos Carrion R
**CIP GmbH**
CCarrion.Akrata@gmail.com
Ccarrion.CIP@CatedraLibre.org

**Resumen:**

Incluyendo software desarrollado y programado por herramientas CASE más prestigiosas en ambiente productivo para sectores de alta demanda y gran cantidad de información se presentan casos en los mismos clientes, que aparte de mala publicidad puede y ha llevado a aplicar demandas judiciales. Entre los niveles más críticos de sistemas o soluciones ERP figuran de Seguridad y Defensa, Financiero Bancario y Gestión de Salud, lo cuales han dado cabida a Software Factory de desarrollar a gran escala y multinacional sus aplicaciones que han ido evolucionando en versiones, revisiones (release), dando lugar a niveles de satisfacción y costo de sus soluciones en los clientes corporativos, medianos y pequeños según su actividad económica. A raíz de las tolerancias que los sistemas han permitido a los hackeadores que además de penetrar a los datos en ciertos casos de empresas e instituciones, han trasladado, modificado e incluso secuestrado dicha información (ransomware) siendo las víctimas sus clientes, cada gran solución privada y software libre han implementado comunidades de prueba, de investigación que día a día reportan vulnerabilidades que se confirman y resuelven a través de parches, cambios o espera de nuevas versiones. Pero muchas veces por el origen de la situación o niveles de alto riesgo (ocurrencia y consecuencia) los programadores y especialistas en algunos casos no han logrado superar estos inconvenientes, haciendo que prescriban sus soluciones, vean reducir su interés en los clientes o solo enviando mensajes a una porción del universo de clientes, como sucedió por ejemplo con la comunidad SAP para evolucionar a SAP HANA en 2007 o como la comunidad de desarrolladores en Rusia inicio en 2012 la campaña de mejoramiento de Calidad de Software a raíz de confirmar la Falla de MS Excel. El objetivo de notar la diferencia entre Falla, Defecto y Error que en las etapas del Desarrollo de Software SDLC se presentan y en la vida real se debe contemplar para actuar acorde a los niveles de criticidad e impacto en el tiempo.

**Descriptores claves**: Falla, Defecto, Error, SDLC, Software Factory, Categorización, CASE.

# TÉCNICAS DE PROGRAMACIÓN SEGURA EN PHP.

Msc. Joffre Monar Monar
**ESPOCH**
jmonarm@yahoo.es
jmonar@espoch.edu.ec

**Resumen:**

Actualmente, la gran mayoría de aplicaciones web contienen vulnerabilidades de seguridad. Probablemente, se deba a falta de cultura de los desarrolladores o a la ausencia de técnicas de codificación específicas. Se analizan varios trabajos relacionados al tema, pero no definen técnicas de programación precisos, ni se enfocan a un lenguaje de programación específico. Se propone un conjunto de técnicas de programación segura para reducir las vulnerabilidades en las aplicaciones web utilizando el entorno de desarrollo PHP. Para esto se determinan diez vulnerabilidades usando las recomendaciones OWASP TOP-10. De éstas, se plantean siete técnicas que se consideran más críticas y su respectiva forma de implementarlas. Para definir la propuesta se tomó como base las recomendaciones de: TOP-10 Controles Proactivos, la Guía de Pruebas OWASP, así como los Controles Estándar de Seguridad (ASVS); todo esto implementado con las técnicas de programación de PHP.

La seguridad fue determinada mediante el nivel de protección de la aplicación web contra las vulnerabilidades más conocidas, es decir, el número de vulnerabilidades altas, medias y bajas detectadas utilizando Acunetix Vulnerability Scanner. Se valida las técnicas propuestas y se mide las vulnerabilidades de una aplicación web en dos escenarios; con y sin la implementación de las técnicas propuestas. Los resultados mostrarán que el uso de las técnicas propuestas se relaciona significativamente con la cantidad de vulnerabilidades encontradas y por lo tanto mejora el nivel de seguridad de las aplicaciones web en entornos PHP. El principal aporte de esta investigación es proponer treinta y cinco técnicas de programación segura organizada en siete grupos, las cuales se enfocan a evitar algunos de los errores muy comunes en programación, tales como: validación de entradas, gestión de sesiones, cifrado de datos, Cross Site Scripting (XSS), instalación y configuración incorrecta del servidor web y base de datos, y CSRF. Por lo que se logra reducir el riesgo de recibir ataques informáticos en las aplicaciones web.

**Descriptores claves**: Vulnerabilidades, OWASP, PHP, programación segura, técnicas

# DEVOPS UN NUEVO CONCEPTO DE LA INGENIERÍA DE SOFTWARE.

MSc. Mayra Alejandra Oñate Andino
**ESPOCH**
alejandraonate.a@gmail.com
Mayra.onate@espoch.edu.ec

**Resumen:**

El desarrollo de software seguro es un asunto de alta importancia en las organizaciones, pues estas dependen de sus sistemas informáticos para su operación diaria más cuando son sistemas críticos. Si bien es importante asegurar que el software se desarrolla de acuerdo a las necesidades del usuario, también lo es garantizar que el mismo sea seguro. Hasta hace poco tiempo la Ingeniería de Software y la Ingeniería de Seguridad venían desarrollándose de forma independiente, limitando la posibilidad de que la seguridad sea considerada como parte del proceso de desarrollo de sistemas de software seguros, paradigma que actualmente se ha roto, y para garantizar un software de calidad uno de los requerimientos importantes es la seguridad. Pero hablar de seguridad no es solamente hablar de un producto sino más bien es la sumatoria de personas, procesos y tecnología. En este contexto, DevOps es una respuesta a la interdependencia del desarrollo de software y las operaciones TI, hablaremos entonces de los aspectos más relevantes de DevOps y Desarrollo de Software Seguro, principios, metodologías, buenas prácticas, que permitan vincular el desarrollo y las operaciones de TI, y ayuden a una organización a producir productos y servicios software más rápidamente, de mejor calidad y a un coste menor.

