ILUMINATE

ISSN 2415 - 2323

La Salle Universidad Bolivia

VOLUMEN 14 | SEPTIEMBRE 2023

INGENIERÍA DE SISTEMAS

PROPUESTA DE BUENAS PRÁCTICAS PARA EL DESARROLLO SEGURO DE SOFTWARE CON DEVSECOPS Y SECURE SCRUM

GAMIFICACIÓN: UNA FORMA DIVERTIDA DE APRENDER

INTRODUCCIÓN A LA ARQUITECTURA DE MICROSERVICIOS

LA IMPORTANCIA DE LA SEGURIDAD PERIMETRAL LOGICA EN LAS ORGANIZACIONES EN BASE A LA NORMATIVA ISO 27001

SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD AYER, HOY Y MAÑANA

CONTROLES DE SEGURIDAD DE LA INFORMACIÓN BASADOS EN RIESGOS GENERADOS POR LOS USUARIOS FINALES

ANÁLISIS COMPARATIVO CON LA NORMA ISO 27032, NORMAS DEL SISTEMA FINANCIERO Y LOS REQUISITOS MÍNIMOS DE SEGURIDAD PARA LOS SERVICIOS DE BANCA DIGITAL.

Solución de un problema inverso de optimización aplicando el criterio del Hessiano

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN MÈDICA

DISEÑO DE UN MODELO DE CONTROL PID PARA UN SISTEMA BALL AND BEAM

El Teletrabajo: ¿Oportunidad o Amenaza?

SEGURIDAD EN EL CONTROL DE ACCESOS BASADO EN EL REGLAMENTO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y EL ESTÁNDAR PCI DSS PARA PROCEDIMIENTO OPERATIVOS

EXPLOIT "DIA CERO"

REVISTA DE INVESTIGACIÓN
ILUMINATE, 14ª Edición

Impresión: Universidad La Salle

Depósito Legal: 4-3-28-09

ISSN 2415-2323

Dirección: Calle Jorge Carrasco, esquina Las Palmas, No 450

Teléfonos: 2723588, 2723598

e-mail: oyokosaki@ulasalle.edu.bo

Visibilidad
Indexada en Revistas Bolivianas

Septiembre de 2023

La Paz- Bolivia

EDITORIAL

En la encrucijada de la era digital, nos encontramos en un momento donde el avance vertiginoso de la tecnología nos ofrece más que simples herramientas o gadgets de entretenimiento. Estamos inmersos en un mundo donde la ingeniería de sistemas ha trascendido fronteras, remodelando no sólo nuestras rutinas diarias, sino también la estructura misma de nuestras sociedades y economías. La 14ª edición de la revista Iluminate busca ser una ventana a ese universo en constante evolución. La ingeniería de sistemas, desde sus inicios, prometía una revolución en cómo interactuamos, trabajamos y jugamos. No obstante, incluso los visionarios de antaño podrían sorprenderse al ver la magnitud de las metamorfosis que esta disciplina ha generado. Esta revolución no ha sido simplemente tecnológica, sino también conceptual, modificando nuestra percepción del mundo y redefiniendo nuestros roles dentro de él.

Ahora bien, como toda disciplina que avanza a pasos agigantados, la ingeniería de sistemas requiere de una introspección y reflexión constante. Necesitamos entender no solo cómo funcionan estas innovaciones, sino cuál es su impacto, sus potenciales riesgos y beneficios, y cómo pueden ser mejor utilizadas para beneficiar a la humanidad en su conjunto. De ahí la trascendental importancia de la investigación. Cada página de investigación, cada experimento, cada idea nueva, sienta las bases para un mañana más informado y preparado. Nos permite, como sociedad, no sólo seguir el ritmo de estos cambios, sino también guiarlos de forma responsable y ética.

En esta edición de Iluminate, hemos reunido una serie de artículos y contribuciones que reflejan ese amplio espectro de conocimiento al que hacíamos referencia. Es un testimonio palpable de cómo cada día, en laboratorios, empresas, universidades y talleres, se está escribiendo el futuro. Y sí, es cierto que la ingeniería de sistemas nos brinda herramientas y soluciones que parecen sacadas de la ciencia ficción. Pero, más allá de eso, nos muestra cómo esas herramientas pueden ser empleadas para construir una sociedad más justa, más inclusiva y más preparada para los desafíos del mañana.

La invitación, entonces, es clara: sumérgete en estas páginas no como quien consulta un manual técnico o un informe de labores, sino como quien se adentra en una narrativa épica. Porque eso es lo que está sucediendo en el mundo de la ingeniería de sistemas: una historia épica en constante evolución, donde los protagonistas somos todos y cada uno de nosotros. Una historia que nos desafía a ser más curiosos, más críticos y, sobre todo, a ser parte activa de la construcción de ese futuro que soñamos. Así que, ya sea que seas un experto en la materia, un apasionado de la tecnología, o simplemente alguien que quiere comprender mejor el mundo que le rodea, te prometemos que en las próximas páginas encontrarás algo que te inspire, te desafíe o te ilumine. Porque eso es, en esencia, lo que busca la revista Iluminate: ser un faro en el vasto océano de la ingeniería de sistemas, mostrándonos que, más allá de las tempestades y desafíos, hay horizontes llenos de posibilidades esperando ser descubiertos.

Te damos la bienvenida a este viaje de descubrimiento y reflexión. Que disfrutes de la travesía tanto como nosotros disfrutamos preparándola para ti.

M.SC. ING. OSAMU MANUEL YOKOSAKI PEÑARANDA

Coordinador de la Carrera de Ingeniería de Sistemas

PRESENTACIÓN

Estimados lectores,

Nos encontramos en una coyuntura de avances, retos y reflexiones, navegando en el vasto océano de la ingeniería de sistemas. Es un mundo que se expande y evoluciona a ritmos exponenciales, abordando desde la complejidad de los problemas matemáticos hasta las dinámicas que transforman la forma en la que aprendemos y trabajamos. Al sumergirnos en esta edición, encontraremos perspectivas que desentrañan los intricados desafíos de optimización, acercándonos a soluciones matizadas y sofisticadas que, hasta hace poco, podían parecer inalcanzables. Asimismo, nos adentraremos en el mundo de la arquitectura tecnológica, explorando innovadoras formas de estructurar y organizar sistemas, con especial atención en las prácticas emergentes que están redefiniendo la infraestructura tecnológica de las empresas.

La seguridad de la información es un tema que, dada su relevancia, ocupa un lugar preponderante en esta edición. Desde los mecanismos para proteger la delicada información médica, hasta el análisis profundo de normativas y estándares internacionales, nuestro objetivo es ofrecer una panorámica que no solo ilustre sobre los riesgos actuales, sino que también provea herramientas y directrices para enfrentarlos. La ciberseguridad,

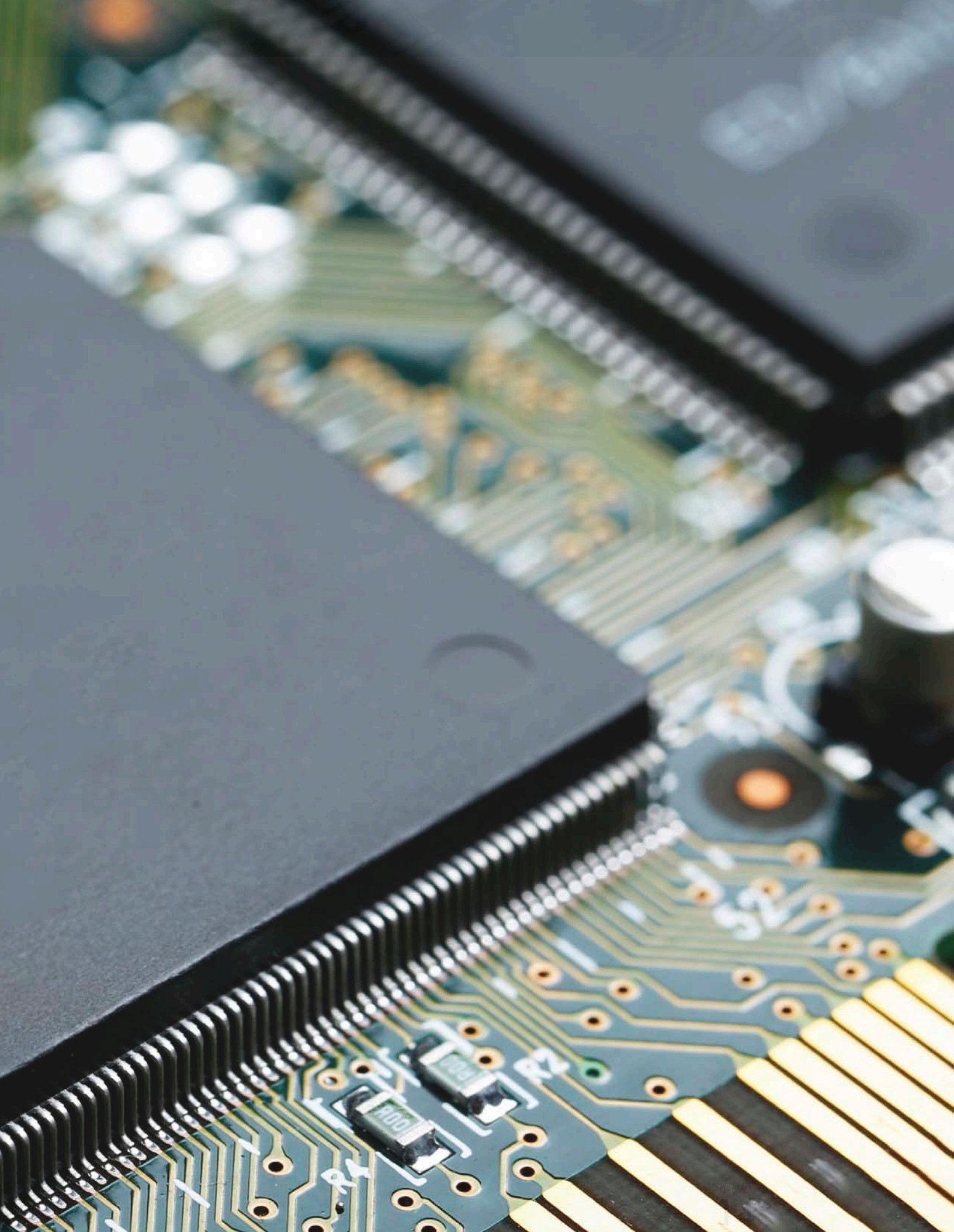
en sus múltiples dimensiones, nos invita a reflexionar sobre cómo asegurar nuestra presente digital sin perder de vista el horizonte de lo que está por venir. El aprendizaje y la adaptación al nuevo mundo laboral también son temáticas presentes. La gamificación, ese interesante entrecruzamiento entre juego y educación, nos muestra que las fronteras entre trabajo y diversión pueden ser más difusas de lo que pensamos. Mientras que el fenómeno del teletrabajo nos invita a sopesar sus múltiples aristas, considerando sus ventajas y desafíos en un mundo cada vez más conectado.

Finalmente, nos zambullimos en el delicado arte de desarrollar software. En un mundo donde la agilidad y la seguridad suelen estar en balanza, exploramos prácticas que buscan armonizar ambas dimensiones, garantizando no solo la eficiencia en el desarrollo, sino también la protección y robustez de las soluciones creadas. Este compendio de perspectivas y análisis ha sido cuidadosamente seleccionado con el propósito de brindarles un panorama amplio y profundo de la ingeniería de sistemas. Es un reflejo del vasto espectro de conocimientos y desafíos que esta disciplina abraza, y que, sin duda, seguirá abordando en el futuro.

Con cordialidad y expectación,
El equipo de Iluminate.

CONTENIDO

Pág.



SOLUCIÓN DE UN PROBLEMA INVERSO DE OPTIMIZACIÓN APLICANDO EL CRITERIO DEL HESSIANO (SOLUTION OF AN INVERSE OPTIMIZATION PROBLEM APPLYING THE HESSIAN CRITERION)

Autor:

Mario Errol Chavez Gordillo

mechavez@doc.ulasalle.edu.bo

Docente de la Universidad La Salle, Carrera de Ingeniería de Sistemas

erosmat@hotmail.com

Resumen

En este artículo construimos un polinomio en 2 variables de grado $(n+1)(m+1)$ cuyo conjunto de puntos extremos contiene un conjunto prescrito de nm puntos. También exhibimos una familia de polinomios en dos variables de grado 6 parametrizadas por puntos en $\mathbb{R}^4$ de tal manera que cada miembro de la familia presenta 2 puntos máximos y 2 puntos mínimos locales que cambian de máximo a mínimo cuando los parámetros pasan del ortante $\mathbb{R}^-\times\mathbb{R}^+\times\mathbb{R}^+\times\mathbb{R}^-$ al ortante $\mathbb{R}^-\times\mathbb{R}^+\times\mathbb{R}^-\times\mathbb{R}^+$. Los 4 puntos extremos dependen únicamente de la parametrización de la familia.

Palabras claves: Problemas Inversos; Optimización; Criterio del Hessiano

Abstract

In this paper we construct a polynomial in 2 variables of degree $(n+1)(m+1)$ whose set of extreme points contains a prescribed set of nm points. We also exhibit a family of polynomials in two variables of degree 6 parameterized by points in $\mathbb{R}^4$ such that each member of the family exhibits 2 maximum points and 2 local minimum points that change from maximum to minimum when the parameters pass from the orthant $\mathbb{R}^-\times\mathbb{R}^+\times\mathbb{R}^+\times\mathbb{R}^-$ to orthant $\mathbb{R}^-\times\mathbb{R}^+\times\mathbb{R}^-\times\mathbb{R}^+$. The 4 endpoints depend only on the parametrization of the family.

Key words: Inverse Problems; Optimization; Hessian Criterion

1 INTRODUCCIÓN

A continuación presentamos el problema que pretendemos resolver en este trabajo:

Dado una colección de puntos $\Lambda = \{P_k\}_{k=1}^m$ en $\mathbb{R}^n$, ¿es posible hallar un función de clase C^∞ o continuamente diferenciables $f: \mathbb{R}^n \to \mathbb{R}$ tales que Λ este contiendo en el conjunto de cuyos puntos máximos locales y puntos mínimos locales de f?.

Una respuesta afirmativa a este problema nos permitirá obtener numeros ejemplos de funciones que presenten puntos máximos locales y puntos mínimos locales, ejemplos muy necesarios a la hora de impartir los cursos de cálculo en varias variables, ver los corolarios 3.3 y 3.4. Además dichos puntos extremos locales estarías formados por cares de número enteros que facilitan los cálculos a la hora de aplicar el criterio de hessiano. Otra aplicación practica se la puede encontrar en el momento de calcular la temperatura de una placa metálica en cualesquiera de sus puntos conociendo únicamente los puntos donde es más caliente y puntos donde es mas frío, con estos datos será posible construir una función que nos prediga la temperatura de la placa en cualquier otro punto de la misma, ver el ejemplo 3.5.

En la literatura podemos encontrar diversos problemas inversos, por ejemplo: El problema de hallar un polinomio con ceros prescritos es un ejemplo del problema inverso. Los problemas espectrales inversos que consisten de una clase de problemas definidos como sigue: dada una clase C de matrices cuadradas de orden n y una n-tupla de números complejos $\Lambda = \{\lambda_1, \ldots, \lambda_n\}$, encontrar una matriz cuadrada, $A \in C$, cuyo espectro $\sigma(A)$ coincida con Λ. En particular C es una clase de matrices bien conocidas por sus propiedades (simétricas, Toeplitz, no negativas, etc.) (ver [1]). Por ejemplo tenemos el problema de valor propio inverso no negativo en donde se busca las condiciones necesarias y suficientes tales que la lista Λ de números complejos sea el espectro de una matriz A no negativa. Si tal matriz A existe, decimos que A realiza Λ (ver [2] y [6]).

El problema de optimización se define como el cálculo de los puntos máximos y mínimos de una función, esto es, encontrar los valores en el dominio de dicha función para los cuales se alcanza el máximo y mínimo en el codominio. Para ser más precisos:

Definición 1.1 (Problema de optimización.) *Dado un conjunto Ω, $\Omega \subset \mathbb{R}^n$, y una función $f: \Omega \to \mathbb{R}$ el problema de hallar $x_* \in \Omega$ tal que $f(x_*) \leq f(x)$ para todo $x \in \Omega$ se dice problema de minimización. El problema de hallar $x_* \in \Omega$ tal que $f(x_*) \geq f(x)$ para todo $x \in \Omega$ se dice problema de maximización. El problema de optimización se refiere a cualesquiera de ambos problemas de maximización o de minimización. El punto x_* se llama punto extremo de f cuando x_* es una solución del problema de optimización de f. Denota el problema de optimización por*

$$\max_{x \in \Omega} f(x) \quad o \quad \min_{x \in \Omega} f(x)$$

A continuación damos la definición del problema inverso de optimización y resolvemos de manera precisa un problema inverso de optimización.

Definición 1.2 (Problema inverso de optimización.) *Por problemas inversos de optimización entenderemos una clase de problemas definidos como sigue: dada una clase $\mathfrak{F}$ de funciones de clase C^∞ definidas sobre $\mathbb{R}^n$ y con valores en $\mathbb{R}$ y una n-tupla de puntos $A = \{(a_1^i, \ldots, a_n^i\}_{i=1}^n$, encontrar una función, $f \in \mathfrak{F}$, cuyo conjunto de puntos extremos contenga a A.*

En este trabajo, dado un conjunto de $nm + 1$ pares ordenados de números reales

$$\Lambda = \{(a_i, b_j): i = 1, \ldots, n,\ j = 1, \ldots, m\}$$

encontramos condiciones necesarias sobre Λ para la existencia de un polinomio en 2 variables de grado $(n+1)(m+1)$ cuyo conjunto de puntos extremos contenga al conjunto Λ. Para cada punto no nulo $(a_p, b_q) \in \Lambda$ definamos las funciones

$$\Phi_{p,q}(x, y) = \prod_{\substack{k=1 \\ k \neq p}}^n (x - a_k) \int_0^y \prod_{j=1}^m (s - b_j)\ d\,s$$

$$\Psi_{p,q}(x, y) = \prod_{\substack{k=1 \\ k \neq q}}^m (y - b_k) \int_0^x \prod_{i=1}^n (t - a_i)\ d\,t$$

Ahora enunciamos nuestro resultado principal que resuelve en parte nuestro problema planteado al inicio de esta sección:

Teorema 1.3 *Para las sucesiones de números reales* $\{a_i\}_{i=1}^n$ *y* $\{b_j\}_{j=1}^n$. *Considere la función*

$$f(x,y) = \int_0^x \prod_{i=1}^n (t-a_i)\ d\,t \int_0^y \prod_{j=1}^m (s-b_j)\ d\,s$$

Si $\Phi_{p,q}(a_p,b_q)\Psi_{p,q}(a_p,b_q) > 0$ para todo $p = 1,\dots,n$ y $q = 1,\dots,m$, entonces el conjunto de pares ordenado $\{(a_i,b_j): i = 1,\dots,n,\ j = 1,\dots,m\}$ esta contenido en el conjunto de puntos extremos locales de la función f. Pero si $\Phi_{p,q}(a_p,b_q)\Psi_{p,q}(a_p,b_q) < 0$, entonces (a_p,b_q) es un punto silla de f.

A partir del teorema 1.3 construimos una familia de polinomios en dos variables de grado 6 cuyo conjunto de índices es $\mathbb{R}^4$ de tal manera que cada miembro de la familia presenta 2 puntos máximos y 2 puntos mínimos locales que cambian de máximo a mínimo cuando los parámetros pasan del ortante $\mathbb{R}^-\times\mathbb{R}^+\times\mathbb{R}^+\times\mathbb{R}^-$ al ortante $\mathbb{R}^-\times\mathbb{R}^+\times\mathbb{R}^-\times\mathbb{R}^+$. Los 4 puntos extremos dependen únicamente de la parametrización de la familia. Esto esta probado en el teorema 3.1.

2 DEMOSTRACIÓN DEL TEOREMA PRINCIPAL

Nuestro teorema principal 1.3 es una consecuencia directa del siguiente teorema 2.1 que enunciamos y demostramos a continuación.

Teorema 2.1 *Para las sucesiones de números reales* $\{a_i\}_{i=1}^n$ *y* $\{b_j\}_{j=1}^n$. *Considere la función*

$$f(x,y) = \int_0^x \prod_{i=1}^n (t-a_i)\ d\,t \int_0^y \prod_{j=1}^m (s-b_j)\ d\,s$$

Para el punto (a_p,b_q) definamos las funciones

$$\Phi_{p,q}(x,y) = \prod_{\substack{k=1\\k\neq p}}^n (x-a_k) \int_0^y \prod_{j=1}^m (s-b_j)\ d\,s$$

$$\Psi_{p,q}(x,y) = \prod_{\substack{k=1\\k\neq q}}^m (y-b_k) \int_0^x \prod_{i=1}^n (t-a_i)\ d\,t$$

- Si $\Phi_{p,q}(a_p,b_q) > 0$, $\Psi_{p,q}(a_p,b_q) > 0$, entonces (a_p,b_q) es un mínimo local de f.
- Si $\Phi_{p,q}(a_p,b_q) < 0$, $\Psi_{p,q}(a_p,b_q) < 0$, entonces (a_p,b_q) es un máximo local de f.
- Si $\Phi_{p,q}(a_p,b_q)\Psi_{p,q}(a_p,b_q) < 0$, entonces (a_p,b_q) es un punto silla de f.

DEMOSTRACIÓN. Las derivadas parciales de Primer Orden de la función

$$f(x,y) = \int_0^x \prod_{i=1}^n (t-a_i)\ d\,t \int_0^y \prod_{j=1}^m (s-b_j)\ d\,s$$

están dados por

$$\frac{\partial f}{\partial x} = \prod_{i=1}^n (x-a_i) \int_0^y \prod_{j=1}^m (s-b_j)\ d\,s$$

$$\frac{\partial f}{\partial x} = \prod_{j=1}^m (y-b_j) \int_0^x \prod_{i=1}^n (t-a_i)\ d\,t$$

Hallamos todos los Puntos Críticos de la función $f(x,y)$, calculando las soluciones del sistemas de ecuaciones

$$\begin{cases} \frac{\partial f}{\partial x} = 0, \\ \frac{\partial f}{\partial y} = 0. \end{cases}, \qquad \begin{cases} \prod_{i=1}^n (x-a_i) \int_0^y \prod_{j=1}^m (s-b_j)\ d\,s = 0, & (1) \\ \prod_{j=1}^m (y-b_j) \int_0^x \prod_{i=1}^n (t-a_i)\ d\,t = 0. & (2) \end{cases}$$

El conjunto de puntos

$$\{(0,0)\} \cup \{(a_i,b_j): i = 1,\dots,n,\ j = 1,\dots,m\}$$

son puntos críticos de la función $f(x,y)$

Es claro que

$$\frac{d}{d\,x}\left[\prod_{i=1}^n (x-a_i)\right] = \sum_{i=1}^n \prod_{\substack{k=1\\k\neq i}}^n (x-a_k)$$

$$= (\widehat{x-a_1})\cdots(x-a_i)\cdots(x-a_n) + \cdots + (x-a_1)\cdots(\widehat{x-a_i})\cdots(x-a_n) + \cdots$$

$$+ (x-a_1)\cdots(x-a_i)\cdots(\widehat{x-a_n})$$

donde $\widehat{m}$ significa que el factor m no esta presente el la multiplicación. Por tanto

$$\frac{d}{dx}\Big|_{x=a_\ell}[\prod_{i=0}^{n}(x-a_i)] = \sum_{i=1}^{n}\prod_{\substack{k=1\\k\neq i}}^{n}(x-a_k) = \prod_{\substack{k=1\\k\neq \ell}}^{n}(a_\ell - a_k)$$

Calcular las derivadas parciales de Segundo Orden

$$\frac{\partial^2 f}{\partial x^2} = \frac{d}{dx}[\prod_{i=1}^{n}(x-a_i)]\int_0^y \prod_{j=1}^{m}(s-b_j)\,ds$$

$$\frac{\partial^2 f}{\partial y^2} = \frac{d}{dy}[\prod_{j=1}^{m}(y-b_j)]\int_0^x \prod_{i=1}^{n}(t-a_i)\,dt$$

$$\frac{\partial^2 f}{\partial x\partial y} = \frac{\partial^2 f}{\partial y\partial x} = \prod_{i=1}^{n}(x-a_i)\prod_{j=1}^{m}(y-b_j)$$

Evaluando en los puntos críticos tenemos

$$\frac{\partial^2 f}{\partial x^2}\Big|_{(x,y)=(a_p,b_q)} = \prod_{\substack{k=1\\k\neq p}}^{n}(a_p-a_k)\int_0^{b_q}\prod_{j=1}^{m}(s-b_j)\,ds$$

$$\frac{\partial^2 f}{\partial y^2}\Big|_{(x,y)=(a_p,b_q)} = \prod_{\substack{k=1\\k\neq q}}^{m}(b_q-b_k)\int_0^{a_p}\prod_{i=1}^{n}(t-a_i)\,dt$$

$$\frac{\partial^2 f}{\partial x\partial y}\Big|_{(x,y)=(a_p,b_q)} = \frac{\partial^2 f}{\partial y\partial x}\Big|_{(x,y)=(a_p,b_q)} = \prod_{i=1}^{n}(a_p-a_i)\prod_{j=1}^{m}(b_q-b_j) = 0$$

Por definición la forma cuadratica hessiana $Hf(x,y)$ de f en el punto (x,y) es dado por

$$Hf(x,y) = \begin{pmatrix} 0.3cm\dfrac{\partial^2 f}{\partial x^2} & \dfrac{\partial^2 f}{\partial x\partial y} \\ 0.3cm\dfrac{\partial^2 f}{\partial y\partial x} & \dfrac{\partial^2 f}{\partial y^2} \end{pmatrix}$$

y por tanto los menores hessianos son dado por

$$\Delta_1(x,y) = \frac{\partial^2 f}{\partial x^2} \qquad \Delta_2(x,y) = \det Hf(x,y)$$

evaluando los menores hessianos en (a_p,b_q) obtenemos

$$\Delta_1(a_p,b_q) = \Phi_{p,q}(a_p,b_q) \qquad \Delta_2(x,y) = \Phi_{p,q}(a_p,b_q)\Psi_{p,q}(a_p,b_q)$$

Asumiendo que $\Phi_{p,q}(a_p,b_q) > 0$, $\Psi_{p,q}(a_p,b_q) > 0$ se sigue que los menores hessianos en (a_p,b_q) ambos son positivos lo cual implica que la forma cuadrática hessiana $Hf(a_p,b_q)$ es definida positiva, aplicando el criterio del hessiano en [3] se sigue que el punto (a_p,b_q) es un punto mínimo local de f.

Ahora bien, en el caso en que $\Phi_{p,q}(a_p,b_q) < 0$, $\Psi_{p,q}(a_p,b_q) < 0$ el primer menor hessiano es negativo y el segundo es positivo haciendo que la forma cuadrática hessiana $Hf(a_p,b_q)$ sea definida negativa, aplicando el criterio del hessiano en [3] conduce a que el punto (a_p,b_q) es un punto máximo local de f.

Un razonamiento similar garantiza que cuando $\Phi_{p,q}(a_p,b_q)\Psi_{p,q}(a_p,b_q) < 0$, el putno (a_p,b_q) es un punto silla de f.

3 CONSECUENCIAS DEL TEOREMA PRINCIPAL

Corolario 3.1 *Para $a,b,c,d \in \mathbb{R}$ definamos la función*

$$f(x,y) = \left(\frac{x^3}{3} - (a+b)\frac{x^2}{2} + abx\right)\left(\frac{y^3}{3} - (c+d)\frac{y^2}{2} + cdy\right)$$

y definamos

$$m_1 = (a-b)(3d-c) \qquad m_2 = (c-d)(3b-a)$$
$$m_3 = (a-b)(3c-d) \qquad m_4 = (c-d)(3a-b)$$

1. Si $m_1 > 0$, $m_2 > 0$, $m_3 < 0$ y $m_4 < 0$, entonces
   (a) Los puntos (a,c) y (b,d) son puntos mínimos locales de f.
   (b) Los puntos (b,c) y (a,d) son puntos máximos locales de f.

2. Si $m_1 < 0$, $m_2 < 0$, $m_3 > 0$ y $m_4 > 0$, entonces
   (a) Los puntos (a,c) y (b,d) son puntos máximos locales de f.
   (b) Los puntos (b,c) y (a,d) son puntos mínimos locales de f.

3. Si $m_1 m_2 < 0$, entonces (a,c) es un punto silla de f.
4. Si $m_3 m_2 > 0$, entonces (a,d) es un punto silla de f.
5. Si $m_1 m_4 > 0$, entonces (b,c) es un punto silla de f.
6. Si $m_3 m_4 < 0$, entonces (b,d) es un punto silla de f.

DEMOSTRACIÓN. Puesto que

$$\int (x-a)(x-b)\ dx = \int (x^2-(a+b)x+ab)\ dx = \frac{x^3}{3} - (a+b)\frac{x^2}{2} + abx$$

Entonces

$$f(x,y) = \int_0^x (t-a)(t-b)\ dt \int_0^y (s-c)(s-d)\ ds$$

Aplicando el teorema 2.1 los puntos

$$(a,c), \quad (a,d), \quad (b,c), \quad (b,d), \quad (0,0),$$

son puntos críticos de la función $f(x,y)$. Definamos la función

$$\Omega(t,u,v) = \int_0^t (\tau-u)(\tau-v)\ d\tau = \frac{t^3}{3} - (u+v)\frac{t^2}{2} + uvt$$

$$\Omega(u,u,v) = \frac{u^3}{3} - (u+v)\frac{u^2}{2} + u^2 v = \frac{u^2(3v-u)}{6}$$

$$\Omega(v,u,v) = \frac{v^3}{3} - (u+v)\frac{v^2}{2} + uv^2 = \frac{v^2(3u-v)}{6}$$

Definamos las funciones

$$\Phi_1(x,y) = (x-b)\Omega(y,c,d), \qquad \Phi_2(x,y) = (x-a)\Omega(y,c,d)$$

$$\Psi_1(x,y) = (y-d)\,\Omega(x,a,b), \qquad \Psi_2(x,y) = (y-c)\,\Omega(x,a,b)$$

Evaluando en (a,c)

$$\Phi_1(a,c) = (a-b)\Omega(c,c,d) = (a-b)\frac{c^2(3d-c)}{6} = \frac{c^2}{6}(a-b)(3d-c) = \frac{c^2}{6} m_1$$

$$\Psi_1(a,c) = (c-d)\Omega(a,a,b) = (c-d)\frac{a^2(3b-a)}{6} = \frac{a^2}{6}(c-d)(3b-a) = \frac{a^2}{6} m_2$$

Evaluando en (a,d)

$$\Phi_1(a,d) = (a-b)\Omega(d,c,d) = (a-b)\frac{d^2(3c-d)}{6} = \frac{d^2}{6}(a-b)(3c-d) = \frac{d^2}{6} m_3$$

$$\Psi_2(a,d) = (d-c)\,\Omega(a,a,b) = -\frac{a^2}{6} m_2$$

Evaluando en (b,c)

$$\Phi_2(b,c) = (b-a)\Omega(c,c,d) = (b-a)\frac{c^2(3d-c)}{6} = -\frac{c^2}{6}(a-b)(3d-c) = -\frac{c^2}{6} m_1$$

$$\Psi_1(b,c) = (c-d)\,\Omega(b,a,b) = (c-d)\frac{b^2(3a-b)}{6} = \frac{b^2}{6} m_4$$

Evaluando en (b,d)

$$\Phi_2(b,d) = (b-a)\Omega(d,c,d) = -\frac{d^2}{6} m_3$$

$$\Psi_2(b,d) = (d-c)\,\Omega(b,a,b) = (d-c)\frac{b^2(3a-b)}{6} = \frac{b^2}{6}(d-c)(3a-b) = -\frac{b^2}{6} m_4$$

172 Supongamos que $m_1 > 0$, $m_2 > 0$, $m_3 < 0$ y $m_4 < 0$, entonces

$$\Phi_1(a,c) > 0, \quad \Psi_1(a,c) > 0, \qquad \Phi_1(a,d) < 0, \quad \Psi_2(a,d) < 0$$

$$\Phi_2(b,c) < 0, \quad \Psi_1(b,c) < 0, \qquad \Phi_2(b,d) > 0, \quad \Psi_2(b,d) > 0$$

Aplicando el teorema 2.1 obtenemos

1. Los puntos (a,c) y (b,d) son puntos mínimos locales de f.
2. Los puntos (b,c) y (a,d) son puntos máximos locales de f.

Si $m_1 m_2 < 0$, entonces

$$\Phi_1(a,c)\,\Psi_1(a,c) = \frac{c^2}{6}\,m_1\,\frac{a^2}{6}\,m_2 = \frac{a^2c^2}{36}\,m_1\,m_2 < 0$$

Aplicando el teorema 2.1 el punto (a,c) es un punto silla de f.

Si $m_3 m_2 > 0$, entonces

$$\Phi_1(a,d)\,\Psi_2(a,d) = -\frac{d^2}{6}\,m_3\,\frac{a^2}{6}\,m_2 = -\frac{a^2d^2}{6}\,m_2\,m_3 < 0$$

Aplicando el teorema 2.1 el punto (a,d) es un punto silla de f.

Si $m_1 m_4 > 0$, entonces

$$\Phi_2(b,c)\,\Psi_1(b,c) = -\frac{c^2}{6}\,m_1\,\frac{b^2}{6}\,m_4 = -\frac{b^2c^2}{36}\,m_1\,m_4 < 0$$

Aplicando el teorema 2.1 el punto (b,c) es un punto silla de f.

Si $m_3 m_4 < 0$, entonces

$$\Phi_2(b,d)\,\Psi_2(b,d) = \frac{d^2}{6}\,m_3\,\frac{b^2}{6}\,m_4 = \frac{b^2d^2}{36}\,m_3\,m_4 < 0$$

Aplicando el teorema 2.1 el punto (b,d) es un punto silla de f.

Corolario 3.2 *Para $a,b,c,d \in \mathbb{R}$ definamos la función*

$$f(x,y) = \left(\frac{x^3}{3} - (a+b)\frac{x^2}{2} + abx\right)\left(\frac{y^3}{3} - (c+d)\frac{y^2}{2} + cdy\right)$$

1. Si $(a < 0 < b \text{ y } d < 0 < c)$ o $(b < 0 < a \text{ y } c < 0 < d)$, entonces
   (a) Los puntos (a,c) y (b,d) son puntos mínimos locales de f.
   (b) Los puntos (b,c) y (a,d) son puntos máximos locales de f.

2. Si $(a < 0 < b \text{ y } c < 0 < d)$ o $(b < 0 < a \text{ y } d < 0 < c)$, entonces
   (a) Los puntos (a,c) y (b,d) son puntos máximos locales de f.
   (b) Los puntos (b,c) y (a,d) son puntos mínimos locales de f.

3. Si $ab < 0$ y $cd < 0$, entonces los puntos (a,c), (b,d), (b,c) y (a,d) son puntos extremos locales de la función f.

DEMOSTRACIÓN.

1. Supongamos que

$$(a < 0 < b \;\; y \;\; d < 0 < c) \quad o \quad (b < 0 < a \;\; y \;\; c < 0 < d)$$

- Supongamos que $a < 0 < b$ y $d < 0 < c$, entonces

$$3a < a < 0 < b < 3b, \qquad 3d < d < 0 < c < 3c$$

$$a - b < 0, \quad 3d - c < 0, \quad c - d > 0, \quad 3b - a > 0$$
$$a - b < 0, \quad 3c - d > 0, \quad c - d > 0, \quad 3a - b < 0$$

- Supongamos que $b < 0 < a$ y $c < 0 < d$, entonces

$$3b < b < 0 < a < 3a, \qquad 3c < c < 0 < d < 3d$$

$$a - b > 0, \quad 3d - c > 0, \quad c - d < 0, \quad 3b - a < 0$$
$$a - b > 0, \quad 3c - d < 0, \quad c - d < 0, \quad 3a - b > 0$$

Para cualesquiera de ambos casos se tiene

$$m_1 = (a-b)(3d-c) > 0 \qquad m_2 = (c-d)(3b-a) > 0$$
$$m_3 = (a-b)(3c-d) < 0 \qquad m_4 = (c-d)(3a-b) < 0$$

Aplicando el corolario 3.1 se tiene el resultado.

2. Supongamos que

$$(a < 0 < b \ y \ c < 0 < d) \quad o \quad (b < 0 < a \ y \ d < 0 < c)$$

- Supongamos que $a < 0 < b$ y $c < 0 < d$, entonces

$$3a < a < 0 < b < 3b, \qquad 3c < c < 0 < d < 3d$$

$$a-b < 0, \quad 3d-c > 0, \quad c-d < 0, \quad 3b-a > 0$$
$$a-b < 0, \quad 3c-d < 0, \quad c-d < 0, \quad 3a-b < 0$$

- Supongamos que $b < 0 < a$ y $d < 0 < c$, entonces

$$3b < b < 0 < a < 3a, \qquad 3d < d < 0 < c < 3c$$

$$a-b > 0, \quad 3d-c < 0, \quad c-d > 0, \quad 3b-a < 0$$
$$a-b > 0, \quad 3c-d > 0, \quad c-d > 0, \quad 3a-b > 0$$

Para cualesquiera de ambos casos se tiene

$$m_1 = (a-b)(3d-c) < 0 \qquad m_2 = (c-d)(3b-a) < 0$$
$$m_3 = (a-b)(3c-d) > 0 \qquad m_4 = (c-d)(3a-b) > 0$$

Aplicando el corolario 3.1 se tiene el resultado.

3. Supongamos que $ab < 0$ y $cd < 0$, entonces

$$(a < 0 < b \ o \ b < 0 < a) \quad y \quad (c < 0 < d \ y \ d < 0 < c)$$

Asignando

$$p: a < 0 < b, \quad q: b < 0 < a, \quad r: c < 0 < d, \quad s: d < 0 < c$$

$$\begin{aligned}(p \vee q) \wedge (r \vee s) &\equiv [(p \vee q) \wedge r] \vee [(p \vee q) \wedge s] \\ &\equiv [(p \wedge r) \vee (q \wedge r)] \vee [(p \wedge s) \vee (q \wedge s)] \\ &\equiv [(p \wedge r) \vee (q \wedge s)] \vee [(p \wedge s) \vee (q \wedge r)]\end{aligned}$$

$$(p \vee q) \wedge (r \vee s) \equiv [(p \wedge r) \vee (q \wedge s)] \vee [(p \wedge s) \vee (q \wedge r)]$$

Luego se presentan dos casos

Caso 1.

$$(a < 0 < b \ y \ c < 0 < d) \quad o \quad (b < 0 < a \ y \ d < 0 < c)$$

Caso 2.

$$(a < 0 < b \ y \ d < 0 < c) \quad o \quad (b < 0 < a \ y \ c < 0 < d)$$

Estos dos casos fueron tratados en los incisos anteriores.

Definamos los subconjuntos de números reales $\mathbb{R}^+$ y $\mathbb{R}^-$ por

$$\mathbb{R}^+ = \{x \in \mathbb{R}: x > 0\}, \qquad \mathbb{R}^- = \{x \in \mathbb{R}: x < 0\}$$

Una consecuencia del corolario 3.2 es el siguiente resultado

Corolario 3.3 *Para* $(a,b,c,d) \in \mathbb{R}^4$ *definamos la familia de funciones dada por*

$$f_{(a,b,c,d)}(x,y) = \left(\frac{x^3}{3} - (a+b)\frac{x^2}{2} + abx\right)\left(\frac{y^3}{3} - (c+d)\frac{y^2}{2} + cdy\right)$$

1. Para todo

$$(a,b,c,d) \in (\mathbb{R}^- \times \mathbb{R}^+ \times \mathbb{R}^+ \times \mathbb{R}^-) \cup (\mathbb{R}^+ \times \mathbb{R}^- \times \mathbb{R}^- \times \mathbb{R}^+)$$

la familia $f_{(a,b,c,d)}$ tiene puntos mínimos locales en (a,c) y (b,d); además presenta puntos máximos locales en (b,c) y (a,d).

2. Para todo

$$(a,b,c,d) \in (\mathbb{R}^-\times\mathbb{R}^+\times\mathbb{R}^-\times\mathbb{R}^+) \cup (\mathbb{R}^+\times\mathbb{R}^-\times\mathbb{R}^+\times\mathbb{R}^-)$$

la familia $f_{(a,b,c,d)}$ tiene puntos mínimos locales en (b,c) y (a,d); además presenta puntos máximos locales en (a,c) y (b,d).

Denotemos por $C^\infty(\mathbb{R}^2,\mathbb{R})$ el espacio de funciones de clase C^∞ definidas sobre $\mathbb{R}^2$ con valores reales. Definamos la curva $F:\mathbb{R}\to C^\infty(\mathbb{R}^2,\mathbb{R})$ por

$$F(t) = F_t:\mathbb{R}^2\to\mathbb{R}, \qquad F_t(x,y) = f_{(-t^2,t^2,-t,t)}(x,y)$$

Una aplicación inmediata del corolario 3.3 es

Corolario 3.4 *Para $t\in\mathbb{R}$ los puntos*

$$P_t = (a=-t^2, c=-t), \qquad Q_t = (b=t^2, d=t),$$

$$R_t = (b=t^2, c=-t), \qquad S_t = (a=-t^2, d=t)$$

son puntos críticos de la familia

$$F_t(x,y) = \left(\frac{x^3}{3} - t^4x\right)\left(\frac{y^3}{3} - t^2y\right)$$

Además

1. Si $t<0$, entonces
   (a) Los puntos P_t y Q_t son puntos mínimos locales de F_t.
   (b) Los puntos R_t y S_t son puntos máximos locales de F_t.

2. Si $t>0$, entonces
   (a) Los puntos P_t y Q_t son puntos máximos locales de F_t.
   (b) Los puntos R_t y S_t son puntos mínimos locales de F_t.

Ahora vamos a usar el corolario 3.3 para resolver el siguiente problema inverso de optimización:

Ejemplo 3.5 *Se sabe que los puntos más calientes están en los puntos $(6,4)$ y $(-4,-2)$ y los puntos más frío de la placa están en los puntos $(6,-2)$ y $(-4,4)$. Hallar una función T para la temperatura de la placa en cada uno de sus puntos (x,y) de tal manera que sus extremos sean los puntos más calientes y puntos más frío de la placa. Además T debe verificar $T(0,0)=10$.*

SOLUCIÓN.- Para los puntos

$$(6,4),\quad (-4,-2),\quad (6,-2),\quad (-4,4)$$

tomemos

$$a=-4,\quad b=6,\quad c=-2,\quad d=4$$

Luego $a+b=-4+6=2$, $ab=-24$, $c+d=-2+4=2$ y $cd=-8$. Ahora usando el usar el corolario 3.3 podemos definir la función T por

$$T(x,y) = 0.004\left(\frac{x^3}{3} - x^2 - 24x\right)\left(\frac{y^3}{3} - y^2 - 8y\right) + 10$$

A continuación usamos un programa en Wolfram Mathematica que implementa el criterio del hessiano que nos permite hallar y clasificar los 13 puntos críticos de la función T, este programa de encuentra en el apéndice. Estos 13 puntos críticos de la función T son los siguientes:

$0.2cm(x = -7.11684, y = -3.62348)$, $(x = -7.11684, y = 0)$,
$0.2cm(x = -7.11684, y = 6.62348)$, $(x = -4, y = -2)$,
$0.2cm(x = -4, y = 4)$, $(x = 0, y = -3.62348)$,
$0.2cm(x = 0, y = 0)$, $(x = 0, y = 6.62348)$,
$0.2cm(x = 6, y = -2)$, $(x = 6, y = 4)$,
$0.2cm(x = 10.1168, y = -3.62348)$, $(x = 10.1168, y = 0)$,
$0.2cm(x = 10.1168, y = 6.62348)$

Evaluando

$0.2cmT(-7.11684, -3.62348) = 10.$ $T(-7.11684,0) = 10.$
$0.2cmT(-7.11684,6.62348) = 10.$ $T(-4., -2.) = 12.1902$
$0.2cmT(-4.,4.) = 3.74222$ $T(0, -3.62348) = 10.$
$0.2cmT(0,0) = 10.$ $T(0,6.62348) = 10.$
$0.2cmT(6., -2.) = 5.968$ $T(6.,4.) = 21.52$
$0.2cmT(10.1168, -3.62348) = 10.$ $T(10.1168,0) = 10.$
$0.2cmT(10.1168,6.62348) = 10.$

el programa en Mathematica evalúa cada punto crítico en los dos menores hessianos y luego usando el criterio del hessiano en [3] se demuestra que los puntos $(6,4)$ y $(-4,-2)$ son puntos máximos locales de la función T y los puntos $(6,-2)$ y $(-4,4)$ son puntos mínimos locales de la función T. El resto de los puntos críticos no nulos de T son puntos silla.

4. APÉNDICE

```
Clear["Global`*"]
NCriticos=13;

Print["Funcion Objetivo"]
f[x_,y_]=0.004*((x^3)/3 - x^2 - 24x)*((y^3)/3 - y^2 - 8y)+10;

Print["f[x,y] = ",f[x,y]]
Print["Derivadas Paricales de Primer Orden"]
Print["∂xf   =   ",Expand[∂x f[x, y]]]

Print["∂yf   =   ",Expand[∂y f[x, y]]]

Print["Funcion Objetivo"]
Print["f[x,y] = ",f[x,y]]

Print["Derivadas Paricales de Primer Orden"]
Print["∂xf   =   ",Expand[∂x f[x, y]]]
Print["∂yf   =   ",Expand[∂y f[x, y]]]

Print["Hallando los Puntos Criticos"]
PCriticos=NSolve[∂x f[x, y]==0&&∂y f[x, y]==0,{x,y},Reals]
For[i=1,i<=NCriticos,i++,
  Print["f(",(x/.PCriticos[[i]]),", ",(y/.PCriticos[[i]]),")=",f[(x/.PCriticos[[i]]),(y/.PCriticos[[i]])]]]
Print["Derivadas Paricales de Segundo Orden"]
Print["∂x,xf   =   ",Factor[∂x,x f[x, y]]]
Print["∂x,yf   =   ",Factor[∂x,y f[x, y]]]
Print["∂y,yf   =   ",Factor[∂y,y f[x, y]]]
```

```
Print["La Matriz Hessiana es"]
Hf={{Factor[∂x,x f[x, y]],Factor[∂x,y f[x, y]]},{Factor[∂x,y f[x, y]],Factor[∂y,y f[x, y]]}};
matrizHf[x_,y_]={{Factor[∂x,x f[x, y]],Factor[∂x,y f[x, y]]},{Factor[∂x,y f[x, y]],Factor[∂y,y f[x, y]]}};
Print["Hf = ",MatrixForm[Hf]]

Print["Menores Principales"]
Delta1[x_,y_]=Simplify[∂x,x f[x, y]];
Print["Delta1 = ",Simplify[∂x,x f[x, y]]];
Delta2[x_,y_]=Det[Hf];
Print["Delta2 = Det",MatrixForm[Hf]," = ",Det[Hf]];

Print["Evaluando los puntos críticos para clasificarlos"]
For[i=1,i<=NCriticos,i++,
 Print["Delta1(", (x/.PCriticos[[i]]),",",(y/.PCriticos[[i]]), ") = ∂x,xf(", (x/.PCriticos[[i]]),",",(y/.PCriticos[[i]]), ") =
",Delta1[(x/.PCriticos[[i]]),(y/.PCriticos[[i]])]]

  Print["Delta2(", (x/.PCriticos[[i]]),",",(y/.PCriticos[[i]]), ") =
det",MatrixForm[Simplify[matrizHf[(x/.PCriticos[[i]]),(y/.PCriticos[[i]])]]]," =
",Delta2[(x/.PCriticos[[i]]),(y/.PCriticos[[i]])]]

  Print["f(",(x/.PCriticos[[i]]),",",(y/.PCriticos[[i]]), ") = ",f[(x/.PCriticos[[i]]),(y/.PCriticos[[i]])]]
 ]
valor=2;
escalaxy=2;
escalaz=1;
Plot3D[f[x,y],{x,-valor,valor},{y,-valor,valor},BoxRatios->{escalaxy,escalaxy,escalaz},PlotRange->Full]
```

BIBLIOGRAFÍA

[1] Caparrós Quintero, Agustín. (2011). 'Problemas Espectrales Inversos Master Thesis', Universidad Nacional de Educación a Distancia (España). Facultad de Ciencias

[2] Patricia D. Egleston, Terry D. Lenker, and Sivaram K. Narayan. 'The nonnegative inverse eigenvalue problem'. Linear Algebra Appl., 379:475–490, 2004. 10th Conference of the International Linear Algebra Society.

[3] Elon Lages Lima (2004), Análise Real, Volume 2, Rio de Janeiro 9 de março de 2004

[4] Elon Lages Lima, (1985), Curso de análise, Volúmen 2, Segunda Edicao, Ed. IMPA, Brasilia.

[5] Michael Spivak, (1970), Cálculo en variedades Ed. Reverté S.A., Barcelona.

[6] Elvis Ronald Valero, Exequiel Mallea-Zepeda, Eber Lenes. 'A recursive condition for the inverse problem of eigenvalue for nonnegative symmetric matrices'. Published in Revista Integración. Vol. 35, no. 1 pp. 37 – 50

Artículo Recibido: 27/04/2023

Artículo Aceptado: 19/05/2023

INTRODUCCIÓN A LA ARQUITECTURA DE MICROSERVICIOS

Autor:

Rodrigo Rubén Alarcón Vargas

rodrigo.alarcon.rv@gmail.com

Instituto de Investigación en Ciencia y Tecnología, Universidad La Salle-Bolivia

Resumen

El presente articulo tiene la intención de introducir los conceptos de herramientas y patrones más usados durante el diseño de una arquitectura de aplicaciones basadas en microservicios. Los conceptos explican el comportamiento y la utilidad de estas herramientas en el ciclo de vida de los sistemas; siendo agnósticos a las tecnologías emergentes y frecuentemente adoptadas, se expresan las técnicas más comunes para la resolución de problemas y escenarios recurrentes.

Palabras clave: Microservicios, computación en la nube, arquitectura, diseño de software.

Abstract

This article intends to introduce the concept of tools and patterns most used during the design of applications based on microservices. The concepts explain the behavior and utility of these tools in the system's life cycle; by being agnostic to emerging and frequently adopted technologies, the most common techniques for solving problems and recurring scenarios are expressed.

Key words: Microservices, cloud computing, software architecture, system design.

Introducción

La arquitectura por microservicios es un método distintivo para el desarrollo de software que ha crecido enormemente en los últimos años. Microservicios conlleva una curva de aprendizaje bastante pronunciada, conocer las técnicas y prácticas comunes son necesarias al momento de su planeación, diseño y construcción.

El objetivo principal del presente artículo es dar a cono-

cer las técnicas y prácticas comunes que son utilizadas durante el ciclo de vida del desarrollo de aplicaciones basadas en microservicios, interpretando y dando una gentil introducción a cada técnica y herramienta.

Conceptos Generales

La arquitectura de microservicios ha sido ampliamente adoptada como una arquitectura que nos permite desarrollar software de manera rápida y segura. El concepto base de esta arquitectura radica en que cada servicio sea independiente y autónomo, cada uno de los servicios es modelado en torno a un dominio dentro del contexto de la lógica de negocios.

Los microservicios son considerados como un tipo de arquitectura orientado a servicios (SOA) debido a que la implementación está basada en componentes reusables denominados servicios. Las interfaces de los servicios proporcionan un acoplamiento flexible, lo que significa que cada uno de los servicios puede ser instanciado sin la necesidad de conocer el proceso actual dentro de la lógica de negocios (IBM, 2021).

Una de las ideas principales detrás de microservicios es que muchos tipos de aplicaciones se vuelven más fáciles de construir y mantener cuando se dividen en piezas más pequeñas que se pueden componer y que funcionan juntas (Novoseltseva, 2020).

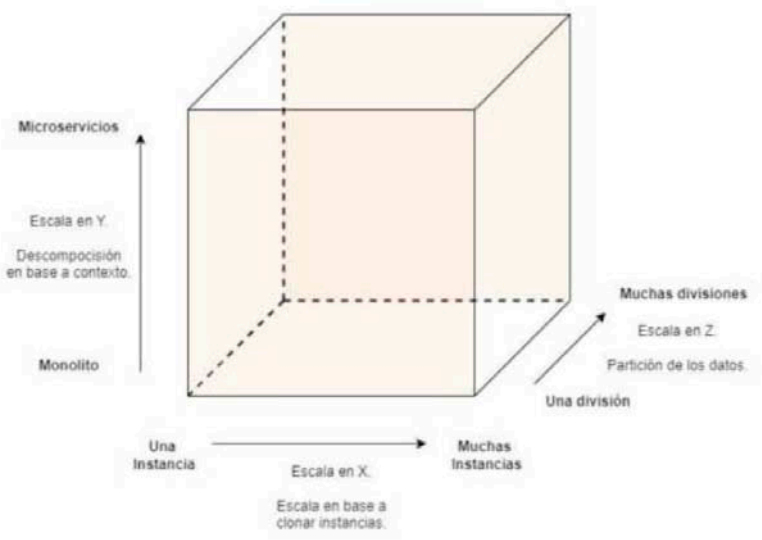
Gracias a su escalabilidad, este método de arquitectura es considerada ideal particularmente cuando se soportan una gran cantidad de plataformas y dispositivos, como web, móviles, internet en las cosas, entre otros.

Monolito y Microservicios

Microservicios nace a causa de problemas de escalabilidad recurrentes en las aplicaciones con una arquitectura monolítica, microservicios soluciona estos problemas basándose en patrones de granularidad, a diferencia de las aplicaciones monolito.

El mantenimiento y estrategias de las arquitecturas de la transición de un monolito a microservicios se puede graficar en base al modelo tridimensional de escalabilidad propuesta por Abbot y Fisher en el año 2015:

Figura 1: Modelo tridimensional de escalabilidad



Fuente: Elaboración propia

El modelo se base en tres caminos de escalabilidad de una aplicación: ejes X, Y, y Z (Richardson, 2019):

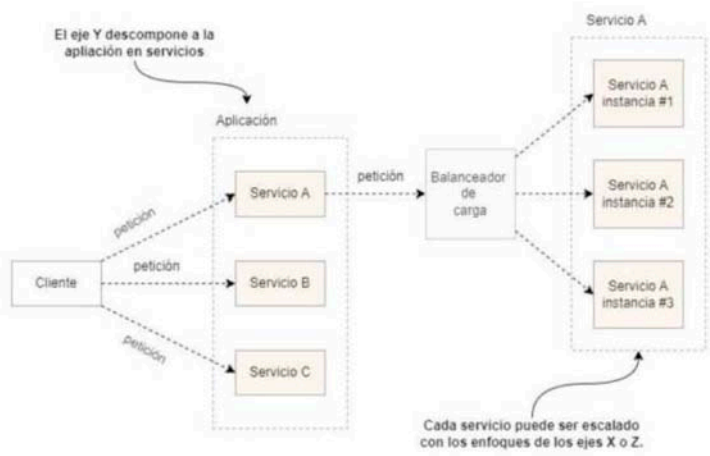
- Eje X: es la forma más común de escalar una aplicación monolito, se ejecutan varias instancias de la misma aplicación detrás de un balanceador de carga

(load balancer). El balanceador de carga es el responsable de distribuir las peticiones entre las instancias existentes.

- Eje Z: del mismo modo se ejecutan múltiples instancias de la misma aplicación, la diferencia radica en que cada instancia se encarga de un subconjunto de los datos. El balanceador de carga se encarga de identificar la instancia apropiada con la que se va a trabajar.

- Eje Y: los dos enfoques previamente descritos pueden mejorar la capacidad y disponibilidad de una aplicación, pero ninguno de los dos resuelve el problema de la complejidad de la arquitectura y desarrollo. Para resolver este problema se necesita aplicar una descomposición funcional (ver Figura 2). Un servicio se enfoca solamente en base a una funcionalidad en particular.

Figura 2: Descomposición funcional (escala en eje Y)



Fuente: Elaboración propia

A continuación, se listan algunas de los notables beneficios de microservicios:

- Cada servicio es pequeño y fácil de mantener.
- Cada servicio es independientemente desplegable.
- Cada servicio es independientemente escalable.
- Ayuda a los equipos a ser autónomos.
- Posibilita la adopción de diferentes tecnologías y lenguajes de programación.

Microservicios aplican un claro ejemplo del principio Open/Closed:

- Son abiertos a extensiones, utilizando las interfaces que exponen.
- Son cerrado a modificación, cada implementación y versionamiento es totalmente independiente.

Patrones y tecnologías

Microservicios ofrece grandes beneficios, pero también genera nuevos retos, los patrones de una arquitectura de microservicios son pilares fundamentales durante el desarrollo de una aplicación basada en microservicios. Durante su diseño se consideran prácticas de integración y entrega continuas (CI/CD). También acelera el proceso de entrega de las nuevas funcionalidad y características dentro de una aplicación por servicio (de la Torre, Wagner, & Mike, 2022).

La siguiente lista muestra aspectos importantes que se debe tomar en cuenta para lograr la ejecución correcta en producción:

- Monitoreo continuo de los servicios y la infraestructura.
- Infraestructura escalable para los servicios.
- Diseño de seguridad e implementación.
- Entregas rápidas.
- Prácticas e infraestructura DevOps y CI/CD.

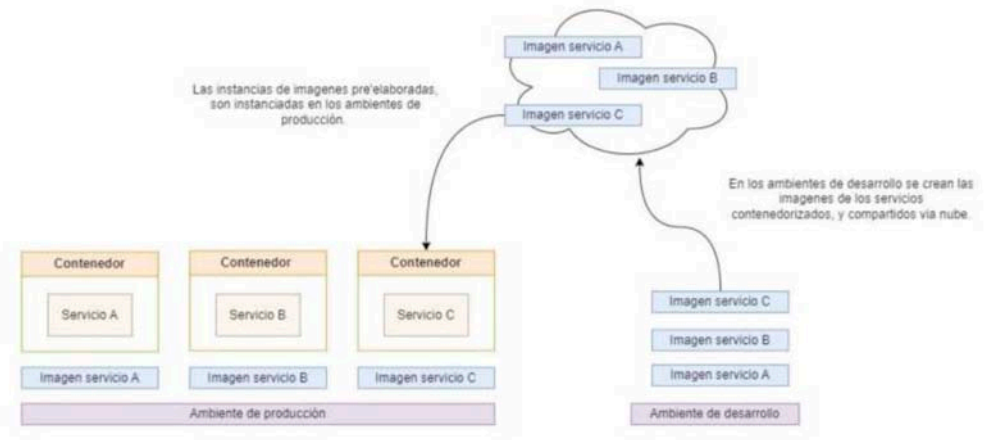
Contenedores (Containers). Los contendores son un factor que extiende y complementa las aplicaciones basadas en microservicios. Un contenedor es un entorno de tiempo de ejecución virtualizado, es usado para crear, ejecutar e implementar aplicaciones que están aisladas del hardware subyacente (Gillis, 2021).

El uso de contenedores en microservicios es realizado en los ambientes de desarrollo y de producción, únicamente un servicio es ejecutado en un contenedor, por consiguiente, se obtiene que cada servicio se ejecutado en un contenedor en particular. De este modo, cada servicio puede aprovechar los recursos y el uso eficiente de la capacidad computacional.

El uso de contendores brinda ventajas como: fácil replicación de servicios, mejor administración del uso de recursos, simpleza en la ejecución de instancias en las practicas CI/CD, y alta portabilidad.

En la siguiente imagen se muestra un ejemplo de ciclo de vida de la integración de contenedores en los ambientes de desarrollo y producción.

Figura 3: Contenedores en producción



Fuente: Elaboración propia

Orquestradores (Orchestrators): Cuando las aplicaciones deben escalar aún más con una arquitectura basada en muchos microservicios, es critica la necesidad de administrar todos los servidores y contenedores, abstrayendo su complejidad en procesos automáticos. Aquí es donde los orquestradores toman lugar.

Un flujo de trabajo de orquestración de microservicios es un método arquitectónico de coordinación de microservicios, en el que los servicios reciben instrucciones de un controlador central, denominado orquestrador. El orquestador actúa como el cerebro, dirigiendo los procesos de ejecución; esta espera por la respuesta de un servicio antes de proceder con el siguiente (Lukmna, 2022).

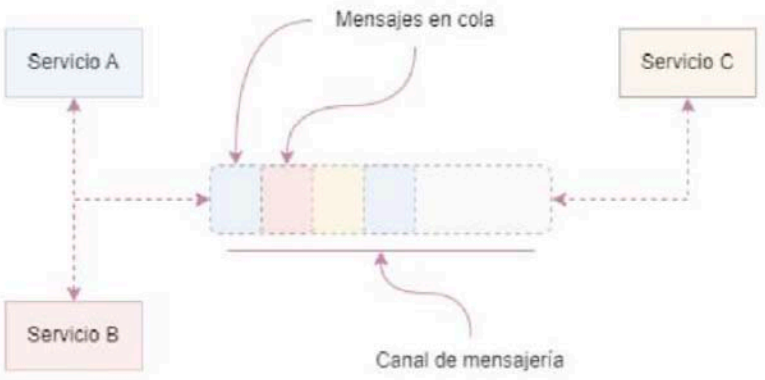
Canales de mensajería (Message Brokers): Los canales de mensajería son un tipo tecnología que permiten la comunicación e intercambio de información entre aplicaciones basadas en microservicios o en la nube, siendo agnósticos al lenguaje o al tipo de implementación.

Los canales de mensajería pueden validar, guardar, enrutar, y entregar mensajes a su destino apropiado. Sirven como un intermediario entre aplicaciones, permitiendo a los remitentes encolar un mensaje sin la necesidad de conocer dónde están los receptores, sin importar si están activos o no, o cuantos de ellos existen. En orden de mantener consistencia en la comunicación los canales de mensajería están soportados por colas de mensajes que guardan la información hasta que los destinatarios sean capaces de procesarlos. En una cola de mensajes, los datos son guardados exactamente en el orden en el que

fueron transmitidos y permanecen ahí hasta que el recipiente los consuma (IBM, 2020).

Este tipo de comunicación es ampliamente adoptado en las arquitecturas de microservicios: los servicios se comunican preferiblemente a través de canales de mensajería en lugar de otro tipo de protocolos de comunicación como HTTP, SOAP, entre otros, debido a que la persistencia de la información es más importante en la arquitectura del lado del servidor.

Figura 4: Canales de mensajería



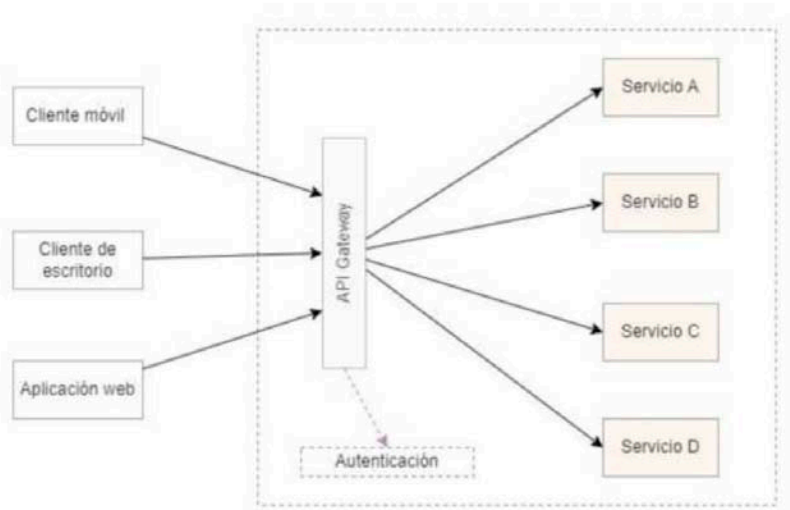
Fuente: Elaboración propia

Puertas de APIs (API Gateway): Debido a la granularidad que ofrece microservicios, la API es separada por servicio, lo que puede forzar que los clientes (entidades que consumen los servicios) interactúen con varios servicios a la vez. Se considera también que diferentes clientes necesitan información diferente, como ejemplo, una computadora comúnmente necesita información más detallada que un cliente móvil (Richardson, 2021).

La solución a este tipo de eventos radica en la implementación de una "puerta" común para cada cliente que sirve como el primer punto de entrada. Una puerta de la API funciona de dos maneras: la primera simplemente redirige la petición al servicio adecuado; la segunda, en cambio, maneja las peticiones desplegándose en múltiples servicios (Richardson, 2021).

Por lo tanto, la puerta de API se encuentra entre los clientes y los microservicios. Actúa como un proxy reverso, redirigiendo cada petición a través de los servicios. También provee otras características como autenticación, terminación SSL y caché (Anil, Buck, Jain, Warren, & Victor, 2022).

Figura 5: Puertas API



Fuente: Elaboración propia

Balanceadores de carga (LoadBalancers): Se entiende a los balanceadores de carga como los responsables de redirigir las peticiones de los que ingresan en la red a través de los servicios backend.

Muchas de las aplicaciones modernas de alto tráfico deben atender más cientos de miles de peticiones simultáneas que esperan una respuesta, como texto, imágenes, videos de manera correcta y completa. Por lo tanto, para escalar de manera rentable la mejor solución es la adición de más servidores (NGINX, 2022).

El uso de la técnica de un balanceador de carga permite redirigir las peticiones a través de los servidores que sean capaces de procesar las peticiones, de esta manera, se logra maximizar la velocidad y el uso de los recursos.

Monitoreo: El monitoreo continuo (Continuous Monitoring) es una extensión de la cultura DevOps aplicada a la arquitectura, el monitoreo continuo es un proceso automático que permite a los equipos a detectar amenazas de seguridad y cumplimiento en el ciclo de vida del software como también en su propia infraestructura (Ruck, 2021).

Continuous Monitoring permite encontrar y mitigar problemas en áreas tales como:

- Aplicación y Código: mediante el monitoreo del rendimiento de la aplicación (APM) es posible rastrear y resolver problemas críticos de rendimiento y problemas de disponibilidad. Los problemas son aislados para que no afecte al resto del sistema.

- Redes: se asegura de que los cambios de configuración realizados en el software o en las redes, no cree amenazas de seguridad.

- Bases de datos: el monitoreo en las bases de datos resulta útil para conocer métricas como el rendimiento de consultas SQL, detalles de sesiones, deadlocks, y transacciones por minuto. En los ambientes de desarrollo, los equipos pueden probar como algunos cambios afectan al rendimiento del sistema y el uso de recursos.

Documentación API: Escribir la documentación de cada servicio es vital para entender su uso, (Hunter) explica que, si los clientes no conocen la estructura de la API, el servicio no será usado. Habilitar toda la documentación, como las respuestas y errores esperados ayuda a los desarrolladores a entender rápidamente las características de cada servicio, por consiguiente, el tiempo de mantenimiento es más menor. Del mismo modo (Hunter) aconseja mantener la separación de la documentación en base a los servicios con un índice de búsqueda rápida.

DevOps

Gran parte de los procesos en la cultura DevOps ha influenciado a las practicas base que se requieren en este tipo de arquitectura. Prácticas de DevOps como integración y entrega continuas (CI/CD) son usado ampliamente para el despliegue, típicamente los microservicios están basados en la nube permitiendo a los equipos de desarrollo a tomar ventaja de escenarios o patrones como Event-Driven-Design (Jacobs, Casey, & Kaim, 2022).

Integración continua (CI): la integración continua es una practica propia de DevOps, donde los desarrolladores fusionan regularmente sus cambios de código en un repositorio central, después de lo cual se ejecutan compilaciones y pruebas automatizadas. La integración continua se refiere a la etapa de construcción o integración del proceso de lanzamiento del software (AWS, 2022).

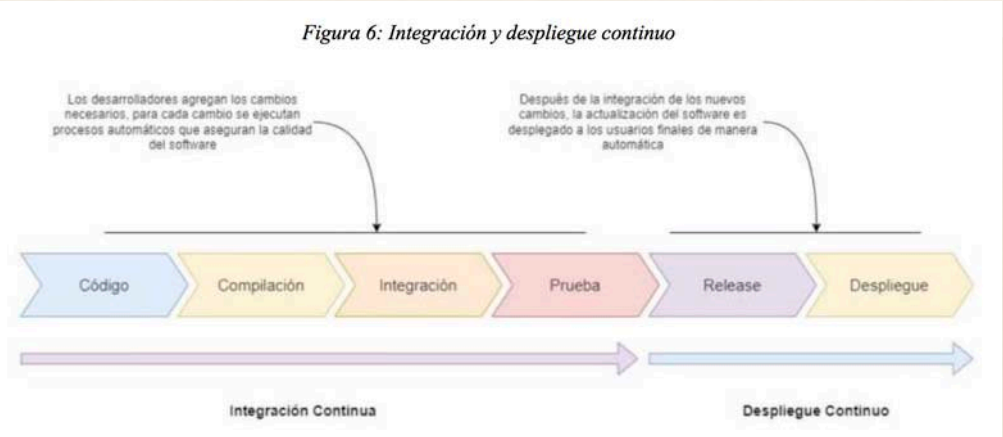
Los objetivos de la integración continua son encontrar y corregir errores más rápido, mejorar la calidad del software y reducir el tiempo que lleva validar y lanzar nuevas actualizaciones.

Entrega continua (CD): la entrega continua es una práctica de desarrollo de software en la que los cambios de código se preparan automáticamente para su lanzamiento a producción. La integración continua se expande mediante la implementation de todos los cambios de código de un entorno de prueba, cuando se implementa correctamente los desarrolladores siempre tendrán un artefacto de compilación listo para la implementación que haya pasado por un proceso de prueba estandarizado (AWS, 2022).

La entrega continua permite a los equipos de software

automatizar las pruebas para la verificación de su funcionamiento antes de la entrega a los usuarios finales.

Figura 6: Integración y despliegue continuo



Fuente: Elaboración propia

Discusión

Como se ha presentado, microservicios es una de las mejores soluciones para aquellas aplicaciones que necesitan ser escalables y fáciles de mantener, reconocer las técnicas y patrones necesarios en el análisis y diseño de estas aplicaciones juegan un papel muy importante que puede beneficiar a los líderes de equipos, arquitectos y desarrolladores que planean adentrarse a la construcción y mantenimiento de este tipo de sistemas.

Cualquier arquitectura tiene tanto sus ventajas, como también desventajas; aplicar microservicios a sistemas pequeños puede resultar contraproducente, debido a que todas las tecnologías y patrones necesarios pueden considerarse abrumadoras para muchos equipos de desarrollo, y pueden generar costos innecesarios para su implementación.

Se tiene que tomar en cuenta también que microservicios solo puede ser aplicado en culturas ágiles, debido a que muchos de sus procesos son iterativos y están orientados a la entrega continua de valor en el software.

Conclusiones

La arquitectura presenta mejoras en el rendimiento, la escalabilidad y su mantenimiento, microservicios puede verse como un sistema complejo compuesto por varios subsistemas que trabajan juntos pero que son diseñados y desarrollados de manera independiente. El uso de las técnicas y patrones introducidos crean una perspectiva general de la composición de esta arquitectura, pero que no abarca todas las posibilidades, por lo tanto, es recomendable indagar aún más en los patrones y tecnologías comúnmente usados en microservicios.

Referencias

Anil, N., Buck, A., Jain, T., Warren, G., & Victor, Y. (09 de Septiembre de 2022). The API gateway pattern versus the Direct client-to-microservice communication. Obtenido de Microsoft learn: https://learn.microsoft.com/en- us/dotnet/architecture/microservices/architect-microservice-container-applications/direct-client-to- microservice-communication-versus-the-api-gateway-pattern

AWS. (2022). What is Continuous Integration? Obtenido de aws: https://aws.amazon.com/devops/continuous- integration/

de la Torre, C., Wagner, B., & Mike, R. (2022). .NET Microservices: Architecture for Containerized .NET Applications. Washington: Microsoft Corporation.

Gillis, A. (Mayo de 2021). Containers and Virtualization. Obtenido de TechTarget: https://www.techtarget.com/searchitoperations/definition/Docker-image#:~:text=A%20Docker%20container%20is%20a,to%20run%20more%20isolated%20processes.

Hunter, T. (2017). Advanced Microservices. California: Appress.

IBM. (23 de Enero de 2020). Message Brokers. Obtenido de IBM: https://www.ibm.com/cloud/learn/message-brokers IBM. (14 de Mayo de 2021). SOA vs. Microservices. Obtenido de IBM: https://www.ibm.com/cloud/blog/soa-vs- microservices

Jacobs, M., Casey, C., & Kaim, E. (21 de Julio de 2022). What are Microservices? Obtenido de Microsoft: https://learn.microsoft.com/en-us/devops/deliver/what-are-microservices

Lukmna, A. (24 de Marzo de 2022). Why is Microservice Orchestration Important Now? Obtenido de orkes: https://orkes.io/content/blog/why-is-microservice-orchestration-important-

now#:~:text=A%20microservice%20orchestration%20workflow%20is,referred%20to%20as%20the%20orches trator.

Nadareishvili, I., Mitra, R., McLarty, M., & Amundsen, M. (s.f.). Microservice Architecture. O'Reilly.

NGINX. (2022). What Is Load Balancing? Obtenido de NGINX: https://www.nginx.com/resources/glossary/load- balancing/

Novoseltseva, E. (18 de abril de 2020). Beneficios Y Ejemplos De La Implementación De Los Microservicios.

Obtenido de Apiumhub: https://apiumhub.com/es/tech-blog-barcelona/los-microservicios/

Pahl, C., & Jamshidi, P. (2016). Microservices: A Systematic Mapping Study.

Richardson, C. (2019). Microservices Pattern. New York: Manning.