**Descriptores claves**: Desarrollo, Software, Sistemas, Seguridad, DevOps.

# Ponencias:

# EL ENTORNO VIRTUAL COMO ELEMENTO INTERACTIVO: APLICAR DESTREZAS COGNITIVAS A PARTIR DE LAS HERRAMIENTAS DE LA TECNOLOGÍA, LA INFORMACIÓN Y LA COMUNICACIÓN CON SOFTWARE FREE.

Lic. Miguel Antonio Álvarez Lazo
**Unidad Educativa Particular Corel**
miguel.alvarezl@ucuenca.ec
u.e.corel@hotmail.com

**Resumen:**

La modernidad trajo consigo a la sociedad humana un conglomerado de cambios y transformaciones que afectaron directamente a su estructura social, política, económica o de educación y su modelo. Sobre este último apartado, la educación supera con creses a la forma tradicional de la enseñanza que, al verla, desde estos tiempos cada vez más modernos, aflora un nuevo paradigma con un tinte de multimodalidades que van desde lo presencia hasta el momento del aula virtual con las vicisitudes que circunda en las Tic como territorio del aprendizaje educativo. Por esta razón, las Tic surgen como una necesidad de integración creativo que permite explorar las distintas capacidades cognitivas en plataformas virtuales, el software free y las apps. Bajo este proceso, la mirada es innovadora. El gran proyecto de aula es asumir este reto, desde allí que, el presente trabajo tiene por finalidad exponer la virtud que trae consigo un cambio educativo basado en el uso de herramientas de enseñanza virtual y el software free. Fue decidor el periodo lectivo 2017-2018 en la Unidad Educativa Particular COREL desde el área de Computación en los cursos de octavo, noveno y décimo de Educación General Básica en el que para el soporte de los resultados se aplicó un sondeo de preferencias entre el uso de programas convencionales: Word, Excel y Power Point frente a la integración de programas con disposición free en Prezi, Powtoon y Duolingo.

**Descriptores claves:** Aprendizaje de máquina, desarrollo guiado por pruebas, pruebas unitarias, Python, visión por computador.

# METODOLOGÍA PARA DEFINIR EL CONJUNTO DE CONDICIONES MÍNIMAS Y NECESARIAS, PARA LA DETECCIÓN DE ERRORES EN CÓDIGO, BAJO FILOSOFÍA TDD, EN MARCO DE UNA APLICACIÓN PARA DETECCIÓN DE OBJETOS POR CARACTERÍSTICAS MORFOLÓGICAS.

PhD Mauricio Holguín Londoño[1]
PhD. Germán Andrés Holguín Londoño[2]
Tecnólogo. Juan Felipe Grajales González[3]
**Universidad Tecnológica de Pereira**

1. mau.hol@utp.edu.co
2. clsantacruzc@ucacue.edu.ec
3. juafelgrajalesg@gmail.com

**Resumen:**

Es requisito implícito en el trabajo de todo programador producir código con características de mantenibilidad, estabilidad, usabilidad, comprobabilidad, legibilidad, seguridad, entre otros aspectos. La introducción de la inteligencia artificial conlleva la implementación de códigos no convencionales, como por ejemplo los algoritmos relacionados con la visión por computador. En un escenario ideal, el desarrollador debería enfocarse únicamente en los ajustes relacionados con su propia metodología, y no en depurar el código de las funcionalidades básicas, por lo cual es necesario mitigar el riesgo de errores de naturaleza humana. Una forma de mitigar dichos errores es utilizando la filosofía de TDD, esto es: crear proposiciones lógicas de validez, y luego desarrollar el código necesario para cumplir con la lógica propuesta. En resumen, este trabajo plantea y define un método que utiliza TDD para el cumplimento satisfactorio de la tarea de escribir los bloques de código fuente, o funciones, dentro del marco de las aplicaciones de reconocimiento de patrones, específicamente, la clasificación de imágenes basada en características morfológicas. El resultado, es una metodología robusta y confiable para el proceso de desarrollo donde el programador se enfoca en el problema de aprendizaje de máquina y el usuario final obtiene un producto de software robusto.

**Descriptores claves:** Multimedia, herramienta didáctica, sistemas motivacionales

# PRACTICAS DE SEGURIDAD APLICADAS A ESCENARIOS DE AUTENTICACIÓN.

MSc. Andrés Santiago Jadan Montero
**Instituto Superior Tecnológico del Azuay**
Asjm123@gmail.com
ajadan@institutos.gob.ec

**Resumen:**

La autenticación en los sistemas informáticos se encarga de verificar la identidad de un usuario que está solicitando acceso a un servicio para con esto proceder a autorizar o no el uso de los servicios. Existen varios esquemas de autenticación en la actualidad los cuales son implementados según sea el nivel de seguridad requerido y el tipo de sistema informático. Sin importar el esquema que se vaya a utilizar es necesario asegurar que este tenga un funcionamiento óptimo ajustándose a los requisitos operativos, funcionales y de seguridad que sean requeridos por el sistema informático o la organización involucrada. El objetivo de este trabajo es analizar escenarios en los que se aplica un esquema de autenticación y presentar un catálogo de buenas prácticas que puedan ser usadas para llevar a cabo una implementación segura de cada esquema.

**Descriptores claves:** Autenticación, Seguridad, Doble Factor de Autenticación, Federación de Identidad.


ISBN: 978-9942-759-94-8