Richardson, C. (2021). API Gateway. Obtenido de Microservices Architecture: https://microservices.io/patterns/apigateway.html

Ruck, D. (22 de Abril de 2021). Continuous Monitoring: What Is It and How Is it Impacting DevOps Today? Obtenido de Lightrun: https://lightrun.com/best-practices/continuous-monitoring-what-is-it-and-how-is-it-impacting- devops-today/

Artículo Recibido: 10/03/2023

Artículo Aceptado: 12/05/2023

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN MÉDICA

Autor:
Rodrigo Casilla Uri
rcasilla10@gmail.com

Resumen

Los riesgos durante el desempeño del trabajo es una situación inherente a cualquier actividad humana. La Seguridad de la información se define como: la condición que garantiza que los pacientes de un centro de atención en salud, estén libres de riesgo a que su historial clínico sea divulgado o en todo caso robado. La construcción de la cultura de prevención parte del conocimiento de los riesgos, la cultura de la seguridad de la información se encuentra directamente relacionada con la calidad de atención del servicio que se otorga, por lo cual en las instituciones de salud estos términos son de especial interés. Hablar de confianza implica determinar todo el riesgo que pudieran provocar un daño considerable a los sistemas.

El presente documento resalta lo importante que se tiene la información del paciente en un Centro de Atención en salud, basadas en políticas de seguridad y la confiabilidad y confianza del paciente, utilizando estándares internacionales de Seguridad de la Información, "La Seguridad de la Información está apoyada en 3 pilares fundamentales de la seguridad estos son: Disponibilidad, Integridad, Confidencialidad.

Palabras Clave: Seguridad, información, Riesgo, Cultura, Paciente, datos, normas

Introducción

Tradicionalmente, los datos se almacenaban en una base de datos o solamente en documentación física dentro de las instalaciones seguras de los hospitales. Un sistema de seguridad bien

establecido podría garantizar que ningún usuario no autorizado pueda acceder a la información confidencial de los pacientes; con el avance de la tecnología ha introducido varios métodos para guardar datos, como la sistematización de atención médica, que permite a los hospitales almacenar una gran cantidad de datos, los profesionales de la seguridad de la información tienen que encontrar soluciones a través de las cuales puedan almacenar datos de manera segura.

Los hospitales almacenan información confidencial de pacientes, como el diagnóstico de enfermedades, historial clínico, información de contacto, número de seguro social. Los piratas informáticos extraen esta información a través de medios no autorizados y la utilizan indebidamente para ganar algo de dinero. Los profesionales de tecnologías de la información deben garantizar que los médicos puedan acceder fácilmente a los datos y que estén lejos del acceso a personas externas que quieren sobar información.

La seguridad de la información se consigue mediante la implantación de un conjunto adecuado de controles, los que incluye políticas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware, para asegurar que se cumplan los objetivos específicos de seguridad de la organización.

Contenido

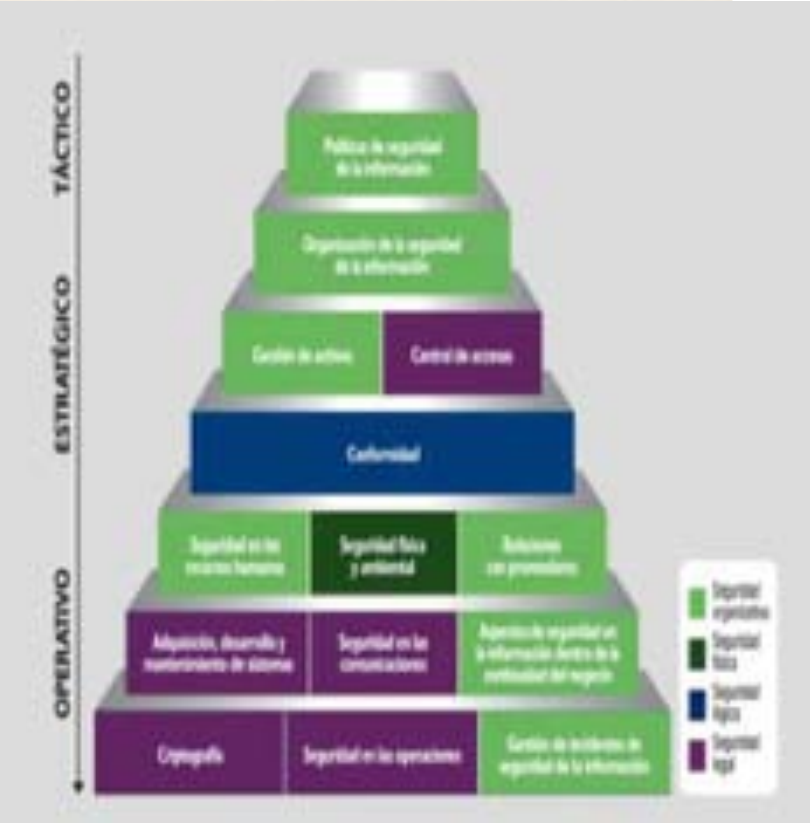
La protección de datos en los centros de atención en salud es cada vez más necesaria y se convierten en un punto crítico para la protección de datos pues manejan información sensible sobre el estado de salud o condiciones de los pacientes.

Sumado a esto, la cantidad de funcionarios de un Centro de atención en salud que pueden tener acceso a esta información es relativamente alta por lo que una fuga de información, especialmente en esta era digital, debe ser tratada con cuidado.

La protección de datos personales es un hecho, hoy en día un usuario puede saber qué datos digitales manejan las organizaciones y habilitar o deshabilitar su uso para fines comerciales, de investigación o de publicación.

Donde se utilizará como un como iniciativa implementación como normativa la ISO 27002, la cual tiene como objetivo de resguardar la información de los pacientes, donde se puede observar en la siguiente imagen la estructura de los dominios de seguridad de la ISO/IEC 27002.

IMAGEN 1.1



Fuente: http s://portal. aenormas. aenor. com/revista/309/ciberseguridad2 - 2-309.html

Se proporcionará orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos de la

organización bajo las leyes y normativas pertinentes en base a la realización que de las políticas de seguridad de la información en el Centro de atención en salud.

POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

Para ayudar a concentrar los esfuerzos, aquí hay algunas políticas de seguridad de la información que pueden ser aplicados para la organización Caja Nacional de Salud

1. Establecer una cultura de seguridad

Las políticas de seguridad no son buenas a menos que los funcionarios estén dispuestos a proteger el hospital y seguir mejores prácticas. Para esto, el equipo encargado de la seguridad dela información debe ser el primero en establecer la protección de datos como una prioridad para la institución, dar ejemplo, capacitar a sus funcionarios y exigir que se cumplan los protocolos.

2. Controle el acceso a la información protegida

Indiscutiblemente uno de los filtros más básicos, pero más importantes, es a qué funcionarios se le otorga acceso al sistema y con qué tanta profundidad. Determine quién necesita acceso a los registros de pacientes y cree perfiles que permitan únicamente a la información que realmente necesitan.

3. Mantener una buena higiene cibernética

Los hábitos saludables son tan vitales para los sistemas hospitalarios como lo son para la salud de los asegurados:

- Desinstalar aplicaciones innecesarias
- Cambiar configuraciones predeterminadas
- Borrar datos de dispositivos desechados

4. Configurar correctamente un cortafuego o “firewall”

Busque personal capacitado para configurar firewalls que protejan el software del centro de atención en salud de ataques externos.

Los firewalls pueden basarse en hardware o software y un experto en seguridad informática podrá aconsejarle de acuerdo a sus necesidades y sensibilidad de la información.

5. Instalar y mantener un software antivirus

El software antivirus protege contra códigos maliciosos que pueden comprometer los sistemas que se utilizan el centro de atención en salud.

Los virus son una forma común en que los piratas informáticos obtienen acceso a los sistemas hospitalarios y evolucionan constantemente por lo que es indispensable mantener activos antivirus en todos los equipos.

6. Copia de seguridad de los datos

Los sistemas son vulnerables a calamidades inesperadas como incendios, inundaciones o el pirateo malicioso.

Hacer una copia de seguridad de los datos de manera regular (para determinar la regularidad con que debe hacer backups piense qué pasaría si pierde la información de un mes, una semana, un día, o incluso, una hora) y mantener esas copias en un lugar seguro.

7. Use contraseñas seguras y cámbielas regularmente

- Utilice las mejores prácticas de contraseña segura, tales como:

- Utilice múltiples contraseñas para diferentes sistemas
- Cambiar contraseñas regularmente
- Use contraseñas complicadas que no son fáciles de adivinar
- Utilice la autenticación multifactor (que se requiere para los sistemas de prescripción electrónica)
- Permitir el restablecimiento de contraseñas para los usuarios que olvidan sus contraseñas para evitar que las contraseñas escritas queden en ubicaciones vulnerables

8. Control de acceso al Hardware

Los computadores portátiles o los dispositivos de almacenamiento de datos que se movilizan de lugar en lugar son fuentes comunes de violaciones de datos en la atención médica.

Estos dispositivos deben mantenerse en lugares seguros donde usuarios ajenos no puedan acceder a ellos y es altamente recomendable que se restrinja su uso fuera de las instalaciones,

Por último, siempre tenga en mente que cualquier intrusión en sus bases de datos o sistemas pueden ser usadas para crímenes de desprestigio o discriminación en contra del paciente, y por supuesto, en contra del centro de atención en salud

Una vez realizada las políticas que tiene que tomar en cuenta para la implantación de la seguridad de la información del centro de atención en salud

La norma ISO/IEC 27002 es una herramienta sencilla que permitirá establecer políticas, y controles bajo el objetivo de disminuir los riesgos que tienen los activos de la organización. En primer lugar, obtenemos una reducción de riesgos debido al establecimiento y seguimiento de controles sobre ellos. Con ello lograremos reducir las amenazas hasta alcanzar un nivel asumible por nuestra organización. De este modo si se produce una incidencia, los daños se minimizan y la continuidad del negocio está asegurada. En segundo lugar, se produce un ahorro de costes derivado de una racionalización de los recursos. Se eliminan las inversiones innecesarias e ineficientes como las producidas por desestimar o sobrestimar riesgos. En tercer lugar, la seguridad se considera y se convierte en una actividad de gestión. La seguridad deja de ser un conjunto de actividades más o menos organizadas y pasa a transformarse en un ciclo de vida metódico y controlado, en el participa toda la organización. En cuarto lugar, la organización se asegura del cumplimiento de la legislación vigente y se evitan riesgos y costes innecesarios. La entidad se asegura del cumplimiento del marco legal que protege a la empresa de aspectos que probablemente no se habían tenido en cuenta anteriormente. Por último, pero no por ello menos importante, la certificación del sistema de gestión de seguridad de la información contribuye a mejorar la competitividad en el mercado, diferenciando a las empresas que lo han conseguido y haciéndoles más fiables e incrementando su prestigio.

La parte principal de la norma se encuentra distribuida en los siguientes dominios, que corresponden a controles de seguridad de la información. Es importante recordar que el centro de

atención en salud puede utilizar esas directrices como base para el desarrollo del SGSI. Como sigue:

Política de Seguridad de la Información

Se crearon políticas de seguridad de la información que contienen conceptos de seguridad de información de los pacientes, la utilización del sistema y toda la parte tecnológica, una estructura para establecer los objetivos y las formas de control, el compromiso de la dirección del centro de atención en salud hacer cumplir toda la política resaltada.

Organización de la Seguridad de la Información

Se gestionará dentro del centro de atención en salud una estructura de manera adecuada, para eso todas las actividades de seguridad de información se deben coordinar con el director del establecimiento y el equipo encargado de la seguridad de la información para tener responsabilidades bien definidas y proteger la información de los pacientes de forma confidencial.

Gestión de activos

Activo, según la norma, es cualquier cosa que tenga valor para el centro de atención en salud y que necesita ser protegido. Pero para ello los activos deben ser identificados y clasificados, de modo que un inventario pueda ser estructurado y posteriormente mantenido. Además, deben seguir reglas documentadas, que definen qué tipo de uso se permite hacer con los activos.

Seguridad en recursos humanos

Antes de la contratación de un empleado para el centro de atención en salud, proveedores es importante que sea debidamente analizado, principalmente si se trata de información de carácter confidencial. La intención de esta sección es mitigar el riesgo de robo, fraude o mal uso de los recursos. Y cuando el empleado esté trabajando en el centro de atención en salud, debe ser consciente de las amenazas relativas a la seguridad de la información, así como de sus responsabilidades y obligaciones.

Seguridad física y del medio ambiente

Los equipos e instalaciones de procesamiento de información crítica o sensible deben mantenerse en áreas seguras dentro del centro, con niveles y controles de acceso apropiados, incluyendo protección contra amenazas físicas, ambientales dando como encargado a un personal de confianza para el resguardo correspondiente.

Seguridad de las operaciones y comunicaciones

Es importante que estén definidos los procedimientos y responsabilidades por la gestión y operación de todos los recursos de procesamiento de la información. Esto incluye la gestión de servicios tercerizados, la planificación de recursos de los sistemas para minimizar el riesgo de fallas, la creación de procedimientos para la generación de copias de seguridad y su recuperación, así como la administración segura de las redes de telecomunicación.

Control de acceso

El acceso a la información, así como a los recursos de procesamiento de la información y los procesos que se realizan dentro del centro de atención en salud, debe ser controlado con base en los requisitos del centro y en la seguridad de la información. Debe garantizarse el acceso de usuario autorizado y prevenido el acceso no autorizado a los sistemas de información, a fin de evitar daños a documentos y recursos de procesamiento de la información que estén al alcance de cualquiera.

Adquisición, desarrollo y mantenimiento de sistemas

Los requisitos de seguridad de los sistemas de información deben ser identificados y acordados con la dirección del centro de atención en salud y el equipo encargado de la seguridad de la información antes de su desarrollo y/o de su implementación, para que así puedan ser protegidos para el mantenimiento de su confidencialidad, autenticidad o integridad por medios criptográficos.

Gestión de incidentes de seguridad de la información

Los procedimientos formales de registro y escalonamiento deben ser establecidos y los empleados, proveedores y terceros deben ser conscientes de los procedimientos para notificar los eventos de seguridad de la información para asegurar que se comuniquen lo más rápido posible y corregidos en tiempo hábil.

Gestión de continuidad del negocio

Los planes de continuidad del negocio deben ser desarrollados e implementados, con el fin de impedir la interrupción de las actividades del negocio y asegurar que las operaciones esenciales sean rápidamente recuperadas.

Conformidad

Es importante evitar la violación de cualquier ley criminal o civil, garantizando estatutos, regulaciones u obligaciones contractuales y de cualesquiera requisitos de seguridad de la información. En caso necesario, el centro de atención en salud puede contratar una consultoría especializada, para que se verifique su conformidad y adherencia a los requisitos legales y reglamentarios.

Conclusiones

Luego del estudio, análisis e implementación de la norma ISO 27002, para el centro de atención en salud para la información médica de los pacientes, se pudo detectar muchas deficiencias en la parte de seguridad de la información. Como consecuencia, la información en todas sus formas y estados Es importante recalcar que, si se cumple al 100% con las políticas desarrolladas por el equipo de Seguridad de la Información, no se garantiza que no tengan problemas de seguridad ya que no existe la seguridad al 100%; con el manual de políticas de seguridad de la información y con el cumplimiento de las mismas da lugar a minimizar los riesgos asociados a los activos reduciendo impactos, fuga de información originados por

la carencia de las normas y políticas de seguridad de la información. Con el manual de políticas de seguridad de la información, proporcionara una guía a seguir para trabajar en los aspectos de seguridad, para lo cual debe tomar seriedad sobre lo documentado y realizar proyectos de enmendadura basados en las políticas de seguridad y por último debe realizar campañas de concientización sobre los temas abordados.

Bibliografía

GUIA DE IMPLEMENTACION ISO 27001:

https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISQ-27001-Guia-de-implantacion.pdf

PORTAL DE ORIENTACION ISO 27002: https://static.eoi.es/inline/une-en iso-iec 27002 norma mincotur.pdf

ISO 27002, Portal de soluciones técnicas y organizativas a los controles de la ISO/IEC 27002: http://iso27002.wiki.zoho.com

Artículo Recibido: 11/03/2023

Artículo Aceptado: 12/05/2023

SEGURIDAD EN EL CONTROL DE ACCESOS BASADO EN EL REGLAMENTO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y EL ESTÁNDAR PCI DSS PARA PROCEDIMIENTO OPERATIVOS

Autor:

Luis Alberto Pilco Vargas

lpilcov@outlook.com

Resumen

La Administración del Control de Accesos, hace referencia al nivel de privilegios de un usuario basados en el mínimo privilegio para su objetivo, por lo que existen reglamentos nacionales como el Reglamento para la Gestión de Seguridad de Información (RGSI) y Estándares internacionales como el PCI DSS, que nos indican controles para la administración de este por lo que las empresas implementan procedimientos operativos. Los procedimientos operativos son conjuntos de instrucciones que describe todos los pasos y actividades relevantes de un proceso basándose en ambos estándares.

Palabras Clave Seguridad, Información, PCI-DSS, RGSI, Estándares, Cumplimiento, Certificación, Modelos, Métodos y Principios

Abstract

The Access Control Administration refers to the level of privileges of a user based on the minimum privilege for its objective, for it there are national regulations such as the Regulation for Information Security Management (RGSI) and international standards such as the PCI DSS, which do not indicate controls for its administration, so companies implement operating procedures. Operating procedures are sets of instructions that describe all the relevant steps and activities of a process required in both standards.

Keywords Security, Information, Audit, Corporate Governance Standards, Compliment, Certification, Models, Methods, and Principles.

1. INTRODUCCIÓN

La información es el activo más preciado en toda organización y entidades en general, por tanto, se deben tomar todas las precauciones necesarias, para mantener y preservar la misma.

La gestión de la seguridad de la información es uno de los componentes para establecer un nivel adecuado de controles y prácticas que son exigidas en la Normativa Nacional e Internacional.

Dentro de la gestión de la seguridad de la información se contempla la administración de Control de Accesos que según el RGSI es de cumplimiento obligatorio, así también para el estándar PCI-DSS. Por lo cual se realizará el nexo entre ambos para establecer controles y procedimientos operativos fortaleciendo los criterios de la seguridad de la información.

Estos lineamientos se basarán en los requerimientos definidos por PCI-DSS y el Reglamento para la Gestión de Seguridad de la Información de la Recopilación de Normas del Sistema Financiero de la Autoridad de Supervisión del Sistema Financiero - ASFI.

2. CONTENIDO

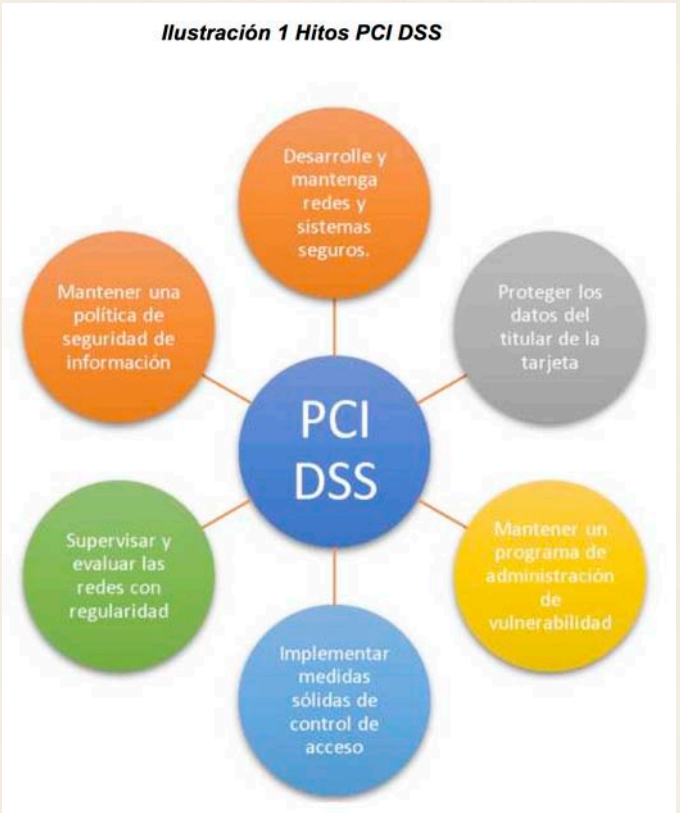
a) PCI-DSS

El Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (Payment Card Industry Data Security Standard - PCI DSS) es un estándar de seguridad publicado por el PCI DSS y orientado a la definición de controles para la protección de los datos del titular de la tarjeta y datos sensibles de autenticación durante su procesamiento, almacenamiento y/o transmisión.

Las Normas de seguridad de datos de la industria de tarjetas de pago (PCI DSS) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar la adopción de medidas de seguridad uniformes a nivel mundial. La PCI DSS proporciona una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de cuentas. La PCI DSS se aplica a todas las entidades que participan en el procesamiento de las tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios. La PCI DSS se aplica a todas las entidades que almacenan, procesan o transmiten datos del titular de la tarjeta (CHD) y/o datos confidenciales de autenticación (SAD). (PCI Security Standards Council, 2018)

En total, el estándar PCI DSS cuenta con 12 requisitos que se esquematizan en 6 grupos o "Hitos" de cumplimiento.

Ilustración 1 Hitos PCI DSS



Fuente: (PCI Security Standards Council, 2018)

1) Desarrolle y mantenga redes y sistemas seguros

1. Instalar y mantener una configuración de firewall para proteger los datos de los titulares de tarjetas.

2. No utilizar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.

2) Proteger los datos del titular de la tarjeta

3. Proteger los datos almacenados de los titulares de tarjetas.

4. Cifrar la transmisión de los datos de los titulares de tarjetas a través de redes públicas abiertas.

3) Mantener un programa de administración de vulnerabilidad

5. Usar y actualizar con regularidad el software antivirus.

6. Desarrollar y mantener sistemas y aplicaciones seguras.

4) Implementar medidas sólidas de control de acceso

7. Limitar el acceso a los datos de los titulares, únicamente a lo que los negocios necesiten saber.

8. Asignar una identificación única a cada persona con acceso a una computadora.

9. Restringir el acceso físico a los datos de los titulares de tarjetas.

5) Supervisar y evaluar las redes con regularidad

10. Rastrear y monitorear todo acceso a los recursos de la red y a los datos de titulares de tarjetas.

11. Probar con regularidad los sistemas y procesos de seguridad.

6) Mantener una política de seguridad de información

12. Mantener una política que aborde la seguridad de la información. (PCI Security Standards Council, 2018)

a) Reglamento para la Gestión de la Seguridad de la Información

El Reglamento tiene por objeto establecer las directrices y requisitos mínimos que las Entidades de Intermediación Financiera, Empresas de Servicios Financieros Complementarios y Sociedades Controladoras de Grupos Financieros, deben cumplir para la gestión de seguridad de la información, de acuerdo con su naturaleza, tamaño y estructura, así como con la complejidad de los procesos y operaciones que realizan.

- Sección 2: Planificación estratégica, estructura y organización de los recursos de tecnologías de la información.

- Sección 3: Administración de la seguridad de la Información.

- Sección 4: Administración del control de accesos

- Sección 5: Desarrollo, mantenimiento e implementación de sistemas de Información.

- Sección 6: Gestión de operaciones de tecnología de información
- Sección 7: Gestión de seguridad en redes y comunicaciones
- Sección 8: Gestión de seguridad en transferencias y transacciones electrónicas
- Sección 9: Gestión de incidentes de seguridad de la información
- Sección 10: Continuidad del negocio
- Sección 11: Administración de servicios y contratos con terceros relacionados con tecnologías de la información. (ASFI, 2017)

Siendo la sección 4 la cual se abordará en el presente artículo, esta compuesta por los siguientes artículos:

- Artículo 1 ° - (Administración de cuentas de usuarios)
- Artículo 2° - (Administración de privilegios)
- Artículo 3° - (Administración de contraseñas de usuarios)
- Artículo 4° - (Monitoreo de actividades de los usuarios)
- Artículo 5° - (Registros de seguridad y pistas de auditoría) (ASFI, 2017)

b) Administración del Control de Accesos

Para el cumplimiento de la sección 4 del Reglamento de Gestión de Seguridad de la Información que se encuentra enfocado en la administración de cuentas de usuarios y privilegios tomaremos en cuenta los siguientes Hitos, procedimientos y requerimientos que nos proporciona el estándar PCI-DSS:

Cumplimiento del Artículo 1, incisos a, c y d:

PCI-DSS Hito 4, requisito 7.2:

Establezca un sistema de control de acceso para los componentes del sistema que restrinja el acceso según la necesidad del usuario de conocer y que se configure para "negar todo", salvo que se permita específicamente.

Este sistema de control de acceso debe incluir lo siguiente:

7.2.1 Cobertura de todos los componentes del sistema.

7.2.2 La asignación de privilegios a una persona se basa en la clasificación del trabajo y su función.

7.2.3 Configuración predeterminada de "negar todos".

Procedimiento 7.2: Evalúe los parámetros del sistema y la documentación del proveedor para verificar que el sistema de control de acceso se implemente de la siguiente manera:

Procedimiento 7.2.1: Confirme que los sistemas de control de acceso se implementen en todos los componentes del sistema.

Procedimiento 7.2.2: Confirme que los sistemas de control de acceso estén configurados de manera tal que los privilegios asignados a una persona se realicen según la clasificación del trabajo y la función.

Procedimiento 7.2.3: Confirme que los sistemas de control de acceso cuenten con la configuración predeterminada de “negar todos”.

Cumplimiento del Artículo 1, inciso b y Artículo 2

PCI-DSS Hito 4, requisito 8.1.1:

Asigne a todos los usuarios una ID exclusiva antes de permitirles acceder a los componentes del sistema o a los datos del titular de la tarjeta.

Procedimiento 8.1.1: Entreviste al personal administrativo y confirme que todos los usuarios tengan asignada una ID exclusiva para tener acceso a los componentes del sistema o los datos del titular de la tarjeta.

Hito 4, requisito 8.1.3:

Cancele de inmediato el acceso a cualquier usuario cesante.

Procedimiento 8.1.3.a: Seleccione una muestra de los usuarios cesantes en los últimos seis meses y revise las listas de acceso de usuarios actuales, tanto para acceso local como remoto, para verificar que sus ID se hayan desactivado o eliminado de las listas de acceso.

Procedimiento 8.1.3.b: Verifique que todos los métodos de autenticación físicos, como tarjetas inteligentes, tokens, etc., se hayan devuelto o desactivado.

Hito 4, requisito 8.1.4:

Elimine o inhabilite las cuentas de usuario inactivas, al menos, cada 90 días.

Procedimiento 8.1.4: Observe las cuentas de usuarios y verifique que se eliminen o inhabiliten las que lleven más de 90 días inactivas.

Hito 4, requisito 8.2.2:

Verifique la identidad del usuario antes de modificar alguna credencial de autenticación, por ejemplo, restablezca la contraseña, entregue nuevos tokens o genere nuevas claves.

Procedimiento 8.2.2: Revise los procedimientos de autenticación para modificar las credenciales de autenticación y observe al personal de seguridad a fin de verificar que, si un usuario solicita el restablecimiento de una credencial de autenticación por teléfono, correo electrónico, Internet u otro método no personal, la identidad del usuario se verificará antes de modificar la credencial de autenticación.

Cumplimiento del Artículo 3: PCI-DSS Hito 2, requisito 2.1:

Siempre cambie los valores predeterminados por el proveedor y elimine o deshabilite las cuentas predeterminadas innecesarias antes de instalar un sistema en la red. Esto rige para TODAS las contraseñas predeterminadas, por ejemplo, entre otras, las utilizadas por los sistemas operativos, los softwares que prestan servicios de seguridad, las cuentas de aplicaciones y sistemas, los terminales de POS (puntos de venta), las aplicaciones de pago, las cadenas comunitarias de SNMP (protocolo simple de administración de red), etc.

Procedimiento 2.1.a: Escoja una muestra de los componentes del sistema e intente acceder a los dispositivos y aplicaciones (con la ayuda del administrador del sistema) con las cuentas y contraseñas predeterminadas por el proveedor y verifique que se hayan cambiado TODAS las contraseñas predeterminadas (incluso las de los sistemas operativos, los software que prestan servicios

de seguridad, las cuentas de aplicaciones y sistemas, los terminales de POS [puntos de ventas], las cadenas comunitarias de SNMP [protocolo simple de administración de red]). (Utilice los manuales y las fuentes de los proveedores que se encuentran en Internet para encontrar las cuentas y las contraseñas proporcionadas por estos). Las personas malintencionadas (externas e internas a la organización), por lo general, utilizan configuraciones predeterminadas por los proveedores, nombres de cuentas y contraseñas para poner en riesgo el software del sistema operativo, las aplicaciones y los sistemas donde están instalados. Debido a que estos parámetros predeterminados suelen publicarse y son conocidos en las comunidades de hackers, cambiar estas configuraciones contribuirá a que el sistema sea menos vulnerable a los ataques. Incluso si una cuenta predeterminada no se creó para usarse, cambiar la contraseña predeterminada por una contraseña única y sólida y, después, deshabilitar la cuenta, evitará que personas maliciosas vuelvan a habilitar la cuenta y accedan con la contraseña predeterminada.

Procedimiento 2.1.b: Para la muestra de los componentes del sistema, verifique que todas las cuentas predeterminadas innecesarias (incluso las cuentas que usan los sistemas operativos, los softwares de seguridad, las aplicaciones, los sistemas, los terminales de POS (puntos de ventas), SNMP (protocolo simple de administración de red), etc.) se hayan eliminado o deshabilitado.

Procedimiento 2.1.c: Entreviste al personal, revise la documentación de respaldo y verifique lo siguiente:

- Se cambian todos los valores predeterminados por proveedores (incluidas las contraseñas predeterminadas de sistemas operativos, software que presta servicios de seguridad, cuentas de aplicaciones y sistemas, terminales de POS, cadenas de comunidad de protocolo simple de administración de red [SNMP], etc.) antes de instalar un sistema en la red.
- Se cambian o inhabilitan las cuentas predeterminadas

Cumplimiento del Artículo 4:

Hito 4, requisito 8.1.6:

Limite los intentos de acceso repetidos mediante el bloqueo de la ID de usuario después de más de seis intentos

Procedimiento 8.1.6.a: En el caso de una muestra de componentes del sistema, inspeccione los parámetros de configuración del sistema para verificar que los parámetros de autenticación se encuentren configurados de manera que se solicite que se bloquee la cuenta del usuario después de realizar, como máximo, seis intentos de inicio de sesión no válidos.

Procedimiento 8.1.6.b: Procedimientos de pruebas adicionales para los proveedores de servicios: Revise los procesos internos y la documentación de cliente/usuario y observe los procesos implementados para verificar que las cuentas de usuarios no consumidores se bloqueen de forma temporal después de, como máximo, seis intentos no válidos de acceso.

Hito 4, requisito 8.1.7:

Establezca la duración del bloqueo a un mínimo de 30 minutos o hasta que el administrador habilite la ID del usuario.

Procedimiento 8.1.7: En el caso de una muestra de componentes del sistema, inspeccione los parámetros de configuración del sistema para verificar que los parámetros de las contraseñas se encuentren configurados de manera que solicite que, al bloquear la cuenta de

un usuario, esta permanezca bloqueada un mínimo de 30 minutos o hasta que el administrador del sistema la restablezca.

Hito 4, requisito 8.1.8:

Si alguna sesión estuvo inactiva durante más de 15 minutos, solicite al usuario que vuelva a

escribir la contraseña para activar la terminal o la sesión nuevamente.

Procedimiento 8.1.8: En el caso de una muestra de componentes del sistema, inspeccione los parámetros de configuración del sistema para verificar que las funciones de tiempo máximo de inactividad del sistema/sesión se encuentren establecidos en 15 minutos o menos.

Hito 4, requisito 8.2.3: Las contraseñas/frases deben tener lo siguiente:

- Una longitud mínima de siete caracteres.
- Combinación de caracteres numéricos y alfabéticos. De manera alternativa, la contraseña/frase debe tener una complejidad y una solidez, al menos, equivalente a los parámetros que se especifican anteriormente.

Procedimiento 8.2.3.a: En el caso de una muestra de los componentes del sistema, inspeccione los parámetros de configuración del sistema para verificar que los parámetros de la contraseña del usuario se encuentren configurados de manera que soliciten, al menos, la siguiente solidez o complejidad:

- Una longitud mínima de siete caracteres.
- Combinación de caracteres numéricos y alfabéticos.

Procedimiento 8.2.3.b Procedimientos de pruebas adicionales para los proveedores de servicios: Revise los procesos internos y la documentación del cliente/usuario para verificar que se solicite que las contraseñas de usuarios no consumidores cumplan, al menos, con la siguiente solidez o complejidad:

- Una longitud mínima de siete caracteres.
- Combinación de caracteres numéricos y alfabéticos.

Hito 4, requisito 8.2.4: Cambie la contraseña/frase de usuario, al menos, cada 90 días.

Procedimiento 8.2.4.a: En el caso de una muestra de componentes del sistema, inspeccione los parámetros de configuración del sistema para verificar que los parámetros de las contraseñas de usuario se encuentren configurados de manera que se le solicite al usuario cambiar su contraseña, al menos, cada 90 días.

Procedimiento 8.2.4.a: Procedimientos de pruebas adicionales solo para proveedor de servicios. los proveedores de servicios: Revise los procesos internos y la documentación del cliente/usuario y verifique lo siguiente:

- Las contraseñas de usuarios no consumidores se deben cambiar periódicamente
- Se debe orientar a los usuarios no consumidores sobre cuándo y en qué situaciones deben cambiar las contraseñas.

Hito 4, requisito 8.2.5: No permita que una persona envíe una contraseña/frase nueva que sea igual a cualquiera de las últimas cuatro contraseñas/frases utilizadas

Procedimiento 8.2.5.a: Para una muestra de componentes del sistema, obtenga e inspeccione los parámetros de configuración del sistema para verificar que los parámetros de las contraseñas se encuentren configurados para que soliciten que las nuevas contraseñas no

sean iguales a las últimas cuatro contraseñas utilizadas.

Procedimiento 8.2.5.b: Procedimientos de pruebas adicionales para los proveedores de servicios: Revise los procesos internos y la documentación de cliente/usuario para verificar que las nuevas contraseñas de usuarios no consumidores no puedan ser iguales a las últimas cuatro contraseñas utilizadas anteriormente.

Hito 4, requisito 8.2.6:

Configure la primera contraseña/frase y las restablecidas en un valor único para cada usuario y cámbiela de inmediato después del primer uso

Procedimiento 8.2.6: Revise los procedimientos de contraseña y observe al personal de seguridad para verificar que las primeras contraseñas para nuevos usuarios, y las contraseñas restablecidas para usuarios existentes, se configuren en un valor único para cada usuario y se cambien después del primer uso.

3. CONCLUSIÓN

El cumplimiento de los reglamentos, así como de los estándares nos ayudan a afianzar que las organizaciones que procesan, almacenan y transmiten información mantienen un entorno seguro. Por el cual utilizar o basarse en no solo un estándar o reglamento es una buena practica para asegurarse que los datos de la organización se encuentran protegidos, en este caso contra el acceso no autorizado y el uso indebido. Llegando así al cumplimiento de la sección 4 del Reglamento para la Gestión de Seguridad de la Información de la Recopilación de Normas del Sistema Financiero de la Autoridad de Supervisión del Sistema Financiero - ASFI.

PCI-DSS nos proporciona como se menciono en el artículo varios hitos y a su vez requerimientos que pueden ser aplicados para el cumplimiento del reglamento ayudándonos a identificar controles y procedimientos no solo para la sección 4 del RGSI.

4. BIBLIOGRAFÍA

ASFI. (2017). Reglamento de la Seguridad de la información. La Paz.

Depok, U. I. (2020). Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. Indonesia.

PCI Security Standards Council, L. (2018). PCI (industria de tarjetas de pago) Normas de seguridad de datos.

Zevallos, C. O. (2016). Mejores prácticas en la Implantación de ISO27001:2013 y PCI/DSS 3.1.

Artículo Recibido: 10/03/2023

Artículo Aceptado: 12/05/2023

GAMIFICACIÓN: UNA FORMA DIVERTIDA DE APRENDER

Autora:
Mariana Nicole Caballero Magnus
mari.ncm.2004@gmail.com

Resumen

Este trabajo se enfoca principalmente en la gamificación, una innovación en el campo del aprendizaje como método aplicable para funcionar en la Universidad La Salle. El propósito de su aplicación se centra en el hecho de que es una excelente fuente motivación capaz de despertar el interés de los estudiantes promoviendo su permanencia en sus estudios, a través de juegos y/o concursos, en plataformas virtuales o en el mismo salón donde se lleva a clase la lección, previa planificación.

Palabras clave Gamificación, estudios, motivación.

Abstract

This work focuses mainly on gamification, wich is a new method in the learning field and can be applicable method at La Salle University. The main reason for it is that gamification is an excellent source of motivation capable of arousing the interest of students and achieving permanence in their studies, through games and/or contests, on virtual platforms or in the same room where the lesson is taken to class, based on a previous planification.

Keywords Gamification, studies, motivation.

Introducción

Durante la pandemia de Covid-19 desatada en la gestión 2019, surge la necesidad de las clases virtuales a nivel mundial. En Bolivia,

esta situación ha develado la poca formación de los docentes en el ámbito tecnológico y, con relación a los estudiantes, la carencia y/o deficiencia en el acceso a los medios digitales (computador, celular, aplicaciones web y de comunicación, etc.). De acuerdo a un artículo publicado en mayo de 2020 en el periódico Los Tiempos, se identificaron cinco problemas al respecto ". . .la brecha digital; la falta de capacitación de profesores, estudiantes y padres; la falta de un plan de contingencia y a largo plazo; las presiones sociales, y la ausencia de un nuevo modelo educativo que incluya procesos semipresenciales. . ." (Peredo, Identifican cinco problemas para la educación en tiempos de pandemia | Los Tiempos, 2022)

Este hecho no ha sido ajeno al ámbito universitario, particularmente en aquellas carreras en las que la práctica es indispensable para adquirir mejores conocimientos. Es por esta razón que surge la inquietud para motivar a los docentes a emprender en las aulas nuevas formas de enseñanza, que a su vez incentiven y motiven a los estudiantes la continuidad de sus estudios.

En ese contexto, la presente investigación tiene como objetivo principal proponer la implementación de la gamificación dentro de la currícula académica a fin de incrementar la motivación al conocimiento en los estudiantes, fundamentalmente de los primeros semestres universitarios.

Un artículo publicado en la página del Centro de Enseñanza Técnica y Superior de México (CETYS) resalta sobre la importancia de la educación, que:

"En lo individual… es un derecho fundamental de todas las personas y la clave para la construcción de sociedades más justas y equitativas.

A nivel global, la educación es considerada un factor de producción, pues permite acabar de raíz con muchos de los problemas económicos de una nación y funge como instrumento regulador de las desigualdades sociales. Sus funciones primordiales son:

Mejorar los niveles de empleabilidad en el país.

Afirmar los valores y la identidad cultural de las sociedades.

Diversificar los campos de desarrollo para la población joven.

Fortalecer la democracia y el estado de derecho.

Fomentar la innovación científica y tecnológica." (CETYS, 2022)

En el marco de esta afirmación, se considera que estas funciones primordiales también se ajustan a la realidad de nuestro país. Por lo tanto, es importante, que dentro de la currícula académica se pueda prever innovaciones que incentiven y motiven en mayor grado a los estudiantes que emprenden el desafío de estudiar y, sobre todo, culminarr una carrera universitaria.

Con este objetivo, en el presente artículo se propone la inserción de la nueva tendencia educativa conocida como GAMIFICACIÓN.

¿QUÉ ES LA GAMIFICACIÓN?

"La gamificación es una técnica de aprendizaje que traslada la mecánica de los juegos al ámbito educativo-profesional con el fin de conseguir mejores resultados: sirve para absorber conocimientos, para mejorar alguna habilidad para recompensar accio-

nes concretas… Es un término que ha adquirido una enorme popularidad en los últimos años, sobre todo en entornos digitales y educativos.”. (¿Qué es la gamificacion y cuáles son sus objetivos? (EDUCION 3.0, 2022)

Para Virginia Gaitán, el aprendizaje es divertido mediante la gamificación, porque “El modelo de juego realmente funciona porque consigue motivar a los alumnos, desarrollando un mayor compromiso de las personas, e incentivando el ánimo de superación. . .La idea de la Gamificación no es crear un juego, sino valernos de los sistemas de puntuación-recompensa-objetivo que normalmente componen a los mismos.” (Gaitán, 2022)

En concordancia con estos conceptos, la presente investigación se realiza en los siguientes ámbitos:

Geográfico: Se desarrolla en la ciudad de La Paz, específicamente en La Universidad La Salle.

Temporal: la investigación para este trabajo se lleva a cabo durante el mes de octubre de la gestión 2022.

Demográfico: Estudiantes del segundo semestre de la carrera Ingeniería de Sistemas de la Universidad La Salle.

Por otra parte, este estudio es no experimental porque no se manipulan variables y, a su vez, es exploratorio en función de que sobre el tema de la gamificación no existe aún producción literaria en nuestro país ya que su aplicación es una innovación.

A objeto de descubrir el nivel de conocimiento sobre la gamificación y su aplicación en el ámbito académico, se realizó un sondeo de opinión online a 19 estudiantes del segundo semestre de la carrera de Ingeniería de Sistemas de la Universidad La Salle, obteniendo los siguientes resultados:

8 de los 19 respondieron a la solicitud.

¿Cuál es tu género?

Tres estudiantes son de género femenino.

Cinco estudiantes son de género masculino.

¿Estás de acuerdo con las clases magistrales?

Ocho estudiantes respondieron estar de acuerdo con las clases magistrales.

Ningún estudiante está en contra.

¿Te gustaría que los docentes aplicaran juegos o concursos sobre los temas que nos enseñan?

Ocho estudiantes están de acuerdo con la idea de implementar juegos o concursos en las clases.

Nadie se mostro contrario a la idea.

¿Qué prefieres como recompensa en la participación en estos concursos?

Nadie busca premios como recompensa.

Tres personan piensan que lo mejor sería obtener puntaje adicional.

Cinco personas prefieren recibir comodines para época de exámenes.

Nadie propuso otra opción.

¿Te gustaría la implementación de videojuegos o juegos tradicionales para el aprendizaje de algunas materias?

Ningún muestra disgusto con la propuesta.

Ocho estudiantes están de acuerdo con la implementación de juegos y/o videojuegos.

¿Sabes lo que es la gamificación?

Tres estudiantes señalaron tener conocimiento sobre el concepto de gamificación.

Cinco estudiantes no saben sobre la gamificación.

Si respondiste afirmativamente, ¿te gustaría que se aplique en la carrera?

Las respuestas aquí fueron:

Si.

Seria algo interesante y divertido de hacer.

Si me gustaría.

Si.

Pese a que afirmaron no conocer la gamificación, uno de los cinco estudiantes está de acuerdo en implementarla en su educación.

Algunas aplicaciones o sitios web que se pueden usar para implementar la gamificación en la carrera de ingeniería de sistemas en la Universidad La Salle son, según (Stock, 2022):

RUBY WARRIOR: un juego con estética arcade donde deberán enfrentarse a numerosos desafíos y enemigos, con el fin de conseguir una gema custodiada por mounstros, para lograrlo se aprende los comandos de Ruby.

CODECOMBAT: Una ayuda para aprender Javascript y Python, en el cual se personifica a un mago, guía de un ejército encargado de combatir a la magia oscura, usando hechizos, que están compuestos por código o script, y completando minijuegos manejando controles para aprender sobre logaritmos.

FLAPPY BIRD: Para aprender a programar desde cero mientras se crea un videojuego en el que se tendrá que hacer que un ave esquive los obstáculos de su camino, usando Code.org para ingresar a su propia ave gratis y sin necesidad de saber programar.

CODE.ORG: Esta plataforma les ayudará a aprender a manejar la lógica de programación, moviendo objetos y personajes por la pantalla.

CODE MONKEY: Aquí serán un mono que recolecta bananas para salvar el mundo, siendo este presentado como un juego online, a través del cual se aprende a codificar y construir juegos en HTML5.

ROBOCODE: Un juego dirigido a aprender el lenguaje Java, donde el jugador personifica a un tanque el cual deberá programar para lanzar/disparar distintos ataques a otros tanques, teniendo que cambiar y renovar el código varias veces dependiendo de las cualidades del enemigo al que enfrente.

Estas son las sugerencias para acceder a algunas de las plataformas y juegos que se podrían implementar en la Universidad La Salle, específicamente en la carrera Ingeniería de Sistemas con el objetivo de introducir la gamificación o enseñanza divertida.

Por otra parte, según (Sobrino, 2022), se podría llegar a implementar una plataforma llamada Classcraft, que consiste en un juego online para docentes y estudiantes donde a medida que avanzan en sus tareas y trabajos, van ganando puntos canjeables en el juego para mejorar a su personaje, sus habilidades y comprar distintos artículos.

Conclusión

La aplicación de juegos, desafíos, concursos, en el desarrollo de la enseñanza siempre obtienen buenos resultados en función de que las personas, de cualquier edad, no sienten la presión de aprender y se enfocan en la parte divertida o desafiante de la actividad.

Las enseñanzas a través de actividades lúdicas son propias del nivel inicial y su aplicación no es ajena en los primeros años de estudio escolar. La diferencia con la gamificación es que ésta no surge de la improvisación sino más bien de ina planificación rigurosa para alcanzar objeticos y metas puntuales.

De acuerdo a las experiencias recogidas en las consultas bibliográficas. la gamificación ha demostrado ser una excelente forma de motivar a los estudiantes a aprender y mantenerse determinados en sus estudios a través de la competencia amistosa y los juegos y/o concursos que se pueden llegar a presentar durante las clases, pudiendo ser la solución para motivar su permanencia en la carrera hasta concluirla.

Actualmente, el uso de la tecnología en el campo de la comunicación, de la información y de la educación es parte de la cotidianidad, mucho más en la juventud, es por esta razón que se propone la aplicación de la gamificación en la carrera de Ingeniería de Sistemas como un método de aprendizaje más ameno e interesante, motivando en los estudiantes el desafío de aprender dentro del uso de sus habilidades en diferentes videojuegos.

Aprender de manera divertida, sin presiones y más bien haciendo algo que es de su agrado, llegando los estudiantes a aprender distintos temas, creando actividades

y recuerdos que quedarán en la memoria de los estudiantes por el resto de sus vidas, enseñanzas que no sean solo de recuerdo para el examen, sino que sean enseñanzas que vengan acompañadas de buenos recuerdos y diversión, que recordaran por siempre al ser algo que les trajo satisfacción.

Referencias

3.0, Educacion. (22 de 10 de 2022). ¿Qué es la gamificacion y cuáles son sus objetivos? | EDUCION 3.0. Obtenido de Educacion 3.0: https://www.educacion-trespuntocero.com/noticias/gamificacion-que-es-objetivos/

ATURA - Experiencia, Tecnología e Innovación. (23 de 10 de 2022). 10 Juegos para aprender a programas si eres principiante. Obtenido de ATURA - Experiencia, Tecnología e Innovación: https://www.atura.mx/blog/10-juegos-para-aprender-a-programar-si-eres-principiante#:~:text=10%20Juegos%20para%20aprender%20a%20programar%20si%20eres,Murder%20Mystery%20...%208%20Untrusted%20...%20M%C3%A1s%20elementos

BI WORLDWIDE. (22 de 10 de 2022). ¿Qué es la Gamificación? Obtenido de BI WORLDWIDE | Inspirando personas. Entregando resultados.: https://www.biworldwide.com/es-CO/gamificacion/

Bolivia, U. (22 de 10 de 2022). UNICEF y AGETIC lanzan segundo curso de robótica con becas para 850 adolescentes mujeres. Obtenido de Educación | UNICEF Bolivia: https://www.unicef.org/bolivia/comunicados-prensa/unicef-y-agetic-lanzan-segundo-curso-de-rob%C3%B3tica-con-becas-para-850-adolescentes

Carrasco, M. I. (22 de 10 de 2022). - Historia de la Gamificación - | Sutori. Obtenido de Presentaciones para el aula | Sutori: https://www.sutori.com/es/historia/historia-de-la-gamificacion--2AVjzp4CcnGSgXPuoB-1VcEGc

CETYS. (22 de 10 de 2022). Importancia de la educación: el camino para una mejor sociedad- CETYS Trends. Obtenido de Principal - CETYS Trends: https://www.cetys.mx/trends/educacion/importancia-de-la-educacion-el-camino-para-una-mejor-sociedad/#:~:text=A%20nivel%20global%2C%20la%20educaci%C3%B3n,de%20empleabilidad%20en%20el%20pa%C3%ADs

Classcraft - Relationships are everything. (23 de 10 de 2022). Classcraft - Relationships are everything. Obtenido de Classcraft - Relationships are everything: https://www.classcraft.com/

Delgado, A. M. (22 de 10 de 2022). Cómo aplicar la gamificación en e-learning - Educativa España. Obtenido de Ecosistemas de soluciones e-learning | Educativa España: https://www.educativa.es/gamificacion-en-elearning/

Ebot. (22 de 10 de 2022). 10 beneficios de introducir la gamificación en el aula. Obtenido de Cursos de Robótica Educativa y Tecnología para niños Madrid | Ebot: https://ebot.es/beneficios-gamificacion-aula/

EQUIPO DE INVESTIGACIÓN SECTORIAL, INDICADORES Y AÁLISIS EDUCATIVO. (22 de 10 de 2022). ESTADÍSTICAS. Obtenido de https://seie.minedu.gob.bo/reportes/estadisticas: https://seie.minedu.gob.bo/reportes/estadisticas/grupo1/matricula

Fundación Aquae. (22 de 10 de 2022). ¿Qué es la gamificación? Definición y objetivos - Fundación Aquae. Obtenido de Fundación Aquae - La Fundación del Agua: https://www.fundacionaquae.org/wiki/que-es-gamificacion/

Gaitán, V. (22 de 10 de 2022). Gamificacion: el aprendizaje divertido | educativa. Obtenido de educativa: Líderes de Iberoamérica en sistemas para formación: https://www.educativa.com/blog-articulos/gamificacion-el-aprendizaje-divertido/

García, L. E. (22 de 10 de 2022). Historia de los Videojuegos. Obtenido de Monografias.com - Tesis, Documentos, Publicaciones y Recursos Educativos.: https://www.monografias.com/trabajos90/historia-videojuegos/historia-videojuegos

Golan, P. (22 de 10 de 2022). ¿Qué es la gamificación? Objetivos educativos + ejemplos (2022). Obtenido de La Mejor Plataforma de ecommerce para Latinoamérica: https://www.shopify.com/es/blog/que-es-gamificacion

IFEMA MADRID. (22 de 10 de 2022). qué es la gamificación y cuáles son sus bjetivos | IFEMA MADRID. Obtenido de IFEMA MADRID: Eventos, Ferias y Congresos | IFEMA MADRID: https://www.ifema.es/noticias/educacion/que-es-la-gamificacion

Ignite Online. (23 de 10 de 2022). What is gamification? And tools to pu it into practice in the classroom | Ignite Online. Obtenido de Ignite-Online | provokes | Connect | transform: https://igniteonline.la/3653/

Instituto Nacional de Estadística. (23 de 10 de 2022). %8,2% de profesionales de la enseñanza es mujer - INE. Obtenido de Instituto Nacional de Estadística - INE: https://www.ine.gob.bo/index.php/582-de-profesionales-de-la-ensenanza-es-mujer/

Malvido, A. (22 de 10 de 2022). La gamificación como estrategía educativa: Tendencias 2019. Obtenido de Cursos gratuitos para trabajadores y desempleados: https://www.cursosfemxa.es/blog/gamificacion-estrategia-educativa

Observatorio De Género coordinadora de la mujer. (22 de 10 de 2022). Observatorio. Obtenido de Observatotio: http://www.coordinadoradelamujer.org.bo/observatorio/index.php

Pañella, O. G. (22 de 10 de 2022). Gamification: qué es la Gamificación y cómo funciona. Obtenido de IEBS - La Escuela de la Innovación y los Emprendedores: https://www.iebschool.com/blog/gamification-innovacion/

Peredo, N. (22 de 10 de 2022). Identifican cinco problemas para la educación en tiempos de pandemia | Los Tiempos. Obtenido de Noticias de Bolivia y del mundo | Los Tiempos: https://www.lostiempos.com/actualidad/pais/20200522/identifican-cinco-problemas-educacion-tiempos-pandemia

Peredo, N. (22 de 10 de 2022). Identifican cinco problemas para la educación en tiempos de pandemia | Los Tiempos. Obtenido de Noticias de Bolivia y del mundo | Los Tiempos: https://www.lostiempos.com/actualidad/pais/20200522/identifican-cinco-problemas-educacion-tiempos-pandemia

Retro Informatica El pasado del futuro. (22 de 10 de 2022). Historia de los videojuegos. Obtenido de Retroinformática. El pasado del futuro: https://www.fib.upc.edu/retro-informatica/historia/videojocs.html

Santander Universidades. (22 de 10 de 2022). ¿Qué es la gamificación en el aula? | Blog Becas Santander. Ob-

tenido de Becas Santander: https://www.becas-santander.com/en/index.html

Sobrino, S. (26 de 10 de 2022). Gamificacion en la educacion. (M. Caballero, Entrevistador)

Stock, A. N.-T. (23 de 10 de 2022). 10 juegos para aprender a programar de forma divertida | Tecnología - ComputerHoy.com. Obtenido de ComputerHoy.com: Todo sobre tecnología, gadgets y novedades: https://computerhoy.com/noticias/tecnologia/10-juegos-aprender-programar-forma-divertida-465909

UNICEF bolivia. (22 de 10 de 2022). Educación | UNICEF Bolivia. Obtenido de UNICEF Bolivia | UNICEF Bolivia: https://www.unicef.org/bolivia/educaci%C3%B3n

UNIR. (22 de 10 de 2022). Gamificación en el aula: ventajas y cómo aplicarla | UNIR. Obtenido de UNIR - La Universidad A Distancia 100% Online: https://www.unir.net/educacion/revista/gamificacion-en-el-aula/

UNIR La Universidad en el Internet. (23 de 10 de 2022). Ejemplos de gamificación en Primaria ¡Ponlo en práctica! Obtenido de UNIR - La Universidad A DIstancia 100% Online: https://www.unir.net/educacion/revista/ejemplos-gamificacion-primaria/#:~:text=De%20esa%20manera%2C%20hay%20diversas%20herramientas%20para%20la,similar%20a%20una%20red%20social.%20...%20M%C3%A1s%20elementos

Artículo Recibido: 14/03/2023

Artículo Aceptado: 12/05/2023

DISEÑO DE UN MODELO DE CONTROL PID PARA UN SISTEMA BALL AND BEAM

PID CONTROL MODEL IMPLEMENTATION FOR A BALL AND BEAM SYSTEM)

Autores:

Univ. Arguedas Meneses Jahstin menesesjahstin@gmail.com

Univ. Paz Rodríguez José Pablo joseppaz2014@gmail.com

Univ. Baldiviezo Laura Adrián adrianbaldiviezo10@gmail.com

Univ. Vargas Azero Marcos mvadvrock@gmail .com

Ing. Kevin Marlon Soza Mamani

Docente de la Universidad La Salle, Carrera de Ingeniería de Sistemas.

kmsoza@doc.ulasalle.edu.bo

Resumen

Este proyecto proporciona la construcción de un sistema de Ball and Beam. Además de los modelos básicos P, PI o PID para verificar. La interfaz de usuario desarrollada en MatLab permite a los usuarios Interactuar con el sistema y realizar la sintonización del controlador. Se presenta un modelo matemático

de un Ball and Beam convencional, la construcción de un prototipo, el acondicionamiento de las señales de entrada, el diseño del controlador y la validación del mismo. El sistema “Ball and Beam” es popular, fácil de entender e implementar. El modelo se basa en el movimiento controlado de la esfera. Hoy en no es usual encontrar sistemas de control con costos bajos. Por lo cual se va a diseñar y construir un módulo de entrenamiento. Este proyecto es el menos costoso y casi tan preciso comparado con otros trabajos similares.

Palabras clave Ball and Beam, Control PID, MatLab, Servomotor, Sensor de ultrasonido, TUNE.

Abstract

This project presents the construction of a Ball and Beam system, to validate basic control strategies such P, PI or PID, also a user interface developed in MatLab where the user can interact with the system and perform tuning of the controller. A mathematical model of a conventional Ball and Beam, the construction of a prototype, the conditioning of the input signals, the design of the controller and its validation are presented. The “Ball and Beam” system is common, easy to understand. The model is based on the controlled movement of the sphere. Today it is not usual to find control systems with low costs. Therefore, a training module will be designed and built. This project is the least expensive and almost as precise compared to other similar jobs.

Keywords Ball and Beam, PID Control, MatLab, Servomotor, Ultrasonic Sensor, TUNE.

Introducción

Sistema de "Ball and Beam". Su dinámica es simple, pero tan buena que controlan conceptos modernos (Dorf et al., 2005; Ogata, 2003). Es el movimiento casi real encontrado en sistemas aeroespaciales (Díaz, 2020).

El sistema de "Ball and Beam" no es un modelo real. En la forma que otros equipos demostrativos de laboratorio lo son, su dinámica contradice hallazgos similares en muchos sistemas de control moderno, como tal, es una importante herramienta para estudiantes y desarrolladores (Obando Correa & Romero Brand, 2010).

Partimos de la necesidad de implementar un sistema demostrativo de control (Lizarazo et al., 2014), la investigación comenzó con varios prototipos (SANTOS & others, 2018). La conclusión de la construcción es un sistema de lazo cerrado llamado "Ball and Beam".

El sistema de "Ball and Beam" es muy importante y un modelo clásico de ingeniería de control. Es muy popular,

simple y fácil de entender, se pueden utilizar en muchos estudios(Jover Ibáñez, 2019). Un estudio de los métodos de planificación clásicos y modernos en ingeniería.

El sistema se muestra en la figura 1. El sistema de control consta del movimiento de la esfera cambiando el ángulo de la palanca para que se adapte a la distancia deseada. El control del movimiento se realiza mediante servomotores.

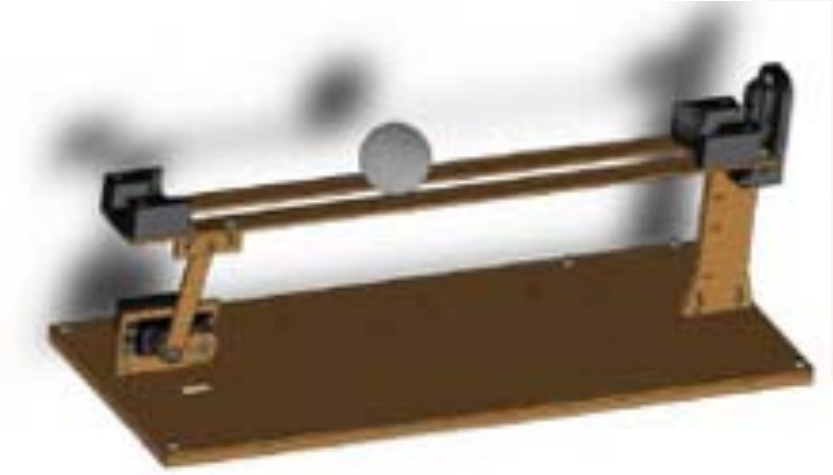


Figura 1. Sistema "Ball and Beam" (Elaboración propia).

Actualmente la ingeniería de control posee pocos sistemas físicos que permitan la retroalimentación visual para que de esta forma el espectador evidencie la correcta implementación del lazo de control cerrado, debido a por su complejidad, hoy en día, los equipos de monitoreo visuales son muy costosos.

Así mismo, éste se considera un trabajo con fines académicos e investigativos. Los estudios del modelo se realizaron en los ambientes controlados del laboratorio 3 de la Universidad La Salle Bolivia.

Objetivo General

Diseñar y construir un módulo de entrenamiento, para implementar modelos de control mediante MatLab.

Objetivos Específicos

- Diseñar y modelar un sistema de control "Ball and Beam".
- Desarrollar una función de transferencia en Matlab para manipular el sistema.
- Sintonizar la función de transferencia mediante la herramienta TUNE de Matlab.
- Implementar el modelo de Ziegler and Nichols de punto crítico para cada constante del PID.

Métodos y Materiales

En base a los datos obtenidos del comportamiento del ángulo del motor se realiza un estudio de simulación en el IDE de MatLab, utilizando la herramienta Simulink, se implementa una función de transferencia G(s) discretizada para poder encontrar las constantes del PID utilizando la herramienta TUNE de MatLab, previamente para conseguir constantes auxiliares y de prueba se utilizó el método de punto crítico de Ziegler y Nichols.

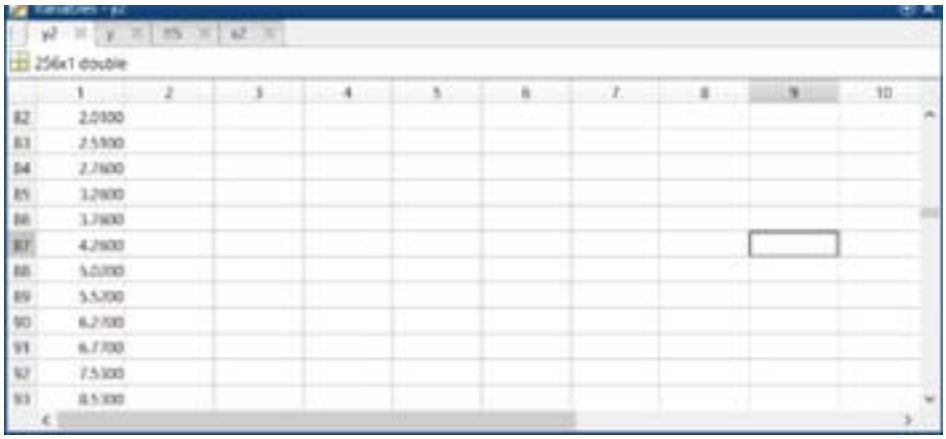


Figura 2. Datos de salida del servomotor (Elaboración propia).

Utilizando los datos generados en base al comportamiento del Servomotor, se generan dos bases de datos para el sistema de lazo cerrado consiguiendo los datos de entrada y salida, para ser importados en el Matlab como matrices numéricas, además de filtrar los datos para reducir picos de inestabilidad utilizando un comando de filtrado de datos (filter) perteneciente a Matlab. Estos procesos se muestran en las Figuras 2 y 3. Posteriormente en la ventana "Ident" verificamos con una gráfica que los datos estén correctamente manejados, una vez esto se verifica pasamos a hallar la función de transferencia discreta que tenga un mejor rendimiento, tal como lo muestra la Figura 4.

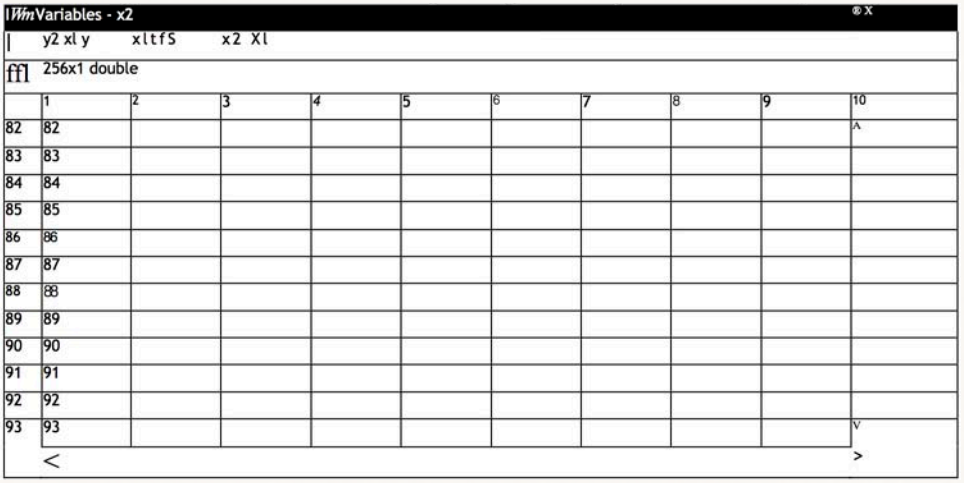


Figura 3. Datos de entrada del servomotor (Elaboración propia).

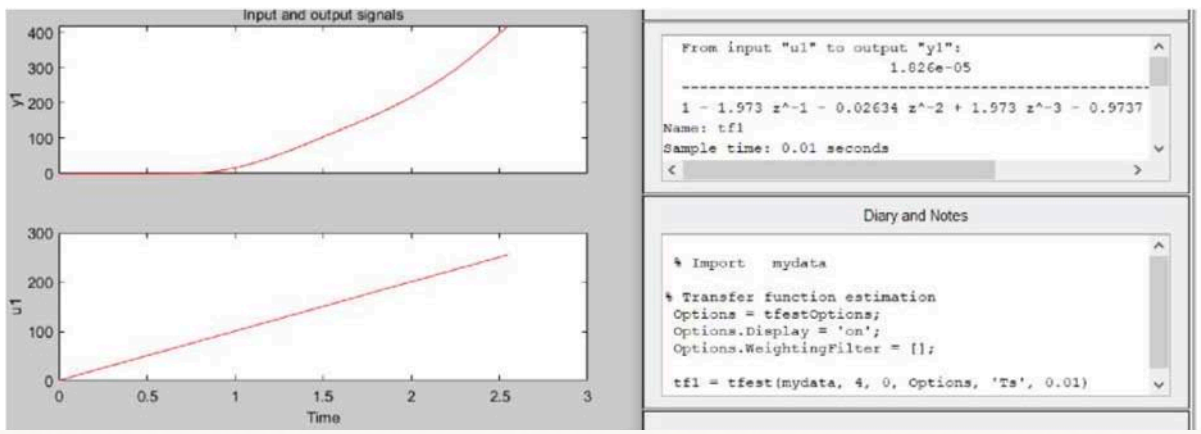


Figura 4. Gráfica de verificación y función de transferencia generada (Elaboración propia).

Como bien se explicó anteriormente se realiza una simulación en Matlab implementando PID y el modelo de ganancia crítica de "Ziegler and Nichols" como se observa en la fig. 7, donde se trata de estabilizar las curvas de la fig. 7 a un mismo punto máximo para obtener los valores de Kcr y Per.

De esta manera podemos obtener datos kp, ki y kd mediante la tabla que nos brinda el modelo de Ziegler y Nichols en la tabla 1 y que genera los resultados en la tabla 2, coeficientes que nos facilitarán la función final del controlador PID como sigue:

$$e(t) = r(t) - y(t)$$

$$u(t) = Kp\, e(t) + Ki \int_0^t e(t)dt + Kd \frac{de(t)}{dt}$$

(2) Y aplicando la transformada de La Place obtenemos un expresión mucho más simplificada y entendible:

$$Función\ de\ transferencia \rightarrow \frac{salida \rightarrow u(s)}{entrada \rightarrow E(s)} = \frac{Kds^2 + Kps + Ki}{s} = G(s)$$

(3)

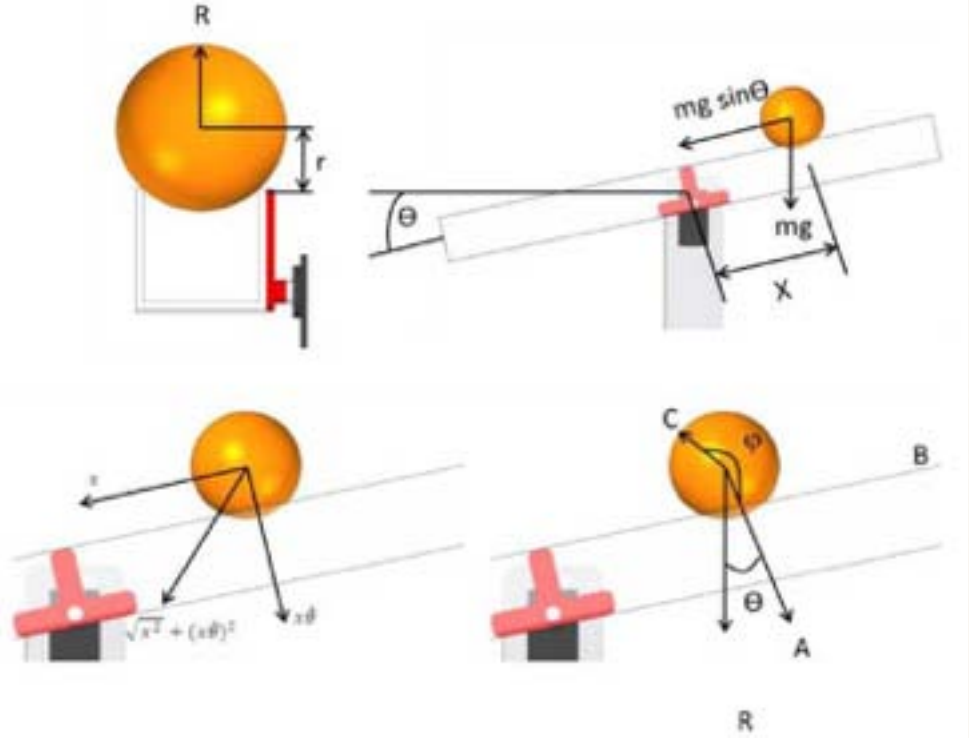
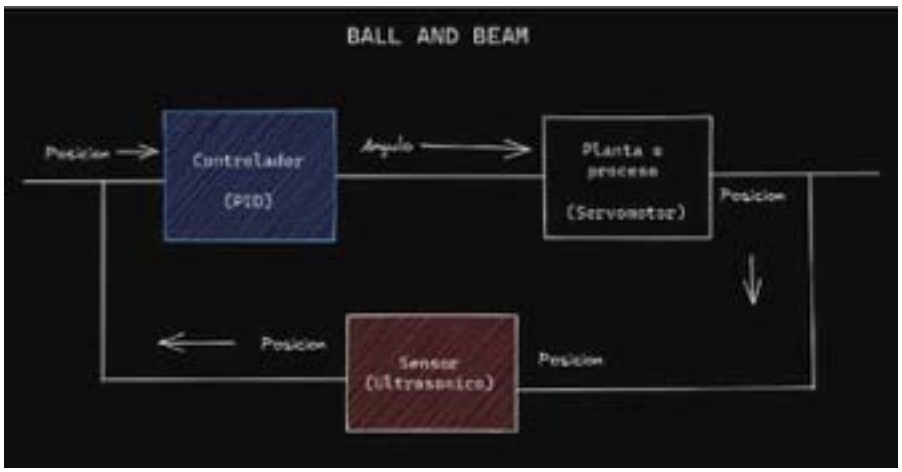


Figura 5. Modelo real "Ball and Beam" (Obando Correa et al., 2013).

El modelo real sin embargo es el que se muestra en la Figura 5. En base a este modelo podemos obtener la inercia general de la esfera. Se linealiza la función para conseguir los parámetros de entrada y salida que son la distancia y el ángulo respectivamente. De esta forma la función de transferencia que se representa de la siguiente manera:

salida ^ x(s) 5gR entrada ^ 9(s) 7Ls2 ^(')

Donde g se define como la gravedad, r es el radio de la esfera y L se considera la longitud de la barra secundaria conectada al motor y a la varilla principal.



En base al análisis del modelo real se diseña un diagrama que contempla los diseños de planta y cómo se manejan los datos de entrada y salida como se muestra en la figura 6.

Figura 6.

Diagrama del modelo "Ball and Beam" (Elaboración Propia).

Por otra parte, en la Figura 7, se puede observar el método experimental para la obtención de la ganancia crítica. En dicho método se estimula la planta hasta conseguir un comportamiento oscilatorio sostenido, tal y como se muestra también en la Figura 8.

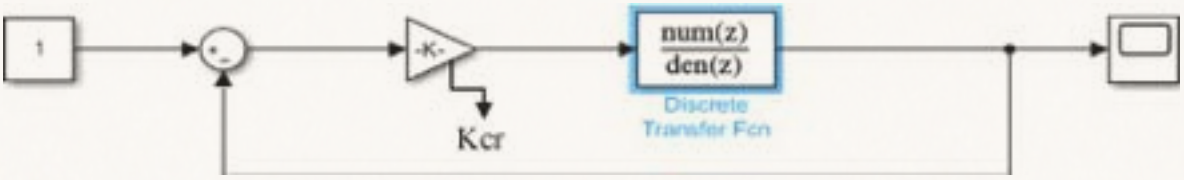


Figura 7. Modelo "Ziggler and Nichols" con ganancia crítica en Matlab (Elaboración propia).

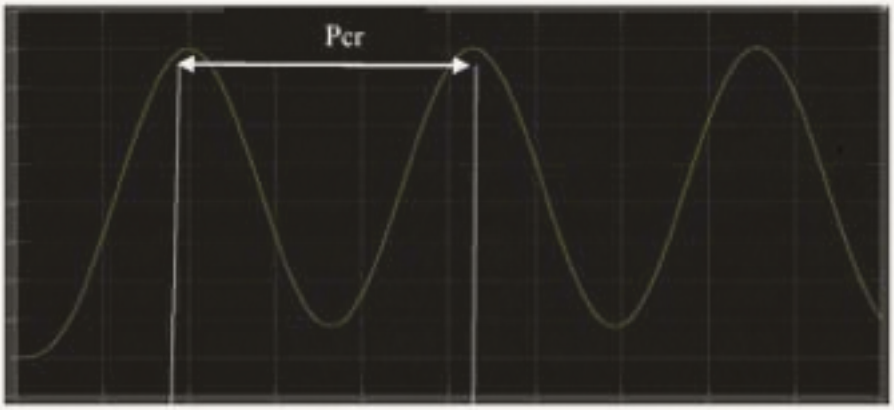


Figura 8. Curvas del gráfico generadas por el modelo "Ziegler and Nichols" (Elaboración propia).

Una vez obtenidos los parámetros del modelo de sintonización de Ziegler y Nichols, se procede a obtener el valor de las ganancias PID para cada caso. La Tabla 1 muestra el método de adquisición de las constantes, mientras la Tabla 2 muestra las ganancias obtenidas del modelo desarrollado (Ball and Beam).

Tipo de controlador	Kp	Ti	Td
P	0,5Kcr	OT	0
PI	0,45Kcr	0,83Pcr	0
PID	0,6Kcr	0,5Pcr	0,125Pcr

Tabla 1. Tabla del método de ganancia crítica.

Tipo de controlador	Kp	Ti	Ki	Td	Kd
P	0,465	OT	OT	0	0
PI	0,4185	2,6975	0,1724	0	0
PID	0,558	1,625	0,2862	0,40625	0,1889

Tabla 2. Tabla de coeficientes resultantes para la sintonización.

Con la función de transferencia discretizada podemos armar el modelo en Matlab y realizar la respectiva simulación y sintonizar lo mejor posible mediante los datos de la tabla 2 como se muestra en la figura y el TUNE en la figura 9 para controlar que se llegue a un punto deseado.

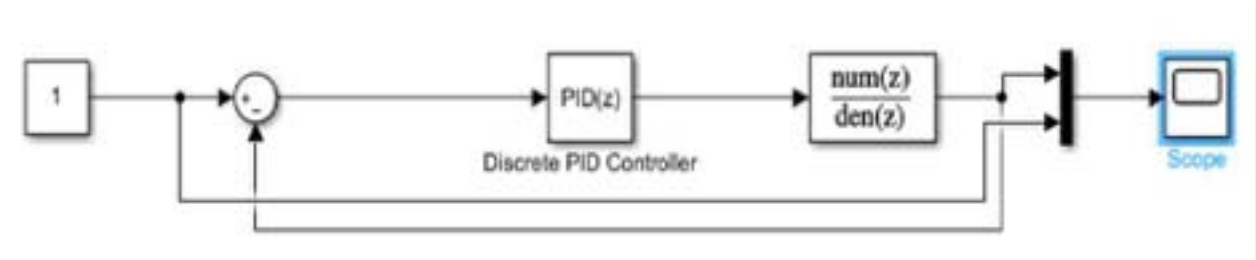


Figura 9. Modelo final para la simulación (Elaboración propia).

Así mismo, una sintonización por medio de la herramienta PID Tunning, perteneciente a Simulink, es realizada a la planta. El modelo encontrado de dicha sintonización puede observarse en la Figura 10.

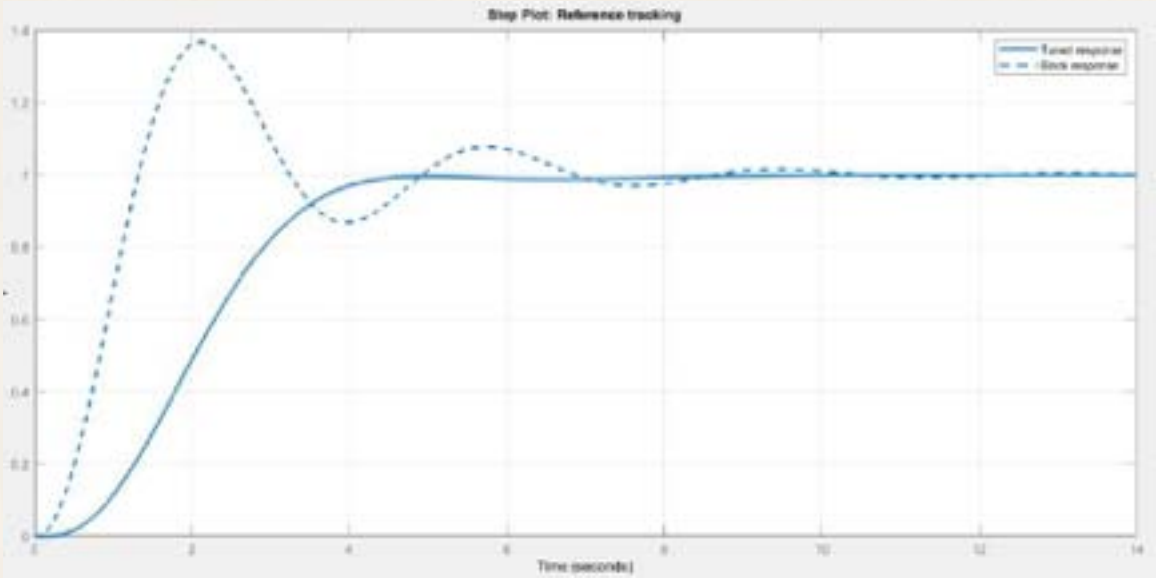


Figura 10. Sintonización mediante TUNE (Elaboración propia).

Resultados

Una vez compilada la simulación, con ambas sintonizaciones realizadas podemos observar que en las figuras 11 y 12 se logra obtener resultados óptimos en cuanto al parámetro deseado que en este caso es 1.

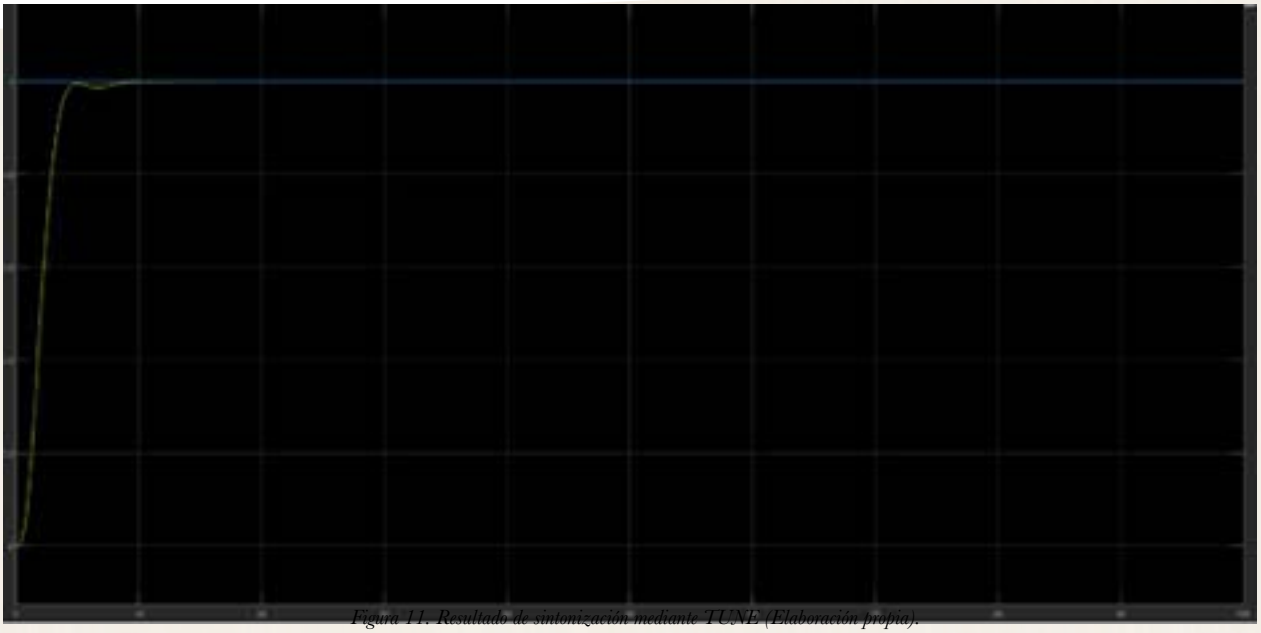


Figura 11. Resultado de sintonización mediante TUNE (Elaboración propia).

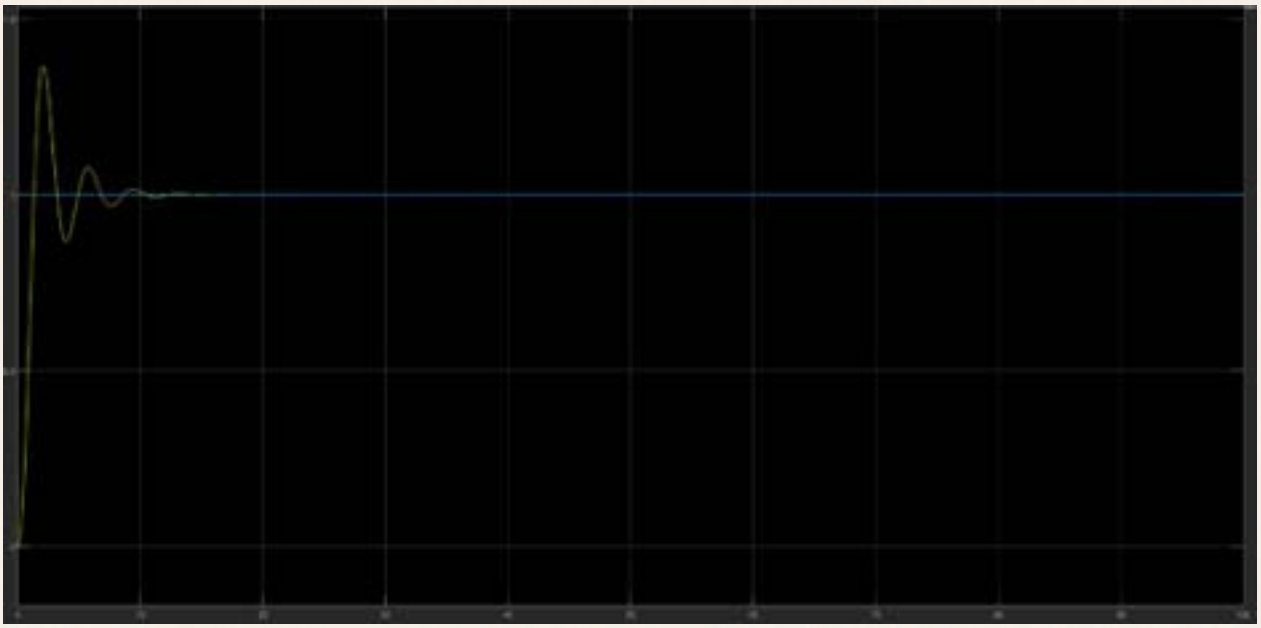


Figura 12. Resultado de sintonización mediante datos de la tabla 2. (Elaboración propia)

Discusión

Un modelo matemático que reproduce fielmente el comportamiento hace que sea más fácil administrar el tiempo y precisión de su controlabilidad. De manera que sea simple, confiable y el sistema se mantenga estable. Un modelo matemático de un sistema dinámico se puede definir como: un conjunto de ecuaciones (generalmente diferenciales) que representan todo el movimiento del sistema en cuestión. Este ejemplo, matemáticamente no es único, sino que depende del sistema en cuestión. Un modelo puede ser más apropiado en algunos casos que en otros.

Así, por ejemplo, en el problema de control óptimo, es provechoso usar representaciones en el espacio de estados. En cambio, para los análisis de la respuesta transitoria o en frecuencia de sistemas lineales con una entrada y una salida invariantes con el tiempo, la representación mediante función de transferencia puede ser más conveniente que cualquier otra. En la obtención de un modelo matemático se debe establecer un equilibrio entre la simplicidad del mismo y la precisión de los resultados del análisis.

Para observar mejor estas diferencias se realiza una comparación con dos trabajos relacionados al proyecto en cuestión. El mismo será enfocado en los materiales utilizados, la implementación del modelo PID y la precisión del sistema.

Parámetros de comparación	**Implementación de un Modelo de Control PID para un Sistema Ball and Beam (Proyecto Actual)**	**Desarrollo de un sistema ball and beam, para implementar estrategias de control mediante Labview (Oscar y Hector)**	**Diseño, implementación y control de un prototipo de Ball & Beam (Guillermo)**
Materiales	Se utilizó en lo posible materiales delgados y de poco peso como madera(venesta) para no tener en cuenta realizar ajustes en el modelo. Y para la posición se usa un sensor ultrasónico y un servomotor para reducir costos.	Se utilizan materiales metálicos para realizar el modelo físico, pero sin embargo se deben realizar ajustes adicionales para tener más control del peso y sin embargo es más costoso debido a que se necesitan piezas específicas y soldaduras.	Se realizan con materiales metálicos y un potenciómetro como sensor analógico de posición, además de otros componentes más especializados con costos altos.
Implementación del modelo PID	La implementación es simple debido a que se codifica en el IDE de Arduino e implementamos PID mediante iteraciones y visualización de los datos de forma directa mediante el puerto serial y la graficadora.	La implementación PID es más compleja debido a que se utiliza un a tarjeta de adquisición de datos (TAD) para la manipulación de los datos, lo que afecta en la complejidad de realizar el proyecto.	Se habla acerca de otros modelos como PID para realizar el proyecto sin embargo, se utiliza un a representación del espacio de estados mediante el método de Newton.
Precisión		La precisión es aceptable en los primeros 5 segundos, pero se recomienda mejorar el sistema de lectura de posición disminuyendo el ruido sin importar el tipo de esfera.	La existencia de la "Zona muerta" causada por la estructura del propio motor provocan la aparición de un error bastante notable respecto a la simulación, pero sin embargo la precisión es muy alta.

Tabla 3. Tabla de comparación y discusión del proyecto.

Conclusiones

Se diseñó un sistema de control "Ball and Beam" en base a un modelo matemático de referencia que toma en cuenta las dimensiones y las velocidades de un sistema real. A partir de los datos obtenidos del sistema real se logró estimar el sistema dinámico de la planta por medio de una función de transferencia de tercer grado y con una aproximación al sistema original cercana al 93 %.

Se realizó una sintonización del sistema por medio del método de Ziegler y Nichols para compararla posteriormente con una sintonización automática por medio de "PID Tunning" de Matlab. Por supuesto, la sintonización por medio de la herramienta de Simulink mostró un mejor desempeño, sin embargo, las ganancias obtenidas son desproporcionadas a comparación de las calculadas por medio del método de Ziegler y Nichols.

Se concluye que la implementación del sistema puede ser mejor beneficiada por las ganancias obtenidas por el método clásico, puesto que sus valores son menos desproporcionados y parecen reflejar de forma más adecuada la respuesta real del sistema.

Referencias

Díaz, A. D. (2020). Diseño, implementación y control de un sistema «ball and beam» [Universidad de Sevilla. Departamento de Ingeniería de Sistemas y Automática]. https://idus.us.es/bitstream/handle/11441/108958/TGF-2871- DELGADO0/o20DIAZ.pdf?sequence=1&isAllowed=y

Dorf, R. C., Bishop, R. H., Canto, S. D., Canto, R. D., & Dormido, S. (2005). Sistemas de control moderno. Pearson Educación.

Jover Ibáñez, G. (2019). Diseño, implementación y control de un prototipo de Ball & Beam.

Lizarazo, D. L. M., Borja, J. A. T., & others. (2014). Ball & beam control system using matlab and lego nxt. Visión electrónica, 8(2), 39-48.

Obando Correa, O. A., & Romero Brand, H. (2010). Desarrollo de un sistema ball and beam, para implementar estrategias de control mediante Labview [UNIVERSIDAD PONTIFICIA BOLIVARIANA].

https://repository.upb.edu.co/bitstream/handle/20.500.11912/1008/digital_19848.pdf Ogata, K. (2003). Ingeniería de control moderna. Pearson Educación.

SANTOS, S. O. & others. (2018). Sintonización de un controlador PID basado en un algoritmo heurístico para el control de un Ball and Beam.

Artículo Recibido: 14/03/2023

Artículo Aceptado: 12/05/2023

CONTROLES DE SEGURIDAD DE LA INFORMACIÓN BASADOS EN RIESGOS GENERADOS POR LOS USUARIOS FINALES

Autora:

Lic. Lourdes Tarqui Lucana

Lulim6@hotmail.com

RESUMEN

En la actualidad la información ha cobrado bastante importancia en las empresas y el sector más vulnerable son los usuarios finales que están expuesto a la ingeniería social, mal uso de la tecnología e incumplimiento a las políticas y controles de seguridad de la información propuesta por la empresa, en este sentido la empresa propone controles basados en la ISO 27001 y 27002 , los cuales serán analizados por los usuarios y así obtener los más adecuados y útiles para la empresa y establecer medidas de seguridad de la información.

En primera instancia se plantea algunos riesgos a los cuales está expuesto al usuario como la ingeniería social, mal uso de la tecnología e incumplimiento a las políticas y controles de seguridad de la información propuesta por la empresa.

Luego se realiza el análisis de los controles adecuados para los riesgos de parte de la empresa, Posteriormente los usuarios analizaran los controles más acordes y que cumplan los objetivos de la empresa.

Finalmente se consideran las medidas a tomar para reducir los riesgos a los cuales son expuestos los usuarios.

Palabras Clave

Seguridad, Información, Riesgo, vulnerabilidad, usuario, medidas.

ABSTRACT

At present, information has become quite important in companies and the most vulnerable sector are end users who are exposed to social engineering, misuse of technology and non-compliance with the information security policies and controls proposed by the company. In this sense, the company proposes controls based on ISO 27001 and 27002, which will be analyzed by users and thus obtain the most appropriate and useful for the company and establish information security measures.

In the first instance, some risks are raised to which the user is exposed, such as social engineering, misuse of technology and non-compliance with the information security policies and controls proposed by the company.

Then the analysis of the appropriate controls for the risks on the part of the company is carried out. Subsequently, the users will analyze the most appropriate controls and that meet the objectives of the company.

Finally, the measures to be taken to reduce the risks to which users are exposed are considered.

INTRODUCCIÓN

Las empresas independientemente al rubro que se dediquen están compuestas por personas, políticas y procedimientos y tecnología; estos componentes interactúan entre sí con la información que actualmente es considerada como activo intangible de las empresas por el valor administrativo, operacional, documental e histórico.

La Seguridad de la información busca aplicar controles para proteger la información y que esté disponible, sea integra y tenga confidencialidad.

Los usuarios finales son el sector más vulnerable a los riesgos como ingeniería social, mal uso de la tecnología o se encuentran con políticas y procedimientos que no están acorde con la empresa.

Es por eso que es importante considerar el análisis de controles y medidas para no descuidar la seguridad de la información.

CONTENIDO

Considerando que para la seguridad de la información los riesgos relacionados a las TI son un punto inicial fundamental se identifica los siguientes riesgos que pueden considerarse los que se presentan con mucha frecuencia en usuarios finales.

RIESGOS PROPENSOS DE LOS USUARIOS FINALES

Clasificación de riesgos generados por usuarios:

A. INGENIERIA SOCIAL EN LA SEGURIDAD DE LA INFORMACIÓN

Los usuarios por una parte son vulnerables la ingeniería social donde los hackers despliegan técnicas en línea para obtener acceso a información confidencial aprovechándose del desconocimiento o falta de capacitación del personal de la empresa y por desgracia, hay muchos sesgos cognitivos que los atacantes pueden explotar en su beneficio, robando los datos privados de la empresa. Las técnicas de ingeniería social explotan esta tendencia a la confianza de muchas maneras diferentes como

el phising, baiting, malware, honey trap y spam en el correo electrónico.

B. MAL USO DE LOS EQUIPOS TECNOLOGICOS

Los daños físicos que pueden sufrir los equipos de computación pueden ser causados por fenómenos naturales como ser inundaciones, tormentas, terremotos, etc y riesgos humanos como actos involuntarios que pueden ocasionar fallas de manera parcial o total a los equipos asignados llegando a afectar a la organización en sus funciones cotidianas.

C. INCUMPLIMIENTO A LAS POLITICAS Y CONTROLES DE SEGURIDAD DE LA INFORMACION PROPUESTA POR LA EMPRESA

El incumplimiento de parte de los usuarios ante las políticas y controles podría por las siguientes razones:

-Las políticas y procedimientos no son acorde a la empresa.

-La documentación es ampulosa y desactualizada.

-No se cuenta con capacitaciones regulares de las políticas y procedimientos.

-No se cuenta con recursos económicos para tener personal designado.

El incumplimiento de las mismas puede llevar a la empresa desde una llamada de atención hasta multas, sanciones legales, pérdidas económicas, pérdida de oportunidades de negocio y afectar la reputación y credibilidad de la empresa convirtiéndose en un obstáculo en sus actividades y planes de crecimiento económico.

CONTROLES DE LOS RIESGOS

Muchas veces los usuarios caen en riesgos debido a que los controles no son realistas o no responden a los objetivos de la empresa por lo tanto al momento de implementar se debe realizar un análisis periódico donde se pueda verificar si los controles son adecuados, útiles y aplicables a la empresa.

Análisis de los controles por parte de los usuarios

En este sentido los usuarios finales son los que realizar el análisis de los controles de aplicabilidad o descartarte así como también la modificación o mejora.

Con esto se pretende obtener los controles más adecuados y útiles a la empresa; se llenara un fichero previa explicación del marco teórico en los cuales los usuarios deberán ver la viabilidad del control dentro de la empresa para su posterior análisis por el área de seguridad de la información.

Tabla 1 Elaboración propia

Control: de acuerdo al análisis de controles.

Aplicable: El usuario considera si es o no aplicable o no tiene una buena base para considerar si es aplicable o no.

Motivo: En este campo el usuario deberá detallar los motivos que considera de acuerdo al campo de aplicabilidad.

Consideración: El usuario podrá sugerir alguna modificación o adición que considere de acuerdo al control.

Después de realizar el análisis los controles que se consideran son:

Riesgo: Ingeniería social

Los controles que a continuación están son los que los usuarios finales determinaron viables para tratar la ingeniería social son:

A.6.2.1 Políticas de dispositivos móviles

Control Se debe adoptar una política y medidas de apoyo a la seguridad para gestionar los riesgos presentados al usar dispositivos móviles.

A.7.2.2 Concientización, educación y formación en seguridad de la información.

Control Todos los empleados de la organización, y en donde sea pertinente, los contratistas deben recibir formación adecuada en concientización y actualizaciones regulares en políticas y procedimientos organizaciones, pertinentes para su función laboral.

A.12.1.1 Procedimientos de operaciones documentados

Control Los procedimientos de operaciones se deben documentar y poner a disposición de todos los usuarios que los necesiten.

A.12.2.1 Controles contra código malicioso.

Control Se deben implementar controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto con los procedimientos adecuados para concientizar a los usuarios.

Riesgo: Mal uso de los equipos tecnológicos.

Los controles que se tienen a continuación son para el riesgo del más uso de los equipos tecnológicos:

A.11.1.3 Seguridad de oficinas, salas e instalaciones

Control se debe diseñar y aplicar la seguridad física en oficinas, salas e instalaciones.

A.11.2.6 Seguridad del equipamiento y los activos fuera de las instalaciones

Control Se deben asegurar todos los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar de las instalaciones de la organización.

A.11.2.8 Equipo de usuario desatendido

Control los usuarios se deben asegurar de que a los equipos desatendidos se les da protección apropiada.

A.11.2.9 Política de escritorio y pantalla limpios

Control Se debe adoptar una política de escritorio limpio para papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procedimientos de información.

Riesgo: Incumplimiento a las políticas y controles de seguridad de la información

A.5.1.1. Políticas para la seguridad de la información

Control La dirección debe definir, aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes un grado de políticas para la seguridad de la información.

A.5.1.2 Revisión de las políticas de seguridad de la información

Control Se deben revisar las políticas de seguridad de la información a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia y eficacia continuas.

A.18.1.1 Identificación de la legislación vigente y los requisitos contractuales

Control Todos los requisitos estatutarios, regulatorios-contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben definir y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.

A.18.2.1 Revisión independiente de la seguridad de la información

Control El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se debe revisar en forma independiente, a intervalos planificados, o cuando ocurran cambios significativos.

Los controles obtenidos de acuerdo a al análisis de los usuarios ante el riesgo de incumplimiento a las políticas y controles de seguridad de la información son:

A.18.2.2 Cumplimiento con las políticas y normas de seguridad

Control Los gerentes deben revisar con regularidad el cumplimiento del procesamiento y los procedimientos de seguridad que están dentro de su área de responsabilidad de acuerdo con las políticas de seguridad, normas y otros requisitos de seguridad pertinentes.

A.18.2.3 Verificación del cumplimiento técnico

Control Se deben verificar regularmente los sistemas de información en cuanto a su cumplimiento con las policías y normas de seguridad de la información de la organización.

MEDIDAS Y RECOMENDACIONES

Una vez que contemos con los ficheros se procederá al análisis y tomar las siguientes medidas:

Deberá redactarse un documento de seguridad con los controles que serán aplicados por la empresa.

Un programa efectivo de educación de manera periódica

La capacitación podrá ser en grupo y de manera específica, personalizada y enfocada en función a los riesgos a los cuales son propensos los usuarios finales, según su función y responsabilidad laboral.

Campañas diseñadas de simulación (phishing y malware) para obtener métricas y realizar programas de concientización y así obtener unos usuarios más preparados

Herramientas de medición con informes gerenciales y de correlación que puedan indicarnos cuales es el nivel de riesgos en porcentajes.

- Rastreo automático de actividades por usuario.
- Aumentará la toma de conciencia de los buenos comportamientos y habilidades de seguridad dentro de la empresa.
- Contar con personal designado para tener un seguimiento y control del análisis de riesgo, controles y medidas de la seguridad de la información.

CONCLUSIÓN

Tomando en cuenta que los usuarios finales son uno de factores importantes dentro de la empresa se pretende que el mismo cualquiera sea su fiuncion pueda ser parte en el análisis de los controles y que estos sean los adecuados, útiles y aplicables a la empresa.

Que la seguridad de la información pueda ser compartida por toda la entidad y así Disminuir la vulnerabilidad de ataques por la vía del personal.

Medidas para reducir el incumplimiento de los controles y contar con un personal capacitado para afrontar los riesgos técnicos y/o ciberataques.

BIBLIOGRAFÍA

(Antivirus, anti espías, cortafuegos, control parental, anti Phishing, protección web, analizador de Url)

https://www.avast.com/es-es/c-social-engineering

https://sites.google.com/site/seguridadinformaticadanigomez/2-seguridad-fisica/2-2--proteccion-fisica-del-equipo

https://normaiso27001.es/a7-seguridad-relativa-a-los-recursos/

https://www.iso27000.es/iso27002 7.h tml

CIS Controls Spanish Translation v.7

http://jlrivas.webs.uvigo.es/downloads/publicaciones/protinf.pdf

https://www.smartfense.com/es- es/nosotros/smartfense/

Tesis Análisis e Implementación de la Norma ISO 27002 para el Departamento de Sistemas de la Universidad Politécnica Salesiana Sede Guayaquil. Autores Sr. Daniel Romo Villafuerte y Joffre Valarezo Constante. Universidad Politécnica Salesiana Ecuador.

Artículo Recibido: 15/03/2023

Artículo Aceptado: 12/05/2023

LA IMPORTANCIA DE LA SEGURIDAD PERIMETRAL LOGICA EN LAS ORGANIZACIONES EN BASE A LA NORMATIVA ISO 27001

Autora:

Jimena Ruth Castellon Mansilla
jimecastellon1@gmail.com

Resumen

La evolución de la tecnología y la constante demanda de seguridad han permitido que los sistemas de seguridad perimetral en redes evolucionen para ofrecer una mayor confiabilidad a los usuarios sobre la transparencia y protección de su información para el acceso de diferentes servicios. Hoy en día existen muchas personas que usan sus conocimientos y ética profesional de una forma incorrecta al ingresar a redes informáticas restringidas ocasionado pérdidas multimillonarias de información alrededor del mundo.

Es ahí donde aparece la seguridad perimetral como método de defensa de las redes informáticas de una organización y su importancia dentro de la misma a través de los tipos de seguridad perimetral que se puedes clasificar: Seguridad Perimetral Física (protección de ambientes con dispositivos de red) y Seguridad Perimetral Lógica (protección de la red desde lo externo a lo interno).

Es así que la seguridad perimetral lógica dentro de una infraestructura de red se ha vuelto un ele realmente importante puesto que esta el a primera barrera de seguridad y protección preventiva ante cualquier daño o ataque externo.

Esto en base al anexo 13 de la ISO 27001 cuyo objetivo es asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte como la gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección de posibles ataques externos.

Introducción

Esta seguridad perimetral es la primera seguridad con la que se encuentra un atacante cuando quiere entrar dentro de las redes de una empresa, por lo que se trata de un tipo de seguridad bastante importante, ya que, dependiendo de su eficacia, será capaz de rechazar el ataque o de por lo menos desmotivar al atacante de cara a seguir con su tarea.

Es por eso que es importante que una empresa invierta en la seguridad perimetral asi puede protegerse de cualquier tipo de amenaza ya sea esta considerada grande o pequeña, puesto que esta puede llegar a afectar el activo principal de cualquier organización que es el información que maneja.

A través de este articulo científico se pretende demostrar la importancia de que una empresa tenga una buena barrera perimetral de seguridad informática, las ventajas y beneficios que puede brindar tenerla, además de los medio de protección que se usan actualmente los cuales van evolucionando constantemente.

Palabras Clave

Seguridad Perimetral, Seguridad, Organización, Empresa, Red

Contenido Definición de seguridad perimetral

La seguridad del perímetro proviene de un sistema multipropósito integrado que detecta amenazas, realiza vigilancia y analiza patrones de ataque. Como tal, a menudo sirve como la primera línea de defensa de una red contra muchos peligros que pueden dañar los sistemas conectados.

Una de las ideas centrales detrás de la protección de la red frente a amenazas externas es desarrollar e implementar múltiples capas superpuestas de soluciones de seguridad con diferentes componentes de seguridad como firewalls, VPN, IDS / P, Proxying, aplicación de técnicas adecuadas, directrices y estrategias de seguridad.

Algo que hay que tener bastante claro es que protección perimetral es un proceso en constante evolución, por el desarrollo de nuevas tecnologías, puesto que el hecho de que un teléfono posea la capacidad del perímetro de una red y es por eso que el perímetro de red de una organización esta en constante expansión, es por eso que los especialistas IT deben estar en constante evaluación del perímetro.

Existen dos tipos de seguridad perimetral que tiene una organización:

- Seguridad perimetral física: Se refiere a la protección física de ambientes críticos donde se encuentran dispositivos instalados para el funcionamiento de la red internet y acceso de sistemas de información de una empresa.

Clasificamos estos sistemas según el método de detección utilizado.

Abiertos

Son aquellos que dependen de las condiciones ambientales para detectar. Por ejemplo, la video vigilancia, las barreras infrarrojas y las barreras de microondas. Esta característica provoca falsas alarmas o falta de sensibilidad en condiciones ambientales adversas.

Cerrados

Son los que no dependen del medio ambiente y controlan exclusivamente el parámetro de control. Por ejemplo, los históricos cables microfónicos, la fibra óptica y los piezo-sensores. Este tipo de sensores suele tener un coste más elevado.

- Seguridad perimetral lógica: Se refiere a la protección de las redes privadas de un sistema informático, desde lo externo a la red interna, para evitar ataques o el ingreso a los sistemas de personas intrusas desde el exterior.

La mayoría de los ataques de hoy en día ocurren en la capa de aplicación y el filtrado en esta capa superior es extremadamente importante para un diseño de seguridad exitoso. Se requiere una inspección de paquetes mejorada con monitoreo e informes adecuados en todos los puntos finales de la red para bloquear el tráfico malicioso dentro y fuera de la red. Hay varias formas y técnicas involucradas en el diseño de una seguridad perimetral y este diseño propone las soluciones específicas para las amenazas de seguridad en una red de campus amplia que en una red empresarial altamente compleja.

Elementos de protección

Los siguientes elementos de protección son implementados para realizar una adecuad gestión de la seguridad de la red de una empresa, para evitar y controlar posibles riesgos esto en cumplimiento del anexo 13.1 de la normativa ISO 27001.

Cortafuegos

Un cortafuegos es un sistema de seguridad de red de computadoras que restringe el tráfico de Internet dentro, fuera o dentro de una red privada.

Este software o unidad de hardware-software dedicada funciona bloqueando o permitiendo de forma selectiva paquetes de datos. Por lo general, su objetivo es evitar que cualquier persona, dentro o fuera de una red privada, participe en actividades web no autorizadas y ayudar a prevenir actividades maliciosas.

Los cortafuegos pueden verse como fronteras cerradas o puertas de enlace que gestionan el recorrido de la actividad web permitida y prohibida en una red privada. El término proviene del concepto de que las paredes físicas son barreras para frenar la propagación del fuego hasta que los servicios de emergencia puedan extinguirlo. De manera similar, los firewalls de seguridad de red son para la gestión del tráfico web, por lo general destinados a ralentizar la propagación de amenazas web.

Los cortafuegos se clasifican en función de la capa del protocolo de comunicaciones en la que actúan en:

Cortafuegos de nivel de red que se caracterizan por controlar las comunicaciones entre redes a nivel de capa de red. Implementan en tiempo real políticas de seguridad entre redes, estableciendo diferentes niveles de confianza. Dentro de esta subcategoría están los routers con funcionalidad de filtrado de paquetes.

Cortafuegos de nivel de aplicación que operan por encima de la capa de red, a nivel de aplicación y son capaces de controlar protocolos específicos y aplicaciones, por ejemplo los cortafuegos para mensajería instantánea o de aplicaciones web y P2P. Dentro de este tipo se incluyen los cortafuegos- proxy (filtran protocolos de nivel de aplicación HTTP, FTP, SMTP,..).

Otra forma de clasificarlos es según su ámbito de protección, es decir, si están destinados a proteger un pues-

to de trabajo o toda una organización:

Cortafuegos personales para uso particular, en un ordenador personal o en un puesto de trabajo que generalmente vienen incorporados a los Sistemas Operativos.

Cortafuegos corporativos pensados para la protección completa de la red de una organización. Se diferencian de los personales o de puesto de trabajo en la potencia y capacidad de proceso que incorporan, necesaria para controlar y gestionar las miles de conexiones que entran y salen a diario de una red corporativa. Este tipo de cortafuegos puede trabajar tanto a nivel de red como de aplicación.

Redes virtuales privadas o VPN

Una red privada virtual o VPN, es una conexión encriptada a través de Internet desde un dispositivo a una red. La conexión cifrada ayuda a garantizar que los datos confidenciales se transmitan de forma segura. Evita que personas no autorizadas escuchen el tráfico y permite al usuario realizar el trabajo de forma remota. La tecnología VPN se usa ampliamente en entornos corporativos.

Una VPN extiende una red corporativa a través de conexiones encriptadas realizadas a través de Internet. Debido a que el tráfico está encriptado entre el dispositivo y la red, el tráfico permanece privado mientras viaja. Un empleado puede trabajar fuera de la oficina y aún así conectarse de forma segura a la red corporativa. Incluso los teléfonos inteligentes y las tabletas pueden conectarse a través de una VPN.

El tráfico en la red virtual se envía de forma segura al establecer una conexión encriptada a través de Internet conocida como túnel. El tráfico de VPN de un dispositivo como una computadora, tableta o teléfono inteligente se cifra mientras viaja a través de este túnel. Los empleados externos pueden utilizar la red virtual para acceder a la red corporativa.

IPS/ IDS

La detección de intrusiones es el proceso de monitorizar los eventos que ocurren en la red y analizarlos en busca de señales de posibles incidentes, violaciones o amenazas inminentes a tus políticas de seguridad. La prevención de intrusiones es el proceso de realizar la detección de intrusiones y luego detener los incidentes detectados. Estas medidas de seguridad están disponibles como sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS), que se vuelven parte de su red para detectar y detener posibles incidentes.

Los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS) vigilan constantemente tu red, identificando posibles incidentes y registrando información sobre ellos, deteniendo los incidentes e informándolos a los administradores de seguridad. Además,

algunas redes utilizan IDS / IPS para identificar problemas con las políticas de seguridad y disuadir a las personas de violar las políticas de seguridad.

Los IDS / IPS se han convertido en una adición necesaria a la infraestructura de seguridad de la mayoría de las organizaciones, precisamente porque pueden detener a los atacantes mientras recopilan información sobre su red.

Controles de acceso e identidad

El control de acceso es un método para garantizar que los usuarios sean quienes dicen ser y que tienen el acceso adecuado a los datos de la empresa.

En un nivel alto, el control de acceso es una restricción selectiva del acceso a los datos. Consta de dos componentes principales: autenticación y autorización.

La autenticación es una técnica que se utiliza para verificar que alguien es quien dice ser. La autenticación no es suficiente por sí sola para proteger los datos. Lo que se necesita es una capa adicional, la autorización, que determina si un usuario debe tener acceso a los datos o realizar la transacción que está intentando.

Sin autenticación y autorización, no hay seguridad de datos.

Cualquier organización cuyos empleados se conecten a Internet, en otras palabras, todas las organizaciones de hoy, necesita algún nivel de control de acceso. Eso es especialmente cierto en las empresas con empleados que trabajan fuera de la oficina y requieren acceso a los recursos y servicios de datos de la empresa.

Honeypots

Un honeypot es un sistema de seguridad perimetral informática diseñado para detectar y contrarrestar el acceso o uso no autorizado de un sistema informático. El nombre "honeypot" se usa en referencia a la forma en que el sistema atrapa a usuarios no autorizados, como piratas informáticos o spammers, para que puedan ser identificados y evitar que causen más problemas.

Los honeypots son diferentes a las soluciones de seguridad típicas porque atraen intencionalmente a piratas informáticos o usuarios con intenciones maliciosas. Por ejemplo, una empresa puede crear deliberadamente un agujero de seguridad en su red que los piratas informáticos podrían explotar para obtener acceso a un sistema informático. El sistema puede contener datos falsos que serían de interés para los piratas informáticos.

Al obtener acceso a los datos, el pirata informático podría revelar información de identificación, como una dirección IP, ubicación geográfica, plataforma informática y otros datos. Esta información se puede utilizar para aumentar la seguridad contra el pirata informático y usuarios similares.

Sistemas anti-DDos

El software anti-DDoS se ejecuta sobre el hardware existente, analizando y filtrando el tráfico malicioso. Como regla general, el software Anti-DDoS es más rentable y más simple de administrar que las soluciones basadas en hardware. Sin embargo, las soluciones de software y secuencias de comandos solo pueden ofrecer protección parcial contra ataques DDoS, son propensas a falsos positivos y no ayudarán a mitigar los ataques DDoS basados en volumen. El software instalado localmente puede verse abrumado más fácilmente que los dispositivos o las soluciones basadas en la nube.

El hardware DDoS es una capa física entre los atacantes potenciales y tu red. Aunque el hardware DDoS puede proteger de ciertos tipos de ataques, otros tipos, como los ataques DNS, no están influenciados en absoluto por el hardware, ya que el daño se hace bien frente a él.

La protección de hardware, por regla general, es una propuesta costosa.

Directrices y buenas prácticas del perímetro de seguridad informática

Debido a que no existe una solución de seguridad única para todos, el equipo de IT debe utilizar una aplicación variada de hardware y mejores prácticas para reforzar la seguridad de la red alrededor de un data center. Aquí, algunas prácticas recomendadas sobre el perímetro de seguridad informática.

Diseño de la red

El primer paso en la protección del perímetro es configurar un diseño de red seguro que incorpore todos los sistemas, el software y el hardware, que se emplearán para proteger tus datos.

En esta fase, entonces, hay que auditar la configuración actual para encontrar los puntos débiles y definir, lo mejor posible, los límites del perímetro.

Mapear los puntos de conectividad externa, ajustar la configuración del firewall y establecer el control de acceso de autenticación de los usuarios, son otros puntos fundamentales del inicio del proceso.

Monitoreo pasivo

Con la ayuda de dispositivos de seguridad, routers, computadoras, servidores remotos y firewalls, puedes hacer un rastreo en busca de vulnerabilidades e identificar los dispositivos conectados a tu red que actúan como los nodos y límites del perímetro.

Para ello existen una serie de herramientas de monitoreo que ayudan en todo el proceso.

Estas herramientas de monitoreo son pasivas porque necesitan ser activadas o programadas a horas determinadas para rastrear las actividades sospechosas en la red.

Monitoreo activo

Cuando necesites una mirada más rigurosa, cubrir todas las posibles vulnerabilidades de la red, así como para crear una imagen de los patrones de comunicación entre los dispositivos vinculados, entonces se recomienda un monitoreo activo.

Con alertas para notificar a tu equipo en tiempo real sobre patrones irregulares de tráfico en la red, intentos fallidos de inicio de sesión o cualquier otra señal de alarma, las herramientas de monitoreo activo garantizan una vigilancia más exhaustiva de la red, con una cobertura 24/7.

Estos tipos de monitoreo evita los ataques pasivos y activos a la red como es nombrado en la norma ISO 27001.

Zonificación de la red

La zonificación de la red es cuando tu equipo identifica, segmenta y genera zonas de seguridad dentro de la infraestructura de la red.

Este proceso tiene en cuenta las diferentes políticas de seguridad de las zonas individuales, ya que cada una puede requerir diversos niveles de restricción o autenticación. Cada una de ellas se divide en zonas controladas, no controladas, restringidas o seguras. El aislamiento de estas zonas concretas ayuda a evitar que un fallo de seguridad en una, afecte a otra.

6 Razones por las cuales tener una barrera de seguridad perimetral Protege la empresa contra ataques externos

La principal función de una red perimetral es proteger la red interna de ataques externos, que pueden utilizar técnicas de hacking para ingresar y robar información o infectar la red con malware. Al implementar una red perimetral, estableces una barrera entre la red interna y el exterior, lo que te ayudará a evitar que los atacantes externos causen daños en la empresa.

Detección de intrusiones

Al implementar una red perimetral, puedes establecer una barrera entre la red interna y el exterior. Esto te ayudará a detectar intrusiones y tomar medidas para

protegerla. La detección de intrusiones en la red perimetral se realiza mediante el uso de un firewall, que analiza el tráfico entrante y saliente y bloquea el tráfico sospechoso.

Protección contra ataques DDoS

Los atacantes envían un gran volumen de tráfico a un servidor o red para sobrecargarla y hacerla inoperable. Los ataques DDoS pueden ser muy dañinos para una empresa y conlleva grandes costes. Con la red perimetral, crearás una barrera entre tus recursos internos y el exterior, además de evitar los ataques DDoS.

Protección contra el robo de información

Los datos robados pueden incluir información confidencial de los clientes, de la empresa o datos personales. Sin embargo, disponer de una red perimetral informática te ayudará a evitar que los atacantes accedan y roben información de la red interna.

Protección contra el malware

El malware puede dañar los sistemas de la empresa, robar información o espiar las actividades de los usuarios. Al implementar una red perimetral, puede establecer una barrera que te ayudará a evitar que los atacantes infecten la red. Esta actúa como un filtro, permitiendo el tráfico entre la empresa y el exterior, pero bloqueando el tráfico no deseado o peligroso.

En lo que va del 2022, los ataques de ransomware han aumentado considerablemente, lo cual se explica a partir del teletrabajo y la digitalización de gran parte de los procesos en las empresas, aunque los números permiten dimensionar de mejor forma el tamaño de la problemática, pues según los resultados de la encuesta "El estado del ransomware 2021" de ThycoticCentrify, reveló que dos de cada tres empresas que encuestaron, fueron atacadas por lo menos una vez durante los últimos 12 meses.

Mejora de la seguridad de la red

La red perimetral es una parte importante de la seguridad de la información de las empresas. Protege los datos y la red interna de los ataques externos, y ayuda a controlar el tráfico entrante y saliente, lo que mejora la seguridad general de la red.

Conclusiones

Es necesario estar un paso adelante en cuanto a las estrategias protección y ciberseguridad por los constantes riesgos y amenazas a las que se puede encontrar expuesta nuestra red.

Es importante que las empresas inviertan en seguridad perimetral para poder tener sus sistemas y datos protegidos.

En muchos países como en el caso de México los ataques de ramsonware aumentan cada mes, por lo que las organizaciones optan por pagar los rescates de su información sin tener la garantía de que su información sea devuelta integra.

Bibliografía

(s.f.). Esemanal. (1 de agosto de 2022). https://esemanal.mx. Obtenido de https://esemanal.mx/2022/08/las-organizaciones-aumentan-sus-presupuestos-a-doble-

digito-en-ciberseguridad-debido-al-ransomware/

Grupo Atico34. (30 de 1 de 2023). Seguridad perimetral informática. Obtenido de Seguridad

perimetral informática. Qué es y objetivos | Grupo Atico34 (protecciondatos-lopd.com)

Grupo Cibernos. (30 de enero de 2023). https://www.grupocibernos.com. Obtenido de

https://www.grupocibernos.com/blog/6-razones-para-tener-una-red-perimetral-informatica-dmz

INVGATE. (29 de enero de 2023). https://blog.invgate.com. Obtenido de https://blog.invgate.com/es/seguridad-perimetral-

informatica#:~:text=En%20pocas%20palabras%2C%20la%20seguridad,de%20software%2C

%20dispositivos%20y%20t%C3%A9cnicas.

ISO 2700.ES. (1 de febrero de 2023). https://www.iso27000.es. Obtenido de https://www.iso27000.es/iso27002_13.html

SIMAD. (22 de abril de 2019). http://www.si-mad.com. Obtenido de http://www.si-mad.com/la- importancia-de-la-seguridad-perimetral-para-las-empresas/

Artículo Recibido: 14/03/2023

Artículo Aceptado: 12/05/2023

SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD AYER, HOY Y MAÑANA

Autor:
Guillermo Vargas Oros
guille4punto0@gmail.com

Resumen

La seguridad de la información y ciberseguridad no nació como tal realmente hasta que los equipos empezaron a conectarse, formando redes. Esto empezó a suceder en la década de 1950, cuando se desarrollaron las primeras redes informáticas y módems. Si los años 60 sentaron las bases del mundo de la ciberseguridad, la década siguiente nos presentó a los protagonistas, los grandes rivales de nuestra historia: el malware y el software de ciberseguridad. Los años 1990 sentaron las bases del actual internet, con todas las amenazas y protocolos de seguridad que conlleva. Sin embargo, fue en la década de 2000 cuando tomó forma nuestro ciberespacio moderno. Con la versión moderna de internet ya plenamente establecida, la década de 2010 fue testigo de una serie de acontecimientos clave.

Aunque solo llevamos unos pocos años en la década de 2020, ya han ocurrido muchas cosas en el ámbito de la ciberseguridad. En este sentido la ciberseguridad toma tanta importancia, en nuestra actualidad llevando a establecer políticas de seguridad de la información y ciberseguridad bajo normativas establecidas para la realización de Sistema de Seguridad de la Información, Sistema de Continuidad y Contingencia, Gestión de Riesgos Tecnológicos, etc. En todo este proceso de la ciberseguridad la intervención humana aún es necesaria, sin embargo uno de los mejores y más populares temas en tecnología de la información es la automatización de la ciberseguridad.

La automatización y la tecnología jugará un papel importante en todas las áreas del negocio: recursos humanos, servicio al cliente, marketing, ventas y más. En toda una organización de TI, existen procesos que se pueden automatizar para disminuir la carga de trabajo de los empleados, hacer que las operaciones sean más eficientes y permitir que los empleados realicen un trabajo más valioso. Las ventajas de automatizar el sistema de gestión de seguridad de la información se puede destacar por la Integridad, Centralización de la información, Capacidad de análisis, Claridad en los procesos, Innovación y desarrollo.

Palabras Clave

Seguridad de la información, Ciberseguridad, Ciberdelincuencia, Automatización.

Abstract

Information security and cybersecurity did not really come into being as such until computers began to connect, forming networks. This began to happen in the 1950s, when the first computer networks and modems were developed. If the 1960s laid the foundations of the cybersecurity world, the following decade introduced us to the protagonists, the great rivals of our history: malware and cybersecurity software. The 1990s laid the foundations for today's Internet, with all the threats and security protocols that go with it. However, it was in the 2000s that our modern cyberspace took shape. With the modern version of the internet now fully established, the 2010s saw a number of key developments.

Although we are only a few years into the 2020s, a lot has already happened in the cybersecurity arena. In this sense cybersecurity takes so much importance, in our present day leading to establish information security and cybersecurity policies under established regulations for the realization of Information Security System, Continuity and Contingency System, Technological Risk Management, etc. In all this process of cybersecurity human intervention is still necessary, however one of the best and most popular topics in information technology is the automation of cybersecurity.

Automation and technology will play an important role in all areas of the business: human resources, customer service, marketing, sales and more. Throughout an IT organization, there are processes that can be automated to decrease employee workload, make operations more efficient and allow employees to do more valuable work. The advantages of automating the information security management system can be highlighted by Integrity, Centralization of information, Analysis capability, Process clarity, Innovation and development.

Keywords Information Security, Cybersecurity, Cybercrime, Automation.

1. INTRODUCCIÓN

La ciberseguridad es una innovación relativamente nueva, surgida en la segunda mitad del siglo XX, pero ya ha pasado por múltiples fases hasta convertirse en el conjunto de herramientas y estrategias que utilizamos hoy en día. Desde el nacimiento de internet hasta los conflictos cibernéticos mundiales, aquí un poco de la historia de la ciberseguridad a lo largo de las décadas.

2. CONTENIDO

Años 60: nacimiento de la ciberseguridad.

Si bien es cierto que los ordenadores son anteriores a internet (el primer computador automático se creó en 1822 y la primera versión digital electrónica, conocida como ABC, apareció en 1942), la ciberseguridad no nació como tal realmente hasta que los equipos empezaron a conectarse, formando redes. Esto empezó a suceder en la década de 1950, cuando se desarrollaron las

primeras redes informáticas y módems. Sin embargo, fue en la década de 1960 cuando el que hoy conocemos comenzó a tomar forma.

A finales de los años 60, la Agencia de Proyectos de Investigación

Avanzada (ARPA) del Pentágono desarrolló un sistema que permitía a los ordenadores comunicarse entre sí a grandes distancias. Anteriormente, la mayoría de los ordenadores sólo podían conectarse en red si se encontraban en la misma zona, e incluso entonces su capacidad para intercambiar datos era limitada.

En 1969, el nuevo sistema de redes de ARPA (conocido como conmutación de paquetes) fue capaz de enviar un mensaje desde un ordenador de la Universidad de California en Los Ángeles a través del estado hasta un dispositivo del Instituto de Investigación de Stanford. De repente, varios ordenadores podían enviar y recibir paquetes de datos, creando una red de internet. Había nacido el ciberespacio.

Década de 1970: una nueva rivalidad.

Si los años 60 sentaron las bases del mundo de la ciberseguridad, la década siguiente nos presentó a los protagonistas, los grandes rivales de nuestra historia: el malware y el software de ciberseguridad.

Creeper y Reaper.

En 1971, apenas dos años después de que se enviara el primer mensaje a través de ARPNET, un investigador que trabajaba en el proyecto creó Creeper. Se trataba de un sencillo programa que funcionaba independientemente del control humano, moviéndose de un ordenador conectado a otro y mostrando el mensaje "Soy creeper. Atrápame si puedes".

El investigador, Bob Thomas, no era un ciberdelincuente; solo estaba jugando con esta tecnología que evolucionaba tan rápido. Sin embargo, su experimento era una señal de lo que estaba por venir. Aquella plantilla, un programa auto operativo y autorreplicante que se propagaba de un dispositivo a otro, presagiaba el malware tal y como lo conocemos ahora.

Como respuesta a Creeper, otro miembro del equipo Ray Tomlinson, el inventor del correo electrónico creó un programa para perseguir y eliminar el virus. Lo llamó Reaper, y es el primer ejemplo que tenemos de software de ciberseguridad. Esta carrera armamentística entre malware y antimalware sigue impulsando el desarrollo de la ciberseguridad hasta nuestros días.

Adopción y riesgo.

A medida que avanzaba la década de 1970, la adopción de estas tecnologías relativamente nuevas (ordenadores y conectividad a internet) empezó a aumentar. El gobierno estadounidense, que había desarrollado ARPNET, fue uno de los primeros en moverse en este espacio, viendo el potencial que tenían estos sistemas para revolucionar las comunicaciones militares.

Sin embargo, la adopción entrañaba riesgos, ya que ahora se almacenaban y accedían a cantidades cada vez mayores de datos incluida información gubernamental sensible en dispositivos conectados. El gobierno estadounidense empezó a desarrollar software para limitar el acceso no autorizado, lanzando un nuevo proyecto

ARPA llamado Análisis de Protección para tratar de encontrar soluciones de seguridad automatizadas.

A finales de la década de 1970, DEC utilizó un sistema informático llamado The Ark para desarrollar sistemas operativos para otros ordenadores.

En 1979, un estudiante de secundaria estadounidense llamado Kevin Mitnick pirateó The Ark y robó copias de los nuevos sistemas operativos de DEC. Este ciberataque fue notable por varias razones: la juventud del atacante, la severidad del castigo que recibió cuando lo atraparon y la facilidad con la que llevó a cabo el delito.

Todo lo que necesitó fue una llamada telefónica. Utilizando una técnica que hoy conocemos como ingeniería social, el joven Mitnick llamó a alguien de DEC y le convenció de que era un ingeniero jefe de software al que habían bloqueado su cuenta. Convenció a su contacto para que le diera los datos de acceso que necesitaba y pronto tuvo acceso no autorizado a grandes cantidades de datos confidenciales de la empresa.

El cifrado se estandariza.

Otro gran avance en ciberseguridad se produjo con el desarrollo del Estándar de Cifrado de Datos (DES). A principios de la década de 1970, el gobierno estadounidense empezó a comprender que los datos almacenados y transmitidos a través de redes informáticas debían protegerse.

En respuesta, el DES fue desarrollado por investigadores de la empresa tecnológica IBM, con cierta participación de la NSA. En 1977 se publicó oficialmente como Norma Federal de Procesamiento de la Información, fomentando la adopción a gran escala del protocolo.

El DES no era el protocolo de cifrado más robusto, pero funcionaba lo suficientemente bien como para ser adoptado y respaldado por la NSA y, a su vez, por la comunidad de seguridad en general. Siguió siendo un método de cifrado muy utilizado hasta que fue sustituido en 2001.

Cuando la ciberseguridad aún estaba en pañales, en la década de 1970 se llegó a la conclusión de que el cifrado podía proteger los datos y prevenir de forma proactiva los ciberataques y las violaciones de datos. Sin embargo, como demostró el incidente de Kevin Mitnick, los piratas informáticos seguían teniendo muchas otras formas de acceder a datos confidenciales. La ingeniería social y el error humano siguen siendo valiosas bazas de los ciberdelincuentes a día de hoy.

Década de 1980: la ciberseguridad se generaliza.

En la década de 1980, los ordenadores con acceso a internet se utilizaban en la administración pública, las instituciones financieras y muchos otros ámbitos de la vida. Esto significaba un número cada vez mayor de oportunidades para que los piratas informáticos robaran información valiosa o simplemente causaran trastornos con virus y otros programas maliciosos.

Los ciberataques acaparan titulares.

A lo largo de la década de 1980, los ciberataques de alto perfil contra AT&T, National CSS y otras instituciones importantes empezaron a aparecer en las noticias. En 1983, los hackers entraron realmente en la corriente principal después de que la película WarGames mostrara una historia ficticia en la que un hacker consigue

acceder a los sistemas de armas nucleares.

La mayoría de las primeras representaciones mediáticas de hackers y ciberdelincuentes eran inexactas y melodramáticas, pero el público empezaba a ser consciente del concepto "cibernético". Internet ya estaba aquí y, aunque la tecnología aún tenía un largo camino por recorrer, la gente empezaba a comprender sus ventajas y riesgos.

Década de 1990: Comienza la era de internet.

Los años 90 continuaron con las tendencias de adopción y riesgo crecientes, pero fue en esta década cuando comenzó a acelerarse la proliferación generalizada de internet.

La nueva normalidad.

Microsoft lanzó múltiples versiones nuevas y mejoradas de su sistema operativo Windows a lo largo de la década de 1990, centrándose cada vez más en dar servicio a los consumidores particulares en lugar de a las empresas u organismos gubernamentales. También lanzó Internet Explorer con Windows 95, que siguió siendo el navegador web más popular durante casi dos décadas.

Este paso fue a la vez un reflejo y una fuerza motriz del hecho de que los ordenadores eran cada vez más asequibles y estaban más al alcance de todos. A lo largo de la década de 1980, el conocimiento público de esta nueva tecnología aumentó considerablemente, y ahora la gente quería poder acceder a internet desde la comodidad de su propia casa.

Los productos de Microsoft, asequibles para el consumidor, hicieron que Internet fuera más accesible que nunca y, de repente, millones de personas de todo el mundo enviaban correos electrónicos, investigaban e incluso jugaban online.

El ciberespacio ya no era dominio exclusivo de las empresas tecnológicas y el ejército. Una sociedad conectada digitalmente era la nueva normalidad, y todo el mundo quería participar en ella.

Los peligros del correo electrónico.

Una de las primeras funciones útiles que internet ha desempeñado para los usuarios particulares ha sido el correo electrónico. Plataformas como Microsoft Outlook ofrecieron a la gente la posibilidad de utilizar servicios de mensajería rápida, algo que nunca antes había existido.

Como es lógico, muchos internautas adoptaron con entusiasmo el correo electrónico como nueva forma de comunicación y, como era de esperar, también lo hicieron los ciberdelincuentes. Uno de los ataques más impactantes y costosos de la década se produjo en 1999, cuando el virus Melissa comenzó a propagarse por las bandejas de entrada de Outlook.

Este incidente demostró dos cosas. En primer lugar, la nueva red mundial de comunicaciones por internet permitía la propagación de programas maliciosos a una velocidad sin precedentes. En segundo lugar, los protocolos de seguridad actuales seguían siendo lamentablemente inadecuados, especialmente cuando había un poco de ingeniería social de por medio. Un software de seguridad robusto seguía sin ser rival para la curiosidad humana que llevó a tantos a abrir un "mensaje importante".

La década de 2000: un nuevo nivel de conectividad.

Los años 90 sentaron las bases del actual internet, con

todas las amenazas y protocolos de seguridad que conlleva. Sin embargo, fue en la década de 2000 cuando tomó forma nuestro ciberespacio moderno.

La ciberdelincuencia evoluciona.

El principal objetivo de los ciberdelincuentes seguía siendo la propagación de programas maliciosos, y a principios de la década de 2000 se empezó a emplear un nuevo método que se sigue utilizando hoy en día. La gente desconfiaba cada vez más de los archivos adjuntos a los correos electrónicos, y algunos servicios de correo electrónico incluso escaneaban ahora los archivos adjuntos para comprobar si presentaban riesgos. Para saltarse estas defensas, los hackers se dieron cuenta de que podían engañar a la gente para que abandonara la relativa seguridad de sus servicios de correo electrónico y visitara una página web creada por el hacker.

Este proceso consiste en convencer a la víctima de que el correo electrónico procede de un remitente de confianza: un banco, por ejemplo, o una agencia gubernamental. El mensaje pide al destinatario que haga clic en un enlace, quizá para cancelar una transferencia bancaria inesperada o reclamar un premio. En realidad, el enlace les lleva a un sitio web donde se puede instalar malware en su dispositivo o donde sus datos personales pueden quedar expuestos.

Una vez más, los hackers se daban cuenta de que podían utilizar la ingeniería social para engañar a la gente y ponerla en peligro de formas que su limitado software de seguridad no podía evitar. Esta técnica se sigue utilizando hoy en día y sigue siendo desgraciadamente eficaz.

En respuesta a la escalada de la ciberdelincuencia, el Departamento de Seguridad Nacional de Estados Unidos fundó su División Nacional de Ciberseguridad. Por primera vez, el gobierno estadounidense y el mundo en general reconocieron el hecho de que la ciberseguridad era ahora una cuestión de importancia nacional e incluso mundial. Defender el ciberespacio de delincuentes y malos actores era una cuestión tanto de seguridad personal como de seguridad estatal.

La década de 2010: conflictos en el ciberespacio.

Con la versión moderna de internet ya plenamente establecida, la década de 2010 fue testigo de una serie de acontecimientos clave: la evolución de nuevas tácticas de guerra cibernética, las crecientes tensiones en torno a la privacidad de los datos personales y los enormes riesgos que plantean las filtraciones de datos corporativos.

El debate sobre la privacidad.

Mientras Rusia y Estados Unidos sondeaban mutuamente sus ciberdefensas, otra batalla empezaba a calentarse: la batalla por la privacidad en línea.

A principios de la década de 2010, empezó a crecer la conciencia pública en torno a la recopilación de datos. Empresas como Facebook y Google estaban recopilando enormes cantidades de información sobre sus usuarios y la utilizaban para dirigir la publicidad a sus propias plataformas o la vendían a terceros anunciantes.

La regulación gubernamental no era suficiente, por lo que muchas empresas podían participar en la recopilación masiva e invasiva de datos sin infringir ninguna ley. En respuesta, muchos particulares tomaron medidas para mejorar su propia seguridad.

Desde entonces, se han aprobado leyes similares en todo el mundo, pero muchos particulares han tomado medidas para mejorar su propia seguridad. Durante la

década de 2010, surgió un nuevo sector del mercado de la ciberseguridad.

La década de 2020 y más allá.

Por último, llegamos a la década actual y al futuro de la ciberseguridad. Aunque solo llevamos unos pocos años en la década de 2020, ya han ocurrido muchas cosas en el ámbito de la ciberseguridad. Hemos visto surgir nuevos riesgos como resultado de Covid-19 y el trabajo a distancia, ataques masivos contra infraestructuras críticas en Estados Unidos y la guerra cibernética llevada a nuevas cotas en la guerra entre Rusia y Ucrania.

La normalidad 2020.

El estallido de la pandemia Covid a principios de 2020 tuvo un profundo impacto en la evolución de la ciberseguridad y la privacidad de los datos.

Por un lado, aceleró un proceso que comenzó en la década de 1990, cuando se generalizó el acceso a los ordenadores e Internet.

El cambio al trabajo a distancia dio lugar a que millones de personas se conectaran a las redes y bases de datos de las empresas desde sus propios hogares, a menudo utilizando sus dispositivos personales. Fue una oportunidad de oro para los piratas informáticos, que lo tuvieron mucho más fácil para atacar los ordenadores personales y los Smartphone de la gente que si esas mismas personas hubieran utilizado dispositivos de trabajo cargados con software de seguridad. Según Sophos Group, una empresa británica de software de seguridad, más de la mitad de las empresas sufrieron ataques de ransomware solo en 2020.

También se produjo un gran aumento de los ataques de phishing relacionados con Covid. Millones de personas recibieron mensajes de texto en los que se les ofrecían vacunas y medicamentos contra el Covid o se les advertía de que habían estado en estrecho contacto con una persona infectada. Por supuesto, cada mensaje instaba al receptor a hacer clic en un enlace, y ya se sabe el resto.

El Covid nos recordó que, cuatro décadas después de que Kevin Mitnick consiguiera entrar en los sistemas de El Arca, la ingeniería social sigue siendo una forma eficaz de saltarse los protocolos de seguridad.

En la actualidad se ve un cambio todavía de mayor calado gracias a la generali¬zación del uso de Internet, la digitalización de la economía a todos los niveles y la aparición de nuevas tecnologías, como la computación en la nube. Una revolución más que una evolución, una transformación global de la economía en la que los datos y la información son la nueva materia prima. Así, los usuarios, tanto personas como empresas, son capaces de darse de alta de forma inmediata, relacionarse con las administraciones, interaccionar entre ellos, muchas veces implicando transacciones económicas, sin salir de casa y utilizando en muchas ocasiones las contraseñas como única forma de garantizar la identidad.

Este nuevo entorno ha permitido el crecimiento exponencial de la economía digital, pero también ha supuesto problemas de seguridad, como la captura de contraseñas que ha llevado a que se hayan producido casos de robo de dinero o de usurpación de la identidad de usuarios. Las personas y organizaciones han ido adqui-

riendo mayor conciencia de esta si¬tuación a medida que el número de actividades que se realizan de forma digital ha ido aumentando y han ido adquiriendo una naturaleza más económica.

Como se ha comentado, los ciberataques sobre las empresas tienen generalmente un impacto, al menos económico, superior a cuando se producen sobre las personas. Por ese motivo las empresas suelen definir planes relativos a la seguridad tecnológica. No obstante, las empresas más pequeñas tienen más dificultad a la hora de poner en marcha estos planes, ya que disponen de menos recursos y formación específica en este tipo de tecnologías.

De entre las empresas que disponen de este tipo de políticas de seguridad, se observa que ya no existe una brecha tan importante entre ellas en función del tamaño, aunque se sigue dando el caso de que las empresas cuanto más grandes, más aspectos tienen en cuenta en los planes de seguridad, además de realizar revisiones de dichos planes con una frecuencia superior.

La ciberseguridad es, en este sentido, un proceso que implica prevención, detección y reacción o respuesta, y que debe incluir un elemento de aprendizaje para la mejora continua del propio proceso.

Por lo antes expuesto es que la ciberseguridad toma tanta importancia, en nuestra actualidad llevando a establecer políticas de seguridad de la información y ciberseguridad, particularmente en Bolivia se han establecido las siguientes normativas para que desarrollen planes institucionales de Seguridad de la Información acordes a los lineamientos establecidos por el CGII (Centro de Gestión de Incidentes informáticos), decretos y demás normativas como las que se describen a continuación:

Decreto Supremo No. 2514 de 9 de septiembre de 2015.

Parágrafo III del Artículo 17, que establece que "Las entidades del sector público deberán desarrollar el Plan Institucional de Seguridad de la Información acorde a los lineamientos establecidos por el CGII".

Planes de Contingencia Tecnológica.

Decreto Supremo No. 1793, de Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, de 13 de noviembre de 2013: Artículo 8 (Plan de contingencia), que establece que: "Las entidades públicas promoverán la seguridad informática para la protección de datos en sus sistemas informáticos, a través de planes de contingencia desarrollados e implementados en cada entidad".

Cuánto hemos avanzado...

Ley General de telecomunicaciones, tecnologías de información y comunicación, 8 de agosto de 2011.

Decreto Supremo No. 1793, 13 de noviembre de 2013.

Decreto Supremo No. 2514, 9 de Septiembre, 2015.

Decreto Supremo No. 3251 del 12 de Julio de 2017.

Ley 164.

El inciso d) del Artículo 4 (Principios), parágrafo II, del Decreto Supremo No. 1793 de 13 de noviembre de 2013 que señala que: "Se debe implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento".

Decreto Supremo 1793.

El Artículo 8 (Plan de contingencia) del Decreto Supremo No. 1793 de 13 de noviembre de 2013 que menciona que: "Las entidades públicas promoverán la seguridad informática para la protección de datos en sus sistemas informáticos, a través de planes de contingencia desarrollados e implementados en cada entidad".

Decreto Supremo 2514.

Inciso f) del Artículo 7 que sostiene que la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación establecerá "los lineamientos técnicos en seguridad de información para las entidades del sector público".

Inciso i) del Artículo 7 que establece entre las funciones de la AGETIC, "Elaborar proponer, promover, gestionar, articular y actualizar el Plan de Implementación de Gobierno Electrónico y el Plan de Implementación de Software Libre y Estándares Abiertos para las entidades del sector público y otros planes relacionados con el ámbito de gobierno electrónico y seguridad informática".

Decreto Supremo 2514.

Parágrafo I del Artículo 8 de creación del "Centro de Gestión de Incidentes Informáticos CGII como parte de la estructura técnico operativa de la AGETIC".

Inciso c) del Parágrafo II del Artículo 8, que menciona como una de las funciones del Centro de Gestión de Incidentes Informáticos CGII, "Establecer los lineamientos para la elaboración de Planes de Seguridad de Información de las entidades del sector público".

Decreto Supremo 2514.

Parágrafo III del Artículo 17 que establece que "Las entidades del sector público deberán desarrollar el Plan Institucional de Seguridad de la Información acorde a los lineamientos establecidos por el CGII".

Parágrafo II del Artículo 18 que señala que "Las entidades del sector público, en el marco de la Soberanía Tecnológica, deben designar un Responsable de Gobierno Electrónico y Tecnologías de Información y Comunicación y un Responsable de Seguridad Informática, encargados de coordinar con la AGETIC".

Decreto Supremo 2514.

Disposición transitoria segunda, que sostiene que "Las entidades del nivel central del Estado deberán presentar a la AGETIC, en un plazo no mayor a un 1 año, desde la aprobación de las políticas de seguridad de la información por la AGETIC, su Plan Institucional de Seguridad de la Información".

Decreto Supremo 3251.

El Decreto Supremo N 3251 del 12 de julio de 2017 de aprobación del Plan de Implementación de Gobierno Electrónico, que establece como una de las líneas estratégicas la seguridad informática y de la información.

Plan institucional de Seguridad de la Información PISI.

Establecer los lineamientos para que las entidades del sector público del Estado Plurinacional de Bolivia puedan elaborar e implementar sus Planes Institucionales de Seguridad de la Información, en concordancia con la normativa vigente.

Partiendo de los requisitos del estándar ISO/IEC 27001 que indican "qué debe tener un SGSI", los miembros de los grupos de trabajo relacionados con este estándar

publican guías de implementación bajo la misma numeración "270xx" orientadas precisamente a servir de ayuda en aspectos prácticos relacionados directos y/o indirectamente con cláusulas concretas de la norma ISO/IEC 27001.

Aunque no son la única referencia útil, las publicaciones de esta serie "270xx" sí evitan en mayor o menor medida "reinventar la rueda" con el sustancial ahorro de tiempo en la implantación, mantenimiento y mejora de los SGSI.

Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044 con 27799 finalizando la serie formalmente en estos momentos.

ISO/IEC 27000.

Publicada el 1 de mayo de 2009, revisada con una segunda edición de 01 de diciembre de 2012, una tercera edición de 14 de enero de 2014 y una cuarta en febrero de 2016. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI.

ISO/IEC 27001.

Publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013 (segunda edición) y actualizada el 25 de octubre de 2022 (versión 3). Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información.

ISO/IEC 27002.

Publicada inicialmente el 1 de julio de 2007, renombra la norma ya publicada ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable.

ISO/IEC 27003.

Publicada el 01 de febrero de 2010 y actualizada el 12 de abril de 2017. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001. Describe el proceso de especificación y diseño.

Publicada el 15 de diciembre de 2009 y revisada en diciembre de 2016. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

ISO/IEC 27005.

Publicada la cuarta edición en octubre de 2022 con actualizaciones respecto a requisitos y estructura de la norma ISO/IEC 27001:2022. Se alinea la terminología con ISO 31000:2018 y se han introducido conceptos en escenarios de riesgos con un enfoque a eventos que contrata con el enfoque clásico basado en activos para la identificación de los riesgos.

ISO/IEC 27006.

Publicada en segunda edición el 1 de diciembre de 2011 (primera edición del 1 de marzo de 2007) y revisada el 30 de septiembre de 2015 con una adenda del

27 de marzo de 2020. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

ISO/IEC TS 27006-2:2021.

Publicada en su primera edición el 26 de junio del 2021 especifica los requisitos y brinda orientación para los organismos que proporcionan servicios de auditoría y certificación de un sistema de gestión de información de privacidad (PIMS) de acuerdo con ISO/IEC 27701 en combinación con ISO/IEC 27001, además de los requisitos contenidos en ISO/IEC 27006 e ISO/ IEC 27701. Está destinado principalmente a respaldar la acreditación de organismos de certificación que brindan la certificación PIMS.

ISO/IEC 27007.

desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

ISO/IEC 27004.

Publicada el 14 de noviembre de 2011, revisada el 09 de octubre de 2017 y con una última versión de 21 de enero de 2020. No certificable. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011.

ISO/IEC TS 27008.

Publicada el 15 de octubre de 2011 como ISO/IEC TR 27008 (Technical Report) es sustituido con una primera edición como "TS" (Technical Specification) desde el 14 de enero de 2019. No certificable. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.

ISO/IEC 27009.

Publicada inicialmente el 15 de junio de 2016, revisada el 21 de abril de 2020. No certificable. Define los requisitos para el uso de la norma ISO/IEC 27001 en cualquier sector específico (campo, área de aplicación o sector industrial). El documento explica cómo refinar e incluir requisitos adicionales a los de la norma ISO/ IEC 27001 y cómo incluir controles o conjuntos de control adicionales a los del Anexo A.

ISO/IEC 27010.

Publicada el 20 de octubre de 2012 y revisada el 10 de noviembre de 2015. Consiste en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores.

ISO/IEC 27011.

Publicada el 15 de diciembre de 2008 y revisada en diciembre de 2016. Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002. Está publicada también como norma ITU-T X.1051.

ISO/IEC 27013.

Publicada el 15 de octubre de 2012 y actualizada el 24 de Noviembre de 2015 y en Noviembre del 2021 en su tercera edición. Es una guía de implementación integrada de ISO/IEC 27001:2013 (gestión de seguridad de la información) y de ISO/IEC 20000-1:2018 (gestión de servicios TI).

ISO/IEC 27014.

Publicada el 23 de abril de 2013 y actualizada en se-

gunda edición en diciembre 2020 consiste en una guía de gobierno corporativo de la seguridad de la información, la ciberseguridad y privacidad.

ISO/IEC TR 27015.

Publicada el 23 de noviembre de 2012. Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros.

ISO/IEC TR 27016.

Publicada el 20 de febrero de 2014. Es una guía de valoración de los aspectos financieros de la seguridad de la información.

ISO/IEC 27021.

Publicada el 31 de octubre de 2017 especifica los requisitos de competencia para aquellos profesionales que lideran o participan en el establecimiento, implementación, mantenimiento y mejora continua de uno o más procesos del sistema de gestión de seguridad de la información (SGSI) que cumplan con ISO/IEC 27001.

ISO/IEC 27035.

Publicada el 17 de agosto de 2011. Proporciona una guía sobre la gestión de incidentes de seguridad en la información.

ISO/IEC 27039.

Publicada el 11 de febrero de 2015. Es una guía para la selección, despliegue y operativa de sistemas de detección y prevención de intrusión (IDS/IPS). Existe una corrección al contenido inicial de 28 de abril de 2016, etc.

La elaboración de Sistema de Seguridad de la Información, Sistema de Continuidad y Contingencia, Gestión de Riesgos Tecnológicos tienen como objetivo evaluar todos los riesgos asociados con los datos e información que se manejan en una empresa, los principales beneficios de un SGSI son:

- Reducción de riesgos.
- Reducción de costes.
- Integración de la seguridad en el negocio.
- Cumplimiento de la normativa vigente en seguridad.
- Incremento de la competitividad.

En todo este proceso de la ciberseguridad la intervención humana aun es necesaria, sin embargo uno de los mejores y más populares temas en tecnología de la información es la automatización de la ciberseguridad. La automatización de tareas repetibles permite a las empresas y a las personas centrarse en más actividades de resolución de problemas. Un enfoque en las actividades de resolución de problemas puede fomentar la innovación y crear una organización más resistente a la cibernética.

La ciberseguridad diseñada para automatizar procesos específicos está muy extendida, y es probable que ya tenga herramientas de automatización en su empresa.

La automatización no es solo una palabra técnica de moda o una moda pasajera. Está siendo adoptado por empresas grandes y pequeñas por igual. Al implementar la automatización en el entorno de una organización, el equipo de ciberseguridad puede concentrarse en actividades que son más complejas. Esto significa que la máquina puede realizar trabajos repetitivos y los miembros del equipo de ciberseguridad pueden participar en trabajos más críticos, creativos y técnicos para resolver problemas y mejorar la postura de riesgo de la organización. Una vez que se automatizan las actividades apropiadas, los profesionales de ciberseguridad

pueden enfocarse en proyectos como:

- Ingeniería y arquitectura.

La automatización permitirá que el equipo de seguridad cibernética se concentre en diseñar e implementar estrategias de seguridad cibernética, incluidas iniciativas como la confianza cero y la higiene cibernética dentro de la empresa.

- Actividades de remediación.

Las brechas identificadas a partir de sus esfuerzos de automatización ayudarán a sus equipos técnicos y de misión al proporcionar una vista más repetible y procesable del entorno comercial que conduce a menos vulnerabilidades.

- Ingeniería y desarrollo de automatización.

La automatización se convertirá en una parte importante del curso de seguridad cibernética en línea que requiere sus propios recursos relacionados con el diseño y la implementación de automatización continua e iterativa.

La automatización y la tecnología juega un papel importante en todas las áreas del negocio: recursos humanos, servicio al cliente, marketing, ventas y más. En toda una organización de TI, existen procesos que se pueden automatizar para disminuir la carga de trabajo de los empleados, hacer que las operaciones sean más eficientes y permitir que los empleados realicen un trabajo más valioso.

Con respecto a las ventajas de automatizar el sistema de gestión de seguridad de la información se puede destacar:

- Integridad.

La información se encuentra en óptimas condiciones al estar en un soporte informático seguro y diseñado especialmente para el fin establecido. Es decir, está en un medio controlado y resulta difícil que dicha información se pierda o se utilice para otros fines, ya que el propio sistema dispone de una serie de medidas preventivas (copias de seguridad, control de accesos, etc.).

- Centralización de la información. El sistema informático será la fuente de información principal, haciendo que documentos, registros y demás información sea manejada a través suyo, lo que contribuye a evitar problemas de revisiones no controladas de los documentos o errores en la distribución de los mismos.

- Capacidad de análisis.

Tener en cuenta la agilidad en la generación de informes, tanto internos como externos. Al contar con información debidamente organizada se pueden tener datos analíticos o estadísticos en tiempo real (permanentemente

actualizados) y de una forma inmediata, evitando pérdidas de tiempo innecesarias.

- Claridad en los procesos.

Los procesos alrededor del sistema de información se tornarán más claros siguiendo unas reglas ágiles y perfectamente identificadas.

- Innovación y desarrollo. Normalmente los sistemas de gestión informatizados están sujetos a la mejora continua a través de los mantenimientos programados de las empresas desarrolladoras de software, en forma de actualizaciones y nuevas versiones, principalmente contando con la aportación de sus propios clientes.

Se deben tener en cuenta los factores culturales mencionados al principio de este artículo y se considera que la automatización del sistema de gestión de seguridad de la información ayudará a minimizar costes de tiempo y dinero a la empresa, su implementación debe ser un objetivo primordial para cualquier organización.

Es necesario mencionar el cambio en el modelo de consultoría de los sistemas automatizados de gestión, no solo en la implementación sino también en la certificación.

Esto significa que la máquina puede realizar trabajos repetitivos y los miembros del equipo de ciberseguridad pueden participar en trabajos más críticos,

creativos y técnicos para resolver problemas y mejorar la postura de riesgo de la organización. Una vez que se automatizan las actividades apropiadas, los profesionales de ciberseguridad pueden enfocarse en proyectos como Ingeniería y arquitectura, Actividades de remediación, Ingeniería y desarrollo de automatización.

3. CONCLUSIONES

El desafío de invertir en la automatización del Sistema de Seguridad de la Información, significa pensar en el problema que tienen latente y a corto plazo: muchos dicen “a mí no me va a pasar” y así asumen el riesgo. La seguridad de la información es la protección de la información o datos que tienen valor para una organización, a través de la reducción de riesgos y mitigando las amenazas posibles, a medida de esto existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes para minimizar los posibles ataques o riesgos de la información estructural de la organización.

El presente artículo tiene como finalidad sugerir la automatización del Sistema de Seguridad de la Información. Teniendo en cuenta que aproximadamente el 30% de los controles contenidos en el estándar internacional ISO/IEC 27002 son automatizables, la aplicación del resultado de esta investigación será una excelente vía para lograr que la gestión de la seguridad informática sea un proceso menos complejo y más efectivo.

4. BIBLIOGRAFÍA

BST, A. (4 de mayo de 2021). Ambit BST. Recuperado el 25 de enero de 2023, de https://www.ambit- bst.com/blog/para-qu%C3%A9- sirve-un-sgsi-controles-y-fases#:~:text=Qu%C3%A9%20es% 20SGSI,se%20manejan%20en%20 una%20empresa.

careerera. (15 de marzo de 2022). careerera. Recuperado el 27 de enenro de 2023, de https://www.careerera.com/es/blog/ is-cyber-security-automation-the- future-es

ISO. (2005). iso27000.es. Recuperado el 1 de febrero de 2023, de https://www.iso27000.es/iso27000. html

Razón, L. (s.f.). La Razón. Recuperado el 1 de enero de 2023, de https://www.la-razon.com/

Sánchez, L. O. (25 de diciembre de 2022). NordVPN. Recuperado el 1 de febrero de 2023, de https://nordvpn.com/es/blog/historia ciberseguridad

Telefónica, F. (2016). Ciberseguridad, la protección de la información en un mundo digital. Barcelona (España): Editorial Ariel, S.A.

Artículo Recibido: 14/03/2023

Artículo Aceptado: 12/05/2023

ANÁLISIS COMPARATIVO CON LA NORMA ISO 27032, NORMAS DEL SISTEMA FINANCIERO Y LOS REQUISITOS MÍNIMOS DE SEGURIDAD PARA LOS SERVICIOS DE BANCA DIGITAL

Autor:

Ing. Michael Mario Sejas Quinteros

micsejas@gmail.com

Resumen

La banca digital es un tipo de banca que se realiza en línea a través de servicios como internet banking, pagos móviles y otros. Esta forma de banca permite a los usuarios realizar transacciones bancarias sin tener que visitar físicamente una sucursal bancaria. Permite el acceso a la banca desde cualquier lugar con una conexión a internet. Algunos de los servicios principales que ofrece la banca digital incluyen transferencias de dinero, pagos de facturas, gestión de cuentas, compra de tarjetas de regalo, inversión en fondos de inversión, préstamos, tarjetas de crédito, tarjetas de débito y tarjetas prepagas. Estas características hacen que la banca digital sea una forma conveniente y segura de realizar transacciones bancarias. Para ello el Banco Central de Bolivia y la Autoridad de Supervisión del Sistema Financiero (ASFI) establecieron normas con sus circulares externas para la protección de los datos en el ciberespacio, en actual documento tiene el propósito de comparar los reglamentos por las entidades antes mencionadas con la ISO27032.

Palabras Claves:

27032, Recopilación de Normas del Sistema Financiero, Servicios de Banca Digital,

Abstract

Digital banking is a type of banking that is done online through services such as internet banking, mobile payments and others. This form of banking allows users to carry out banking transactions without having to physically visit a bank branch. Allows access to banking from anywhere with an internet connection. Some of the main services offered by digital banking include money transfers, bill payments, account management, purchasing gift cards, investing in mutual funds, loans, credit cards, debit cards, and prepaid cards. These features make digital banking a convenient and secure way to conduct banking transactions. For this, the Central Bank of Bolivia and the Supervision Authority of the Financial System (ASFI) carry out regulations with their external circulars for the protection of data in cyberspace, the current document has the purpose of comparing the regulations by the aforementioned entities with the ISO27032.

Introducción

En los últimos años la necesidad de avanzar a servicios de Banca Digital se ha vuelto una necesidad para llegar a más usuarios y así mismos las entidades financieras que no tienen los servicios antes mencionados el BCB (Banco Central de Bolivia) en la CIEXN°59/2020 del 23 de diciembre de 2020 con Ref: INTEROPERABILIDAD DE CANALES ELECTRÓNICOS Y OPERATIVA 24/7 PARA EL PROCESAMIENTO DE ORDENES ELECTRÓNICOS, en la circular externa menciona el Banco Central de Bolivia promueve en la regulación de pagos nacional el servicio de Ordenes electrónicas (OETFS) con las que cuenta para el modulo de Liquidación Diferida (MLD) y el Sistema de liquidación integrada de pagos (LIP) para el procesamiento de las OETF las 24 horas del días y los 7 días de la semana por otro lado menciona que se debe dar fiel cumplimiento de a los plazos comprometidos por las Instituciones Financieras.

Contenido

2.1 27032

ISO/IEC 27032 es una norma internacional publicada por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. Describe un enfoque integral de la seguridad cibernética, que tiene como objetivo ayudar a las organizaciones y las personas a proteger su información y los sistemas de información de las amenazas cibernéticas. El estándar está organizado en seis áreas clave: Gestión de riesgos, Gobernanza de la seguridad, Gestión de activos, Gestión de identidades y accesos, Gestión de amenazas y vulnerabilidades y Gestión de incidentes de seguridad.

La capacitación en ISO/IEC 27032 puede proporcionar a las organizaciones e individuos el conocimiento y las habilidades para implementar efectivamente el estándar en su organización. La capacitación puede incluir temas como la evaluación de riesgos, la gobernanza de la seguridad, la gestión de activos, la gestión de identidades y accesos, la gestión de amenazas y vulnerabilidades y la gestión de incidentes de seguridad.

Además, la capacitación puede incluir temas como políticas de seguridad, implementación de controles de seguridad y conciencia de seguridad. La capacitación también puede incluir otros temas, según sea necesario, como los requisitos legales y reglamentarios, y la privacidad y la protección de datos.

Por otro lado, establece controles por los diferentes ámbitos sin embargo estos controles son de manera genérica para por otro denomina a los activos en el ciberespacio como ser:

La información

Software como programa de computadora.

Físico, como el de computadora

Los servidores.

Las personas, sus cualidades, habilidades y experiencia.

Los activos intangibles como reputación e imagen.

2.2 Normativa ASFI

Por otro lado, la ASFI en su Libro 3° Título VII Capítulo II Sección 1 inciso l define la Computación en la nube (Cloud Computing) como un "Modelo de Acceso bajo demanda a través de una red (Internet), a un conjunto compartido de recursos informáticos o computacionales (redes, servidores, almacenamiento, aplicaciones o servicios) que pueden ser rápidamente provisionados y publicados con un mínimo esfuerzo de administración o de interacción con el proveedor de servicios, con un sistema de precios basado en el consumo realizado" y en Libro 3° Título VII Capítulo II Sección 11 Articulo 10 Servicio de computación en la nube, donde la entidad supervisada "debe solicitar la no objeción a ASFI en forma escrita, adjuntando para su evaluación el "Proyecto de implementación del servicio de computación en la nube", el cual tiene que reflejar mínimamente, el cumplimiento de los siguientes aspectos:

a. Que no se vulnerará el Derecho a la Reserva y Confidencialidad, establecida en

el Artículo 472 de la Ley N°393 de Servicios Financieros;

b. Que no se encuentra dentro de las Limitaciones y Prohibiciones, establecidas en los Títulos II, III y IV de la Ley N°393 de Servicios Financieros, referidos a "Servicios Financieros y Régimen de Autorizaciones", que pueden realizar las entidades supervisadas por ASFI;

c. Que el proveedor del servicio cumpla con los requisitos de seguridad de la información dispuestos en el presente Reglamento;

d. Que el proveedor del servicio cumpla con la normativa y legislación del Estado Plurinacional de Bolivia, existiendo la posibilidad de poder ser examinado por ASFI y/o empresas de auditoría externa bolivianas;

e. Que, en su análisis y evaluación de riesgos en seguridad de la información, se justifique la pertinencia de contratar el servicio de computación en la nube;

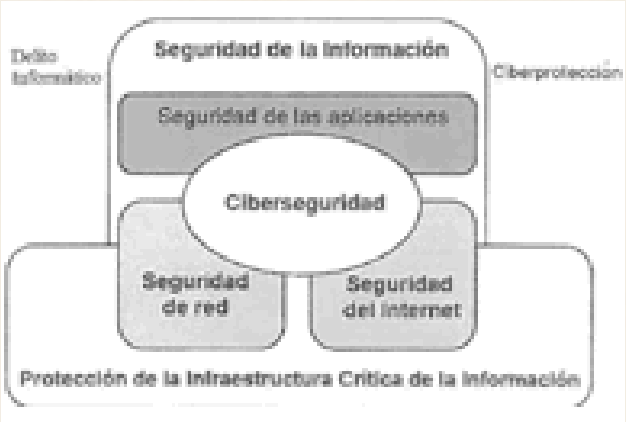
f. Que en las cláusulas del contrato se contemplen los aspectos señalados en los incisos a, b, c y d del presente Artículo.

ASFI podrá objetar la implementación del servicio de computación en la nube, cuando el proyecto presentado, incumpla con lo señalado en los incisos a, b, c, d y f y/o considere insuficiente el análisis y evaluación de riesgos en seguridad de la información, en lo referido a la pertinencia de contratar el servicio de computación

en la nube (inciso e). A efectos de realizar la evaluación del citado proyecto, la Entidad Supervisada debe remitir adjunto a éste copia del borrador del contrato, así como otra documentación que considere pertinente"

Tras la verificación con la ISO/IEC 27032 la misma no se encuentra alejada de la que menciona la norma en la que se basa la documentación y por otro la Recopilación de Normas del Sistema Financiero no es limitativo y las mismas pueden ser utilizadas con otras normas relacionadas, en los controles de la ISO/IEC 27032 establece mecanismos para la protección de los datos Controles de Ciberseguridad las mismas establece los siguientes controles:

- Controles a nivel de aplicación
- Protección del servidor.



Fuente: ISO/IEC 27032

2.3. REQUERIMIENTOS OPERATIVOS MÍNIMOS DE SEGURIDAD PARA INSTRUMENTOS ELECTRÓNICOS DE PAGO DEL BANCO CENTRAL DE BOLIVIA

Los requisitos mínimos de estudio son las emitidas del Banco Central de Bolivia.

Requerimientos Operativos Mínimos de Seguridad para canales electrónicos de pago (banca electrónica y banca móvil)

Las entidades deben implementar medidas de seguridad para sus aplicaciones web y móviles, en función de su análisis y evaluación de riesgos en seguridad de la información, así como asumir medidas de mitigación de riesgos.

Las entidades deben proporcionar al cliente una contraseña para autenticarse al servicio, siendo su cambio obligatorio después del primer inicio de sesión y contar con mecanismos para recordarle su cambio al menos cada noventa (90) días.

Las entidades deben garantizar que sus aplicaciones web y móviles no almacenen información sensible y/o confidencial en HTML campos ocultos, cookies o cualquier otra forma de almacenamiento del lado del cliente que pueda comprometer su confidencialidad o la integridad de los datos.

Las aplicaciones web y móviles no deben exponer los datos del usuario en el inicio de sesión.

El restablecimiento de las sesiones en las aplicaciones web o móviles, después de interrupciones o de un periodo de inactividad, debe requerir una nueva autenticación del usuario. Toda sesión debe ser finalizada automáticamente después de cinco (5) minutos de inactividad como máximo.

Se debe implementar controles de seguridad, seguimiento y notificación de acceso de dispositivos electrónicos a aplicaciones web y móviles.

Se debe implementar mecanismos de registro/vinculación de dispositivos para acceso a servicios electrónicos, detección de redes no seguras y monitoreo de transacciones sospechosas.

Implementar mecanismos no presenciales para la actualización de información personal, la modificación de funcionalidades habilitadas, confirmación de cambios

y actualizaciones en canales electrónicos con el uso de firma digital sin costo adicional para el cliente.

Los mensajes de comunicación que remitan los emisores a través de correo electrónico y/o SMS no deben ser genéricos y deben especificar la operación a ser autorizada, considerando, según corresponda, el código de confirmación, monto, entidad financiera destino, cuenta del beneficiario, fecha y hora de la operación.

Requerimientos Operativos Mínimos de Seguridad para Billetera Móvil

1. El emisor debe vincular al número de cuenta de billetera móvil, el nombre completo del titular, documento de identidad y el número de su línea de telefonía móvil, siempre y cuando previamente se efectúe la verificación positiva de la identidad del titular de la billetera móvil. Asimismo, debe mantener el registro de las operaciones procesadas por un periodo de al menos diez (10) años.

2. Las órdenes de pago deben ser procesadas a través de medios que garanticen el cumplimiento de las siguientes características de seguridad:

a) Autenticidad. Contar con mecanismos que permitan verificar la identidad del titular del instrumento electrónico de pago en cada transacción.

b) Integridad. Estar protegidos contra alteraciones originadas por contingencias tecnológicas o acciones intencionales o accidentales durante su procesamiento, transporte y almacenamiento.

c) Confidencialidad. Contar con mecanismos de cifrado estándar que eviten la difusión o divulgación no autorizada de la información contenida en la operación durante toda la transacción, que pueda ser utilizada para materializar eventos de fraude.

d) No repudio. Garantizar que ninguna de las partes implicadas en la transacción pueda negar su participación en la misma.

e) Disponibilidad. El sistema de procesamiento de transacciones de billetera móvil debe estar disponible para los clientes según las condiciones publicitadas, informadas o pactadas contractualmente con los consumidores financieros.

3. El emisor debe proporcionar al usuario una contraseña para autenticarse al servicio, la cual debe ser cambiada después del primer inicio de sesión y contar con mecanismos para recordarle su cambio al menos cada noventa (90) días. En ningún momento esta clave deberá almacenarse en la billetera móvil.

4. Los emisores deben implementar mecanismos de autenticación robusta para sus usuarios en los siguientes procesos de autorización:

a) Procesamiento de las órdenes de pago.

b) Registro y modificación de los datos de beneficiarios, así como otra información sensible y confidencial cuya modificación podría facilitar la comisión de delitos o fraudes.

c) Definición y modificación de límites transaccionales.

d) Otras inherentes al procesamiento de órdenes de pago.

Al menos uno de los factores que se aplique no debe ser reutilizable, ni replicable, ni ser susceptible de ser robado vía internet. Cuando se utilice una contraseña de un solo uso, la vigencia de ésta no deberá ser mayor a dos (2) minutos. Únicamente para el inicio de sesión se podrá utilizar la autenticación de un solo factor, en función del análisis y evaluación de riesgos en seguridad de la información que efectúe la entidad financiera o ESP.

Tras el análisis comparativo con la 27032 y los requerimientos operativos mínimos de seguridad para instrumentos electrónicos de pago del Banco Central de Bolivia.

BCB	27032	EXISTE
1. Las entidades deben implementar medidas de seguridad para sus aplicaciones web y móviles, en función de su análisis y evaluación de riesgos en seguridad de la información, así como asumir medidas de mitigación de riesgos.	Según numeral 12 Controles a nivel de aplicación y protección a nivel de servidor	Aplica
2. Las entidades deben proporcionar al cliente una contraseña para autenticarse al servicio, siendo su cambio obligatorio después del primer inicio de sesión y contar con mecanismos para recordarle su cambio al menos cada noventa (90) días.	Según numeral 12 Controles a nivel de aplicación inciso f	Aplica
3. Las entidades deben garantizar que sus aplicaciones web y móviles no almacenen información sensible y/o confidencial en HTML campos ocultos, cookies o cualquier otra forma de almacenamiento del lado del cliente que pueda comprometer su confidencialidad o la integridad de los datos.	Acorde al numeral 12.2 Controles a nivel a nivel de aplicación inciso d	Aplica
4. Las aplicaciones web y móviles no deben exponer los datos del usuario en el inicio de sesión.	Acorde al numeral 12.2 Controles a nivel a nivel de aplicación inciso b	Aplica
5. El restablecimiento de las sesiones en las aplicaciones web o móviles, después de interrupciones o de un periodo de inactividad, debe requerir una nueva autenticación del usuario. Toda sesión debe ser finalizada automáticamente después de cinco (5) minutos de inactividad como máximo.	Acorde al numeral 12.2 Controles a nivel a nivel de aplicación inciso c	Aplica
6. Se debe implementar controles de seguridad, seguimiento y notificación de acceso de dispositivos electrónicos a aplicaciones web y móviles.	Acorde al numeral 12.2 Controles a nivel a nivel de aplicación inciso a	Aplica
7. Se debe implementar mecanismos de registro/vinculación de dispositivos para acceso a servicios electrónicos, detección de redes no seguras y monitoreo de transacciones sospechosas.	Según numeral 12 Controles a nivel de aplicación inciso f	Aplica

Si bien para para los canales electrónicos de pago de banca electrónica y banca móvil no menciona, los controles de ciberseguridad a nivel de servidores para prevenir los accesos no autorizados y contenido malicioso.

BCB	27032	EXISTE
1. El emisor debe vincular al número de cuenta de billetera móvil, el nombre completo del titular, documento de identidad y el número de su línea de telefonía móvil, siempre y cuando previamente se efectúe la verificación positiva de la identidad del titular de la billetera móvil. Asimismo, debe mantener el registro de las operaciones procesadas por un periodo de al menos diez (10) años.	Acorde al numeral 11 Directrices de las partes interesadas, orientada a los consumidores	Aplica
2. Las órdenes de pago deben ser procesadas a través de medios que garanticen el cumplimiento de las siguientes características de seguridad: **a) Autenticidad**. Contar con mecanismos que permitan verificar la identidad del titular del instrumento electrónico de pago en cada transacción. **b) Integridad.** Estar protegidos contra alteraciones originadas por contingencias te **c) Confidencialidad.** Contar con mecanismos de cifrado estándar que eviten la difusión o divulgación no autorizada de fraude. **d) No repudio**. Garantizar que ninguna de las partes implicadas en la transacción pueda negar su participación en la misma. **e) Disponibilidad**. El sistema de procesamiento de transacciones de billetera móvil debe estar disponible para los clientes	Acorde al numeral 11.4.4 Orientación de seguridad, orientada a los consumidores	Aplica
3. El emisor debe proporcionar al usuario una contraseña para autenticarse al servicio, la cual debe ser cambiada después del primer inicio de sesión y contar con mecanismos para recordarle su cambio al menos cada noventa (90) días. En ningún momento esta clave deberá almacenarse en la billetera móvil.	Acorde al numeral 11.4.4 Orientación de seguridad, orientada a los consumidores	Aplica

4. Los emisores deben implementar mecanismos de autenticación robusta para sus usuarios en los siguientes procesos de autorización: a) Procesamiento de las órdenes de pago. b) Registro y modificación de los datos de beneficiarios, así como otra información sensible y confidencial cuya modificación podría facilitar la comisión de delitos o fraudes. c) Definición y modificación de límites transaccionales. d) Otras inherentes al procesamiento de órdenes de pago.		

Conclusiones

Tras la verificación de la norma ISO/IEC 27032 y la comparación con los REQUERIMIENTOS OPERATIVOS MÍNIMOS DE SEGURIDAD PARA INSTRUMENTOS ELECTRÓNICOS DE PAGOS, no se encuentran alineados a controles para la protección de servidores, con el propósito para la configuración de la seguridad y la ejecución de control de software para llevar a cabo las evaluaciones de vulnerabilidades regulares, por otro lado no se cuenta con controles para los usuarios finales, se recomienda que las entidades de Intermediación financiera pueda implementar políticas y procedimientos para actualización de los servidores, controles y monitoreo de usuarios finales, evaluación recurrentes a sus sistemas para la detección de vulnerabilidades y el análisis de activos en ciberseguridad.

Bibliografía

https://www.asfi.gob.bo/index.php/norm- serv-fina-norm/recopilacion-de-normas.html

https://servdmzw.asfi.gob.bo/circular/textos/L03T07.pdf

https://www.bcb.gob.bo/webdocs/sistema_p agos/CIEX_N_26_2022.PDF

https://www.isotools.org/2022/05/06/conocie ndo-la-iso-27032-para-ciberseguridad/

https://www.iso.org/home.html

Artículo Recibido: 10/03/2023

Artículo Aceptado: 12/05/2023

EL TELETRABAJO: ¿OPORTUNIDAD O AMENAZA? (TELECOMMUTING: ¿OPPORTUNITY OR THREAT?)

Autor:

Osamu Manuel Yokosaki Peñaranda 1

osamu.yokosaki@gmail.com

Resumen

El teletrabajo no es una opción emergente del escenario de la pandemia por COVID 19, aunque fueron las medidas de bioseguridad las que pusieron en evidencia la importancia de esta alternativa a la forma tradicional de contemplar el entorno laboral. Este artículo es un análisis comparativo entre los beneficios y contratiempos que se dan como consecuencia de adoptar el teletrabajo. Para ello se consideró a Google Academics, fuentes gubernamentales de varios países, la base de datos de Scielo y "Hootsuite-We Are Social". El resultado al que se pudo arribar expresa que el teletrabajo como alternativa se constituye en un aporte trascendental en el escenario de nuevas culturas laborales con alto desempeño y bajo consumo de recursos, empero, este debe ser llevado de forma sistemática, planificada y organizada en el entendido de que las actividades que son habituales para el normal desenvolvimiento de las entidades deben someterse a procesos de análisis y transformación, lo cual representa en sí misma una verdadera amenaza para la subsistencia de la organización.

Palabras clave

Alternativa, contratiempo, fuente laboral, planificación, sistemático, teletrabajo, TIC.

1 Ingeniero de Sistemas, especialista en tecnologías de Información, magister con mención en Ciencias, coordinador de la carrera de ingeniería de sistemas, universidad La Salle, especialista en educación a distancia. ORCID: **0000-0002-6670-4380**

Abstract

Telecommuting is not an emerging option based in the COVID 19 pandemic scenario, although it was the biosafety measures that highlighted the importance of this alternative to the traditional way of looking at working environments. This article is a comparative analysis between the benefits and setbacks that became as a result of adopting teleworking. Were considered for this purpose resources as Google Academics, government sources from several countries, the Scielo database and "Hootsuite-We Are Social". The reached result expresses that telecommuting as an alternative constitutes a transcendental contribution in the scenario of new work cultures with high performance and low resource consumption, however, this must be considered as systematically, planned and organized in the understanding that the activities that are habitual for the normal development of the entities must undergo processes of analysis and transformation, which in itself represents a real threat to the survival of the organization.

Key words

Alternative, employment source, planning, systematic, telecommuting, threats, ICT.

Introducción

La evolución es un concepto aplicable a diversos ámbitos y acompañó al ser humano desde sus inicios, si trasladamos estos cambios al trabajo podremos asegurar que este también ha pasado por procesos evolutivos, pues, el ser humano pasó de realizar tareas manuales vinculadas exclusivamente a la supervivencia y que posteriormente superó esta premisa inicial y ha aportado con nuevos conceptos, incluida la comodidad, y es a través de estos cambios que llegamos a la actualidad.

Es así que los cambios que se realizaron según el tipo de actividad también fueron llevados al ambiente en el que se desarrollaron, desde labrar la tierra, la caza, pesca, recolección de frutos entre otros, hasta el día de hoy, en el que la diversidad de tareas hacen que el trabajo para un grupo importante de personas se lleve a cabo en ambientes que conocemos como oficinas, pues bien, un elemento que se considera como fundamental en este sentido es que las oficinas como tal ofrecen, al menos en teoría, las condiciones para el desempeño de las actividades propias del sentido de la organización.

Sin embargo, de un tiempo a esta parte, existen organizaciones que han encontrado en la forma del teletrabajo una alternativa que desplaza algunas o la mayoría las tareas que antes se llevaban a cabo en las oficinas para ser realizada en el los domicilios particulares, y como sucede habitualmente, los cambios conllevan factores que pueden ser considerados como positivos y otros que simplemente no lo son, de hecho, es posible que los aspectos negativos que rodean este nuevo esquema de trabajo se relacionen al impacto en las costumbres bajo las cuales se establecen los lineamientos, normativas y reglamentos que son la consecuencia natural de la estructura mental de empleadores y colaboradores en este ámbito y que a su vez se constituyen en el criterio de normalidad.

El problema radica en la resistencia al cambio la cual se vincula inexpugnablemente al concepto de "zona de confort", que a su vez se ha de vincular a la siguiente paradoja: "La racionalidad individual conduce a la irracionalidad colectiva que se traduce en resultados indeseados, las organizaciones con sus proyectos se aíslan, el conocimiento permanece silenciado y es guardado bajo siete llaves o simplemente se repite el enfoque que los proyectos traen sin que el conocimiento de las familias tenga valor y sea referente de políticas." (Mendoza V., 2011) en la que se plantea que la opción adoptada en base a la certeza inherente de los procedimientos conocidos lleva resultados desconocidos en función a la transformación de los escenarios.

Es entonces el planteamiento ofrecido el que indica que el teletrabajo en si mismo ha de ofrecer alternativas al menos viables para dar continuidad a las operaciones de organizaciones, es posible que el impacto inicial sea lo suficientemente fuerte como para desestabilizar al conjunto de involucrados, empero, una vez superada la transición, los beneficios han de ser sustanciales (Camacho, 2018).

Por otra parte, el teletrabajo se expresa bajo los términos nativos de una negociación laboral y por ello es que se debe considerar que existirán intereses que deben ser considerados, y si bien, es una alternativa viable e incluso factible, esta da pié a malinterpretaciones que han de ser perjuciales para el empleador y el empleado, esto a raíz de que las caracteristicas de las instalaciones físicas de la organización han de ofrecer las condiciones para cumplir con las metas de la organización y por otra parte, dispondra de las facilidades en el acceso a recursos que se espera para el efecto. Siendo que el control existente por parte del empleador permitirá contar con métricas mas precisas acerca de las actividades realizadas.

Sería inapropiado el considerar al teletrabajo como la evolución del trabajo y el reemplazo natural de la presencialidad en el ámbito laboral, pues esto representaría el cambio de paradigma actual y por tanto una afirmación poco acertada de que las oficinas serán obsoletas, empero se debe considerar escenarios emergentes y característicos de la sociedad en la actualidad, lo que en suma ha de ser objeto de análisis en el presente documento.

El desafío del presente documento de investigación radica en la posibilidad de ofrecer lineamientos que permitan equilibrar ambos escenarios en virtud de obtener provecho de las propiedades que ostentan las dos opciones, esto bajo la premisa de que no es posible generali-

zar las oportunidades y amenazas.

Problema: En este sentido es que es posible inferir que el teletrabajo en sí mismo no puede ser contemplado como un reemplazo completo del trabajo en oficinas pues existen actividades que requieren de la interacción de las personas de la forma tradicional, empero, la contraparte emergente del teletrabajo brinda soluciones eficientes para tareas que claramente pueden ser ejecutadas a distancia. En cuyo caso, son beneficiosas para la organización.

Objetivo: Brindar un análisis comparativo de las características de ambos esquemas laborales para optar por una combinación entre el trabajo presencial y el teletrabajo que beneficie a la organización y a la sociedad en su conjunto.

Referentes conceptuales

El concepto fundamental bajo el cual se trazan los esquemas una relación laboral ha sido definida por la OIT de la siguiente manera: "El Tesauro de la Organización Internacional del Trabajo (OIT) define al trabajo como el conjunto de actividades humanas, remuneradas o no, que producen bienes o servicios en una economía, o que satisfacen las necesidades de una comunidad o proveen los medios de sustento necesarios para los individuos." Esto sin especificar el lugar en el que se han de realizar estas actividades, es por ello que se añadieron nuevas especificaciones, como la que hace mención al teletrabajo, y para ello la OIT indica que han de establecer ciertos criterios que posteriormente se dan también desde la misma institución de la siguiente manera "El teletrabajo se define como el uso de tecnologías de la información y las comunicaciones –como teléfonos inteligentes, tabletas, computadoras portátiles y de escritorio– para trabajar fuera de las instalaciones del empleador (Eurofound y OIT, 2019). En otras palabras, el teletrabajo conlleva un trabajo realizado con la ayuda de las TIC, fuera de las instalaciones del empleador."

Es bajo esta premisa que el trabajo en sí mismo no ha de cambiar sustancialmente en relación a la finalidad del mismo, por cuanto las tareas y responsabilidades no han de perder sus propiedades, la diferencia radica en el uso y posible dependencia hacia las TIC's.

Métodos y materiales

Para la elaboración del presente artículo de investigación se contemplaron criterios tanto cualitativos como cuantitativos, esto a raíz de que se contrastaron entrevistas a colaboradores que se hallan o al menos que realizaron teletrabajo durante el periodo de cuarentena por la pandemia de COVID-19, por otra parte, se consultaron indicadores estadísticos que expresan la creciente participación de las TIC's en el ámbito laboral. Se consideró adicionalmente la importancia de documentos técnicos que incluyen legislación internacional e indicadores de rendimiento que sirvieron como referencia para la investigación.

Fuente Primaria

Las fuente primaria se expresa en libros técnicos destinados a la impementación de la modalidad de teletrabajo en Argentina y Colombia, asi como la legislación que integra al sector público y privado, y en ambos casos se estudio a normativa, empleador y empledo. Lo que ha generado un apropiado nivel de abstracción y por tanto la objetividad del estudio.

El criterio de uso de las fuentes de investigación aborda la incidencia ya sea positiva o negativa del teletrabajo considerando para el efecto la productividad, supervisión, control, seguimiento, flexibilidad, brecha digital y resistencia al cambio. Los cuales son elementos que participan e incluso se contrastan para encontrar un equilibrio que optimice el rendimiento de la organización aplicando de manera planificada la modalidad de trabajo a distancia.

La comprensión de los indicadores o criterios involucrados en la generación de lineamientos y normativa que respalda la aplicación del teletrabajo de forma personalizada según la organización se traduce en la valoración y determinación de la importancia de cada indicador a ser considerado para optar por esta alternativa. El componente cualitativo se llevó a cabo a partir de entrevistas con dos empleados del sector privado en los que el rendimiento desde la perspectiva profesional se contrasto con la vida personal y la existencia de beneficios asociados al aprovechamiento flexible del tiempo y una administración basada en la consecución de objetivos puntuales con reducción de actividades distractivas propias de la oficina. Por otra parte, se entrevisto a tres empleados de cargo ejecutivo y estrategico que contrastaron factores de control y seguimiento con factores asociados al aprovechamiento de la inversión institucional.

Para el análisis cuantitativo se contemplaron las estadísticas emergentes del periodo de cuarentena rígida y fueron contrastadas con los indicadores de uso de TIC, ya sea dispositivos celulares y computadoras.

Fuentes Secundarias

En este sentido, las fuentes secundarias permitieron el uso de las definiciones y por tanto se constituyen en la fundamentación teórica, con lo cual fue posible establecer los factores relevantes que dan la pauta para la agrupación de criterios, y de esta manera es posible inferir el equilibrio. Para ello se utilizarón guias de implementación de teletrabajo, estadísticas de uso de tecnologías de comunicación, así también libros que abordan la temática.

Desarrollo

El teletrabajo plantea transformación, y esta ha de ser de forma natural un desafío para la organización, se ha podido establecer que el caos provocado por la violenta transición del trabajo en las instalaciones físicas como se llevaron a cabo en el periodo previo a la pandemia, y posteriormente estos valores cambiaron radicalmente con un crecimiento descontrolado (Peiró, 2022). El cambio que se ha producido a partir de una transición inesperada carente de planificación a provocado que ciertos aspectos vinculados al liderazgo, control y seguimiento se vieron afectados por cuanto la ausencia de capacitación se han

evidenciado de forma dramática, esto a raíz de que las organizaciones no cumplieron estos procesos de transición bajo una evolución controlada y principalmente planificada. (Timothy, 2013).

En el contexto del crecimiento en el uso de tecnologías se puede apreciar que a nivel mundial el número de personas que utilizan dispositivos electrónicos de comunicación alcanza los 5.2 billones de personas y 4.66 billones cuentan con acceso a internet, todo ello con un crecimiento estimado de 1 % para la posesión de dispositivos y 1.8% para el acceso a internet (Social, 2021). Ahora bien, la tendencia de la aplicación de la modalidad de teletrabajo ha de ser negativa en los próximos años en la medida de que la pandemia y las respectivas restricciones de circulación vayan disminuyendo.

Indicadores de Productividad

La productividad es un criterio dentro del ámbito laboral que ha de permitir medir el rendimiento que un colaborador posee en virtud al costo de pero este debe adecuarse apropiadamente al tipo de trabajo por cuanto no en todos los casos genera un resultado al menos eficaz, en un estudio realizado en Estados Unidos que se llevó a cabo en el contexto del teletrabajo se entrevistaron a 273 colaboradores que desempeñaron funciones bajo un esquema de trabajo remoto, se pudo eviodenciar que mas allá de las capacidades de los empleados, las tareas en si misma no se podían efectuar sin la presencia física de la persona, por el otro lado, el máximo rendimiento se obtuvo en aquellos que desempeñaban un grupo de tareas en específico (Marja Coenen, 2014). Es entonces que si se desea aplicar el modelo de teletrabajo en organizaciones que tienen un esquema de trabajo basado en actividades que requieren de mano de obra, se restringe la posibilidad de su implementación.

La productividad ha de contemplar diversas perspectivas, considerando para ello el entorno en el cual se desarrollan las actividades, los recursos que estas han de utilizar y de acuerdo a estos valores considerar una valoración en función a su participación para los fines comprometidos.

Indicadores de Rendimiento

Si bien es posible asociar el rendimiento con la productividad, son criterios complementarios pero diferentes pues abordan distintos elementos en función a los resultados que es posible alcanzar mediante la combinación de ambos, en este sentido es posible considerar los indicadores que corresponden a cada uno de los los conceptos de tal manera que se trsanversalicen sin generar conflictos de valoración.

El rendimiento se mide considerando los diferentes factores que inciden en el éxito de la organización, esto enlazando elementos conceptuales como la estructura, estrategias, operaciones, recursos, productividad entre otros, es por ello que se analizarán los indicadores que así se requiera para determinar la eficiencia de la aplicación de medidas según sea el caso. En este sentido es posible coincidir que el teletrabajo ha de incidir en el rendimiento de la organización y por ello tambien deberá ser considerado como un factor influyente.

Clima Organizacional

En toda organización es importante el contemplar que la convivencia de sus actores ha de ser determinante en el progreso de cada una de las actividades razón por la cual se ha de considerar que el conocimiento en este sentido hace que el conjunto se vea beneficiado bajo la premisa de que "La investigación sobre el clima organizacional, se constituye en un proceso necesario para tomar decisiones ante problemas que puedan limitar el desempeño de una organización y de manera especial, en aquellas que deben asumir de forma exitosa, sensibles y complejas tareas "(Rodríguez Lorenzo & Herrera Barrueta, 2016)

Lo antes mencionado encierra un conjunto de factores que han de incidir en la determinación del espacio en el que se desarrollan las actividades, ello enmarcado en la interacción preexistente que ha de ser trasladada a un escenario nuevo, lo que ha de incidir en el comportamiento de los actores que han de relacionarse contemplando los mismos objetivos con la intervención de un agente modificador del comportamiento de los participantes. Ello llevado a un escenario que deja de lado factores que se consideraban anteriormente que son reemplazados, que, aunque pueden generar resultados similares ellos se hallan bajo diferentes causas, todas ellas llevadas a una valoración sistematizada podrán determinar decisiones acertadas.

Resultados y Discusión

La conjunción de criterios abordados contemplan elementos coincidentes con el presente, ellos abordan la temática desde diversas perspectivas, pues existe un factor que se considera en los documentos citados y es que el teletrabajo como tal ofrece oportunidades, pero contempla amenazas.

Beneficios

Uno de los principales beneficios del teletrabajo está vinculado a la redistribución de tiempo con el que los colaboradores cuentan para su asignación a actividades profesionales, las que se asignan a la vida personal, haciendo que aspectos trascendentales como el compartir más tiempo con la familia sean posibles, pues se reemplazan tiempos de traslado o alimentación a un ambiente familiar, lo que beneficia a la sociedad en su conjunto.

El teletrabajo ha de beneficiar a la organización que adopta este modelo de trabajo pues transfiere costos

operativos al colaborador (Marja Coenen, 2014), siendo que aspectos como el traslado, la alimentación, aseo, bioseguridad y costos indirectos se reducen sustancialmente al no contar con la presencia de personas en las instalaciones, promoviendo según sea el caso la reducción en gastos como alquileres o servicios. Pues, ante la reducción de personal asistente es posible migrar a espacios más reducidos, incrementando el rendimiento por concepto de costo por espacio utilizado.

Un factor que se ha evidenciado gracias a la incursión del teletrabajo radica en la posibilidad de incrementar la movilidad del personal de las organizaciones (LIBRO BLANCO EL ABC DEL TELETRABAJO EN COLOMBIA, 2012), pues la ubicación física de los colaboradores no es relevante al momento de medir su productividad, desplazando la relación horas/hombre hacia el cumplimiento de metas u objetivos con plazos flexibles que dan la oportunidad de una administración del tiempo por parte colaborador y una reducción significativa en el control de asistencia, mismo que se ha demostrado no siempre puede medir de forma acertada la productividad.

Amenazas

La ausencia de fronteras físicas propias de las instalaciones del edificio donde se halla la organización genera la perdida de límites vinculados a la vida personal de sus integrantes como lo mencionan Alberto Pinto y Gonzalo Muñoz cuando afirman que "es crítico tener conciencia de que el teletrabajo expone a los trabajadores a la inmediatez de las redes y contactos electrónicos, como WhatsApp, e-mails, y teleconferencias. La experiencia subjetiva de ansiedad y el sentirse presionado a responder a demandas laborales excesivas que aparecen en el contexto del teletrabajo se conoce como telepresión." Donde es posible reconocer escenarios que se han convertido en habituales, extendiendo las horas de trabajo.

Por otra parte, el control y supervisión de actividades se reduce significativamente en el marco de la capacidad de interconexión por dispositivos móviles, esto hace que la dedicación requerida al cumplimiento de las tareas encomendadas no sea mesurables y por tanto el crecimiento en la incertidumbre sea gravitante. Esto sin duda es una amenaza a la organización afectando el rendimiento y productividad de sus colaboradores.

Una amenaza emergente del contexto de teletrabajo se basa en la percepción de pertenencia de los empleados, esto porque la imagen, clima y cultura organizacional se difumina en interacciones programadas para tareas demasiado específicas como la coordinación, seguimiento y evaluación. Dejando de lado la interacción casual que se asocia a las charlas casuales, las cuales son una fuente que provee de ideas y proyectos que de otra manera son muy poco probables.

Un factor que es relevante pero que no ha sido abordado en esta ocasión se vincula al aprovechamiento de la inversión realizada por las organizaciones para la acogida de sus colaboradores en sus instalaciones, pues esta responde a criterios asociados a la productividad de las personas en función a la inversión en equipamiento, haciendo que en ciertos casos requiera de inversión adicional que reduce el rendimiento de la organización.

Conclusiones

El teletrabajo como una forma de interacción en el ámbito laboral es, en sí misma, una alternativa que se ha llevado a cabo desde mucho antes de las restricciones de la pandemia por COVID-19, la incursión de las TIC's ha generado una invasión a la privacidad de los colaboradores por desaparición de las fronteras propias de las instalaciones físicas de las organizaciones, las cuales difuminaron la frontera entre lo personal y lo laboral. Esto sufrió una dramática transformación desde las restricciones de la pandemia, generando un nuevo escenario en el que la presencialidad fue reemplazada por el agente difuminador que son las TIC's.

El dramatismo de la transición obligada de la presencialidad a la virtualidad redujo la capacidad de control de las organizaciones bajo los esquemas tradicionales de interacción, afectando la gran mayoría de los procesos preestablecidos, generando un caos previsible, esto vinculado a que elementos planificados de forma adecuada y con rendimientos probados como eficientes quedaron inoperantes en vista de un factor primordial, la asistencia obligatoria del personal de la organización. Llevando a escenarios de elevada incertidumbre acerca de la forma en la que las actividades se llevarían a cabo, esto genera de forma natural el rechazo, que sumado a criterios como "Zona de Confort" o "Brecha Digital" han potenciado la resistencia a la adopción del modelo.

Ahora bien, ya que se ha podido evidenciar que el teletrabajo genera un escenario nuevo y desafiante, es posible prevenir y de hecho aprovechar las virtudes detectadas de la modalidad en un nuevo paradigma laboral, el que podrá diferenciar de forma apropiada el perfil de los colaboradores de acuerdo a las características de las funciones encomendadas, delimitando eficientemente el ambiente en el que los empleados pueden realizar las actividades, promoviendo nuevos escenarios laborales con indicadores mejorados de rendimiento que podrán, según corresponda, evolucionar hacia la consecución de metas en lugar de consumo de tiempo.

Finalmente, no es posible afirmar que el teletrabajo reemplazara por completo a la presencialidad pues existen actividades que requieren de la asistencia del empleado, de otra manera no podrá operar la organización, empero, existen actividades que se ven altamente beneficiadas en función a la reducción de interacción de la persona con su medio, y por último, existe un grupo importante que reúne a quienes están sujetos a un análisis particular que equilibre ambas modalidades, generando escenarios híbridos que serán el resultado de análisis y planificación que produzca resultados eficientes para la organización, enriquecedores para el empleado e incluso, beneficiosos para el medio ambiente.

Referencias

Sánchez-Toledo Ledesma, Agustín María. (2021). Efectos del teletrabajo sobre el bienestar de los trabajadores. Revista de la Asociación Española de Especialistas en Medicina del Trabajo, 30(2), 234-254. Epub 18 de octubre de 2021. Recuperado en 27 de marzo de 2022, de http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1132-62552021000200234&lng=es&tlng=es.

Mora Eguiarte, Damian. (2017). Horarios flexibles como estrategia para mejorar la productividad y reducir la rotación. Academo (Asunción), 4(2), 55-62. https://dx.doi.org/10.30545/academo.2017.jul-dic.8

Barreto-Osma, Doris Amparo, Rojas-Castro, Slendy Xiomara, & Uribe-Barrera, Daniela Alejandra. (2021). Fatiga laboral en personas que realizaron trabajo en casa en tiempos de confinamiento por COVID-19. Universidad y Salud, 23(3, Suppl. 1), 309-319. Epub December 03, 2021.https://doi.org/10.22267/rus.212303.245

Undurraga, Rosario, Simbürger, Elisabeth, & Mora, Claudia. (2021). Desborde y desazón versus flexibilidad y concentración: Teletrabajo académico y género en tiempos de pandemia. Polis (Santiago), 20(59), 12-38. https://dx.doi.org/10.32735/s0718-6568/2021-n59-1594

Miglioretti, Massimo, Gragnano, Andrea, Margheritti, Simona, & Picco, Eleonora. (2021). Not all telework is valuable. Revista de Psicología del Trabajo y de las Organizaciones, 37(1), 11-19. Epub 29 de marzo de 2021. https://dx.doi.org/10.5093/jwop2021a6

Sánchez-Toledo Ledesma, Agustín María. (2021). Efectos del teletrabajo sobre el bienestar de los trabajadores. Revista de la Asociación Española de Especialistas en Medicina del Trabajo, 30(2), 234-254. Epub 18 de octubre de 2021. Recuperado en 27 de marzo de 2022, de http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1132-62552021000200234&lng=es&tlng=es.

Contreras, Orlando E., & Rozo Rojas, Ivanhoe. (2015). Teletrabajo y sostenibilidad empresarial. Una reflexión desde la gerencia del talento humano en Colombia. Suma de Negocios, 6(13), 74-83. https://doi.org/10.1016/j.sumneg.2015.08.006

Restrepo Pimienta, Jorge Luis, & Forero Contreras, Rafael. (2015). Usos y prácticas de las técnicas de información y de la comunicación TIC's en la enseñanza del derecho del trabajo. Justicia Juris, 11(1), 63-70. Retrieved March 26, 2022, from http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1692-85712015000100006&lng=en&tlng=es.

López, Nelson W., Pérez-Simon, M. Claudia, Nagham-Ngwessitcheu, Edwige G., & Vázquez-Ubago, María. (2014). Teletrabajo, un enfoque desde la perspectiva de la salud laboral. Medicina y Seguridad del Trabajo, 60(236), 587-599. https://dx.doi.org/10.4321/S0465-546X2014000300009

Bonilla Prieto, Liliana Andrea, Plaza Rocha, Diana Carolina, De Cerquera, Gladys Soacha, & Riaño-Casallas, Martha Isabel. (2014). Teletrabajo y su Relación con la Seguridad y Salud en el Trabajo. Ciencia & trabajo, 16(49), 38-42. https://dx.doi.org/10.4067/S0718-24492014000100007

Camacho Peláez, Rafael Hernando, & Higuita López, Daimer. (2013). Teletrabajo con calidad de vida laboral y productividad. Una aproximación a un modelo en una empresa del sector energético. Pensamiento & Gestión, (35), 87-118. Retrieved March 26, 2022, from http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1657-62762013000200005&lng=en&tlng=es.

Caamaño Rojo, Eduardo. (2010). El teletrabajo como una alternativa para promover y facilitar la conciliación de responsabilidades laborales y familiares. Revista de derecho (Valparaíso), (35), 79-105. https://dx.doi.org/10.4067/S0718-68512010000200003

Lenguita, Paula. (2010). Las relaciones de teletrabajo: entre la protección y la reforma. Argumentos (México, D.F.), 23(64), 245-263. Recuperado en 27 de marzo de 2022, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-57952010000300011&lng=es&tlng=es.

Rodríguez Mejía, Marcela. (2007). El teletrabajo en el mundo y Colombia. Gaceta Laboral , 13(1), 29-42. Recuperado en 27 de marzo de 2022, de http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1315-85972007000100002&lng=es&tlng=es.

Prieto-Díez, Francisco, Postigo, Álvaro, Cuesta, Marcelino, & Muñiz, José. (2021). Compromiso laboral: nueva escala para su medición. Revista Latinoamericana de Psicología, 53, 133-142. Epub August 02, 2021.https://doi.org/710.14349/rlp.2021.v53.15

Barón Chacón, N. A. (11 de 04 de 2021). Factores que influyen a nivel individual y grupal en el comportamiento de los colaboradores frente a los cambios en el proceso organizacional de la empresa Gaedpsi. Factores que influyen a nivel individual y grupal en el comportamiento de los colaboradores frente a los cambios en el proceso organizacional de la empresa Gaedpsi. Bogotá D.C., Bogotá D.C., Colombia: Sistema Nacional de Bibliotecas SISNAB. Obtenido de http://hdl.handle.net/10823/2606

Camacho, C. M. (10 de Marzo de 2018). Teletrabajo: Una Revisión Teórica sobre sus Ventajas y Desventajas. INVESTIGATIO, 41-54.

Fuller James, F. A. (2008). Inlfuencia del Plomo en el poder de distribución del sistema de protección. IEEE Trans. Power Delivery, 17,34.

LIBRO BLANCO EL ABC DEL TELETRABAJO EN COLOMBIA. (2012). Bogota: Colombia Digital. Obtenido de https://www.mintrabajo.gov.co/teletrabajo

Marja Coenen, R. A. (2014). Workplace flexibility and new product development performance: The role of telework and flexible work schedules. European Management Journal, 32(4), 564-576. doi:https://doi.org/10.1016/j.emj.2013.12.003.

Mendoza V., R. (2011). El dilema de la acción colectiva y la trampa de la "zona de confort". Promotora del desarrollo en Nicaragua.

Peiró, J. (2020). EL IMPULSO AL TELETRABAJO DURANTE EL COVID-19 Y LOS RETOS QUE PLANTEA. IvieExpress.

Robinsson, M. (2004). Antenas de Transmisión. Los Angeles: Mc Graw Hill.

Rodríguez Lorenzo, M., & Herrera Barrueta, M. (2016). El clima organizacional, un aspecto importante a tener en cuenta en los trabajadores del grupo de control de vectores. Revista Cubana de Salud Pública, 1-3. Obtenido de https://www.redalyc.org/articulo.oa?id=21447534012

Social, H. -W. (2021). Digital Overview 2021 . Hootsuite.

Timothy, R. (2013). Telecommuting and Leadership Style. Public Personnel Management, 42, 438-451.

Artículo Recibido: 27/04/2023

Artículo Aceptado: 19/05/2023

PROPUESTA DE BUENAS PRÁCTICAS PARA EL DESARROLLO SEGURO DE SOFTWARE CON DEVSECOPS Y SECURE SCRUM

DIPLOMADO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Autor:
Apolinar Linares Flores

Resumen

La ciberseguridad ha sido uno de los problemas principales en la informática, pero más aún en el proceso de desarrollo de software ya que con las nuevas tecnologías y/o lenguajes de programación van apareciendo nuevas vulnerabilidades en el ciclo de vida del software. El presente articulo de investigación aborda como tema principal plantear una propuesta de buenas prácticas para el desarrollo seguro de software con DevSecOps y secure Scrum, la combinación de DevSecOps y Secure Scrum como una solución para controlar y mejorar la seguridad del software. DevSecOps se enfoca a integrar la seguridad en todas las fases del ciclo de vida del software, mientras que Secure Scrum es una metodología de desarrollo de software seguro basada en Scrum. Al complementarlas, estas prácticas permiten a los equipos de desarrollo a construir software de manera más eficiente y segura, minimizando los riesgos y protegiendo sus activos.

Palabras Clave: DevSecOps, Secure Scrum, buenas prácticas, procesos de desarrollo de software

Abstract

Cybersecurity has been one of the main problems in computer science, but even more in the software development process because with new technologies and/or programming languages new vulnerabilities are appearing in the software life cycle. The main topic of this research article is to raise a proposal of best practices for secure software development with DevSecOps and Secure Scrum, the combination of DevSecOps and Secure Scrum as a solution to control and improve software security. DevSecOps focuses on integrating security into all phases of the software lifecycle, while Secure Scrum is a secure software development methodology based on Scrum. By complementing each other, these practices enable development teams to build software more efficiently and securely, minimizing risks and protecting their assets.

Keywords: DevSecOps, Secure Scrum, best practices, software development processes,

1. Introducción

El desarrollo de software ha evolucionado con el pasar del tiempo, los programadores o empresas dedicados al desarrollo de software se han visto en la necesidad de acelerar el proceso de construcción de cualquier sistema informático.

El surgimiento de las metodologías ágiles permite que se pueda desarrollar sistemas informáticos con mayor rapidez y eficacia, utilizar una metodología ágil permite al equipo de desarrollo trabajar de manera incremental e iterativa dejando en el pasado el proceso secuencial que se utilizaba.

El uso de una metodología ágil no es suficiente para la creación de software, es importante agregar un equipo de seguridad en todo el proceso y no solo al final. El agregar un equipo de seguridad en el proceso de desarrollo nos permite minimizar costos y poner en marcha el software sin problema. El presente articulo propone tener un conjunto de buenas prácticas para el desarrollo de software seguro, para asegurar que el software cumpla con los estándares de seguridad necesarios protegiendo la información confidencial y sensible de los usuarios. Estas practicas también pueden prevenir posibles vulnerabilidades y amenazas que podrían afectar el rendimiento y la disponibilidad del software. Al seguir las buenas prácticas de seguridad en en el proceso de construcción del software, el equipo de desarrollo puede mejorar la confianza y satisfacción de los usuarios y clientes, en materia de seguridad de la información.

2. Contenido

Para brindar un proceso de desarrollo de software seguro, se propone seguir Secure Scrum que es una metodología de desarrollo de software que combina los principios y valores de Scrum con los aspectos de seguridad de la información. Esta metodología involucra a todos los miembros del equipo en la identificación y mitigación de los riesgos de seguridad, y se integra con

otros procesos de seguridad de la información. Ademas, complementar con el enfoque DevSecOps que integra consideraciones de seguridad en todas las etapas del ciclo de vida del desarrollo de software. DevSecOps busca automatizar e incorporar prácticas de seguridad en el flujo de trabajo para acelerar el tiempo de entrega sin comprometer la seguridad.

Secure Scrum surge como variante de la metodología de desarrollo ágil Scrum, su principal tarea es identificar las vulnerabilidades y asegurarse que no sea rentable para un intruso explotar las secciones inseguras. Según Pohl & Holf, 2015 esta metodología consta de 4 etapas principales mismas que se integran con Scrum.

Figura 1 – Integración de Secure Scrum en Scrum Tradicional

Fuente: Elaboración Propia

Se puede observar la integración del scrum tradicional con los procesos de seguridad.

IDENTIFICACIÓN DE COMPONENTES

Esta etapa se encuentra en la sección del Product Backlog Inicial, en la planificación del sprint y refinamiento del product Backlog. En esta etapa el equipo de trabajo y el Product Owner asignan una puntuación a las historias de usuario en función a su valor perdido. Se organiza según el nivel de riesgo y se asocian las historias de usuario con "S-tags" que describen posibles riesgos encontrados.

IMPLEMENTACIÓN DE COMPONENTES

En el sprint se implementa un subconjunto de funcionalidades con los S-tag asociados. Cada historia se puede dividir en un conjunto de tareas, mismas que están asociadas a la funcionalidad que se les asigna al inicio del sprint.

VERIFICACIÓN DE COMPONENTES

La tarea principal en esta etapa es la realización de pruebas necesarias a las tareas realizadas de los S-tag. Se pueden utilizar herramientas o recursos externos. Por ejemplo consultores de seguridad que ayuden a mostrar y mejorar el conocimiento sobre seguridad al equipo de trabajo, ademas de ayudar a cubrir posibles vulnerabilidades.

DEFINICIÓN DE COMPONENTE REALIZADO

Se comprobará el cumplimiento de los criterios de calidad de las tareas que se definieron en el sprint. Una vez probados, se debe definir como tareas realizadas sin

perder la asociación a las S-tags.

DevSecOps es una metodología de desarrollo de software seguro, su principal tarea es la gestión de recursos, se enfoca en encontrar los problemas de seguridad desde el inicio y durante el ciclo de vida del software, y no al final del proceso de desarrollo. Según Raynaud, 2017 esta metodología "permite reducir costos y aumentar la velocidad de recuperación frente a un incidente de seguridad"

DevSecOps tiene como buenas practicas asociado a 3 conceptos: personas, procesos y tecnología.

PERSONAS

El factor humano es considerado como el punto más vulnerable en la seguridad de software, por lo tanto es necesario incluir personal de seguridad a la brevedad posible dentro del ciclo de vida del software. Se debe integrar un desarrollador de software que posee y aplica amplios conocimientos de seguridad dentro de un equipo de desarrollo (Security Champion).

PROCESOS

la metodología propone que los procesos estén integrados entre si para lograr un proceso de desarrollo más seguro.

- Integración de Procesos, la seguridad debe formar parte desde la toma de requerimientos para evitar añadir costos después de terminado el software.

- Arquitectura de seguridad, mismo que se basa en el conjunto de principios que tenga la organización o institución.

- Gestión de incidentes, se debe definir un plan de acción frente a incidentes de seguridad, mismo que sea consistente, repetible y medible.

- Equipos rojos y recompensas de Bug, se debe tener encargados de cazar amenazas para encontrar y planear soluciones, así brindar a los desarrolladores retroalimentación de seguridad. Plantear un plan de recompensas para que el equipo de desarrollo informe sobre vulnerabilidades o fallos del software.

- Inteligencia de Amenaza, se debe actualizar planes de acción automatizados de los planes ya existentes.

TECNOLOGÍAS

Para ejecutar correctamente los procesos de DevSecOps se tiene:

- Automatización y Gestión de la configuración.

- Seguridad como código.

- Auditorías y exploración a nivel de aplicación.

"El propósito y la intención de DevSecOps es crear sobre la mentalidad de que todo el mundo es responsable por la seguridad, con el objetivo de distribuir de manera segura las decisiones de seguridad rápidamente y escalar para aquellos que mantienen el nivel más alto de contexto, sin sacrificar la seguridad necesaria" (Shannon Lietz, coautora del "Manifiesto DevSecOps")

Analizando las características que presentan la metodología secure scrum y el enfoque DevSecOps se puede generar una guía de buenas practicas para el desarrollador o equipo de software que sea el encargado de crear un nuevo software para las pequeñas empresas. El objetivo principal será el de obtener un software seguro y de calidad a un costo aceptable, mismo que sea desarrollado en un corto tiempo.

Las buenas practicas que se plantea se basan en seguir la metodología Scrum combinando características del enfoque DevSecOps, por lo que se tendrá una etapa de planificación.

3. Resultados

Una vez que se ha revisado documentación sobre la metodología ágil y el enfoque de desarrollo seguro, en el presente articulo de investigación se plantea seguir un esquema como guía de buenas practicas en el desarrollo de software para pequeñas empresas, misma que se puede observar en la figura nro. 2.

Lo primero que se tiene que hacer antes de iniciar la construcción de un software para pequeñas empresas es armar un equipo de desarrollo donde se tenga incluido un Security Champion, luego iniciar con los pasos de la metodología ágil con el enfoque de desarrollo seguro, el siguiente paso es la planificación donde se elaborará el product backlog y el secure backlog para iniciar con la planificación y ejecución del sprint. Como se puede observar en la figura 2.

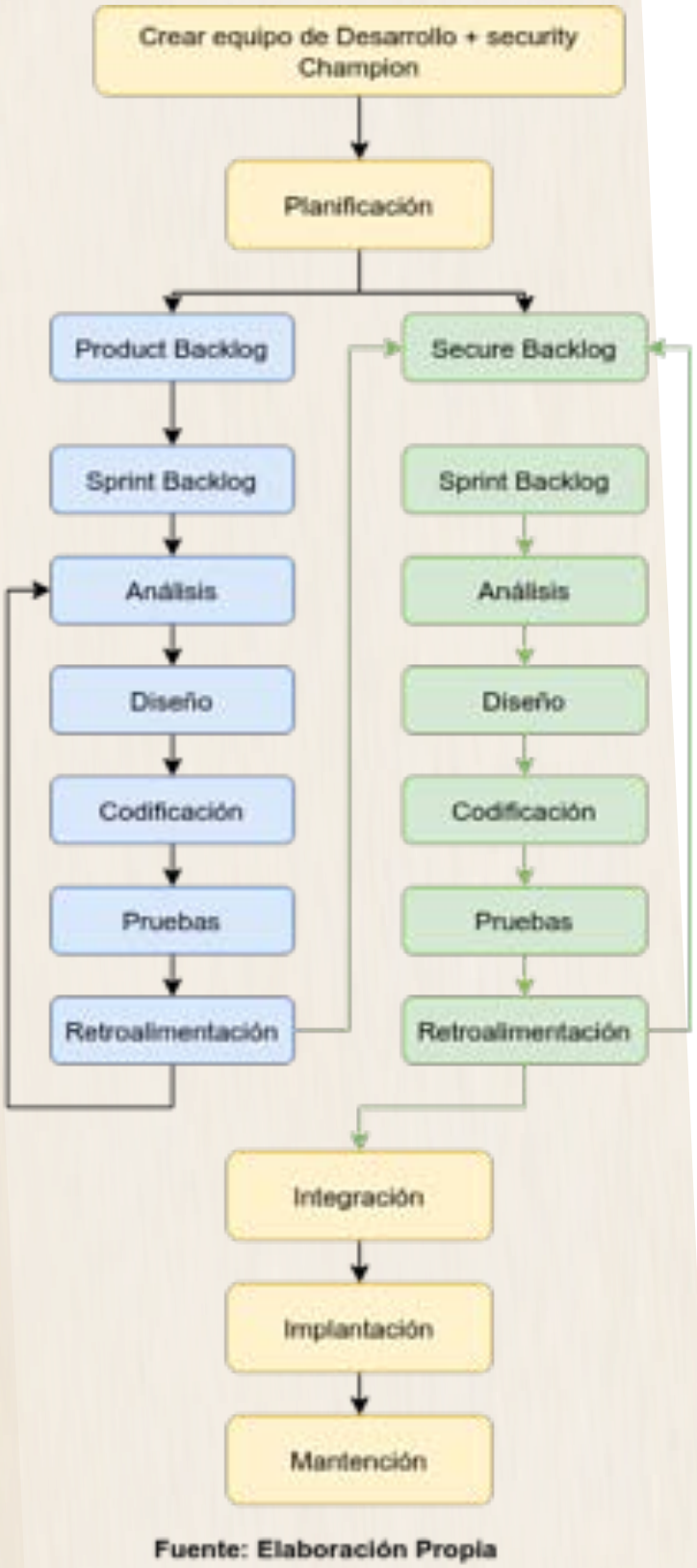


Figura 2 – Pasos a seguir para el desarrollado de Software Seguro

Una vez culminada la etapa de planificación se inicia el desarrollo o ejecución de los sprints, cada sprint del proyecto, considera un segundo sprint asociado al Secure Backlog, el primer sprint asociado al Product Backlog tendrá una duración estimada de 10 a 15 días, mientras que el segundo se dará solo 5 días (la duración del sprint dependerá de las políticas de la pequeña empresa y en coordinación con el equipo de desarrollo). Cada sprint tendrá las etapas de análisis, diseño, codificación, pruebas y retroalimentación. Donde el sprint del producto tiene la posibilidad de volver al análisis para mejorar el desarrollo del módulo, mientras que en el de seguridad no, por lo tanto lo que resulte de la retroalimentación será agregado al Secure Backlog para ser resuelto en la siguiente iteración.

4. Discusión

En el desarrollo de software los problemas más comunes que se enfrentan al tratar de seguir una metodología de desarrollo ágil seguro suelen ser:

- Falta de costumbre en identificar puntos inseguros o vulnerables.
- Falta de claridad en los requisitos: requisitos cambian de forma constantemente, es difícil mantener un enfoque seguro en el desarrollo del software.
- Integración de seguridad tardía: La integración de seguridad a menudo se retrasa hasta la fase final del desarrollo, lo que puede resultar en soluciones de seguridad ineficaces o incluso en la introducción de vulnerabilidades, en especial este aspecto de evitará al seguir la propuesta que el presente articulo propone.
- Colaboración y comunicación limitadas: La falta de colaboración y comunicación entre los equipos de desarrollo y seguridad puede resultar en soluciones de software que no cumplen con los requisitos de seguridad.
- Dificultades para hacer seguimiento a la evolución de la seguridad: En un entorno ágil, puede ser difícil mantener un seguimiento continuo de la evolución de la seguridad del software.
- Cambios frecuentes en los integrantes del equipo y en la asignación de tareas: En un entorno ágil, los equipos y las asignaciones de tareas pueden cambiar con frecuencia, lo que puede resultar en la falta de continuidad en la implementación de medidas de seguridad.

5. Conclusiones

La construcción de software tiene la compleja tarea de crear un software que no descuide la seguridad durante todo el ciclo de vida, es por ese motivo que la implementación de Scrum Secure y DevSecOps para el desarrollo de software seguro probablemente tendrá un gran impacto al culminar el desarrollo de software.

El seguir buenas prácticas que se propone permitirá:

- Mejora de la seguridad: Al integrar la seguridad en todas las fases del ciclo de vida del software.
- Mayor eficiencia: Al utilizar Scrum Secure y

DevSecOps, el equipo de desarrollo puede detectar y corregir problemas de seguridad más temprano, lo que reduce el tiempo y los costos de corrección.

- Mayor colaboración: Scrum Secure y DevSecOps promueven una mayor colaboración entre los equipos de desarrollo y seguridad.

- Mayor confianza en el software: Al asegurarse de que el software cumpla con los estándares de seguridad, los clientes y usuarios finales tendrán más confianza en el software desarrollado.

En resumen, la implementación de Scrum Secure y DevSecOps puede ayudar a mejorar la seguridad, la eficiencia, la colaboración y la confianza en el software desarrollado.

6. Referencias Bibliográficas

- Piña Gargiullo, B. A. (2019). PROPUESTA DE METODOLOGÍA DE DESARROLLO SEGURO DE SOFTWARE [Tesis de Grado, Universidad Andrés Bello]. Repositorio Institucional – Universidad Andrés Bello.

- Díaz, Javier & Sancho Núñez, José Carlos & Gutiérrez, Oscar & Homaei, Mohammadhossein. (2022). Un nuevo enfoque DevSecOps al modelo Viewnext-Uex.

- Rodríguez Carracedo, R. (2022). Análisis de servicios y mecanismos de seguridad desde el diseño en front-ends de desarrollo web. Universidad de Valladolid.

- Pérez Lastra, O., Gainza Reyes, D., & González Brito,

H. R. (2023). Estudio del desarrollo seguro del software. Serie Científica De La Universidad De Las Ciencias Informáticas, 16(1), 131-145.

- Carter, Kim. (2017). Francois Raynaud on DevSecOps. IEEE Software. 34. 93-96. 10.1109/MS.2017.3571578.

Artículo Recibido: 14/03/2023

Artículo Aceptado: 12/05/2023

EXPLOIT "DIA CERO"

Autor:
Juan Andrés Avila Cruz
andrucrux@gmail.com

Resumen

Actualmente tenemos un mundo basado en la informática donde los sistemas de información son esenciales para una empresa por la disponibilidad de información la confidencialidad y la seguridad de la información, sin embargo una de las amenazas más problemáticas de los sistemas informáticos a las cuales nos adentraremos es el uso de exploits(código malicioso que busca una vulnerabilidad en la seguridad de los sistemas para ingresar de forma no autorizada), algunos exploit ya son conocidos como día cero ocasionados por fallos de diseño que aún no se han corregido o reportado pues los desarrolladores aún no han podido detectar , en el presente artículo veremos cómo podría afectar a un sistema empresarial y qué medidas se deberían tomar para evitarlos desde un punto de vista hacker utilizando buenas prácticas de seguridad de la información, sin olvidar que tener un sistema 100% seguro es imposible .

Palabras Clave: Exploit, Información, Auditoria, desarrollador, Empresa, Hacker, Crackers, Estándares, Buenas Prácticas, informática, Modelos, Sistema.

Abstract

We currently have a world based on information technology where information systems are essential for a company due to the availability of information, the confidentiality and security of information, however one of the most problematic threats to information systems that we will delve into is the use of exploits (malicious code that seeks a vulnerability in the security of systems to enter unauthorizedly), some exploits are already known and others that are not yet known or were not disclosed due to design flaws that They have not yet been corrected or reported because the developers have not yet been able to detect them. In this article we will see how it could affect a business system and what measures should be taken to avoid them from a hacker point of view using good information security practices, without forgetting that having a 100% secure system is impossible.

Keywords: Exploit, Information, Audit, developer, Company, Standards, Good Practices, computing, Models, System.

Introducción

Aunque las empresas siempre han tenido que enfrentarse a muchas amenazas, los ciberataques son cada vez más preocupantes. Una vulnerabilidad de día cero a través de exploit, es una de las amenazas de malware más graves.

Los ciberataques pueden tener graves consecuencias para las empresas, ya que los piratas informáticos pueden robar dinero, datos o propiedad intelectual que comprometan tus operaciones. Y ninguna empresa es inmune. Afectan a los comerciantes, a las empresas locales, a las cadenas nacionales e incluso a los gigantes mundiales como Google (sufre como más de 20 ataques que afectan sus servicios cada año).

Los sistemas actuales están migrando cada día a la nube siendo las plataformas de desarrollo más populares basadas en lenguajes de programación como PHP, Java, Visual Basic .net entre otras, al estar en la nube los sistemas son accesibles para

Contenido

"Día cero" es un término amplio que describe vulnerabilidades de seguridad recién descubiertas que los hackers usan para atacar sistemas. El término "día cero" se refiere al hecho de que el proveedor o desarrollador acaba de conocer acerca de la falla, lo que significa que ha tenido "cero días" para corregirla. Un ataque de día cero ocurre cuando los hackers aprovechan la falla antes de que los desarrolladores tengan la oportunidad de solucionarla.

"Día cero"

a veces suele escribirse como "día 0". Las palabras "vulnerabilidad", "exploit" y "ataque" suelen usarse junto al concepto de día cero, y es muy útil entender la diferencia:

Una vulnerabilidad de día cero es una vulnerabilidad de software que los atacantes descubrieron antes de que el proveedor sepa siquiera de su existencia. Debido a que los

todo tipo y nivel de usuario que requiera ingresar al servicio ya sea público o privado, es así que los sistemas en la nube pueden ser identificados por Crackers que nos pueden empezar a atacar los ciberataques son inevitables, sin embargo, hay medidas que podemos tomar para protegernos.proveedores desconocen este problema, no existen parches para vulnerabilidades de día cero, por lo cual es muy probable que los ataques tengan éxito.

Un exploit de día cero es el método que usan los hackers para atacar sistemas con una vulnerabilidad anteriormente no identificada.

Un ataque de día cero es el uso de un exploit de día cero para causar daños o robar datos a un sistema afectado por una vulnerabilidad

De: latam.kaspersky.com

ATAQUES DÍA CERO A menudo, el software tiene vulnerabilidades de seguridad que los hackers pueden aprovechar para provocar el caos. Los desarrolladores de software siempre buscan vulnerabilidades para "parchear"; es decir, desarrollan una solución que lanzan en una nueva actualización.

Sin embargo, a veces los hackers o las entidades maliciosas detectan la vulnerabilidad antes de que los desarrolladores de software lo hagan. Mientras la vulnera-

bilidad sigue disponible, los atacantes pueden escribir e implementar un código para aprovecharse de ella. Esto se conoce como código de exploit.

El código de exploit puede dar lugar a que los usuarios de software sean víctimas; por ejemplo, mediante el robo

de identidad u otras formas de cibercrimen. Una vez que los atacantes identifican una vulnerabilidad de día cero, necesitan una forma de comunicarse con el sistema vulnerable. Para ello, a menudo usan un correo electrónico que usa ingeniería social; es decir, un correo electrónico u otro mensaje que supuestamente proviene de un remitente conocido o legítimo, pero que realmente proviene de un atacante. El mensaje intenta convencer a un usuario que realice una acción como abrir un archivo o visitar un sitio web malicioso. Tras hacerlo, se descarga el malware del atacante, el cual se infiltra en los archivos del usuario y roba datos confidenciales.

Cuando se conoce una vulnerabilidad, los desarrolladores intentan corregirla para detener el ataque. Sin embargo, a menudo las vulnerabilidades de seguridad no se descubren de inmediato. A veces, pueden pasar días, semanas o incluso meses antes de que los desarrolladores identifiquen la vulnerabilidad que dio lugar al ataque. Además, incluso si se publica un parche de día cero, no todos los usuarios lo implementan rápidamente. En años recientes, los hackers se han vuelto más rápidos en abusar de las vulnerabilidades apenas las descubren.

Los exploits se pueden vender en la web oscura por grandes sumas de dinero. Una vez que se descubre y corrige un exploit, ya no se conoce como una amenaza de día cero.

Los ataques de día cero son especialmente peligrosos debido a que las únicas personas que saben de ellos son los atacantes mismos. Una vez que se infiltran en una red, los criminales pueden atacar inmediatamente o esperar el mejor momento para hacerlo. De:latam.kaspersky.com

PRINCIPALES ATACANTES

Cibercriminales: hackers cuya motivación suele ser obtener ganancias financieras.

Hacktivistas: hackers motivados por una causa política o social que desean que los ataques sean visibles para llamar la atención a su causa.

Espionaje corporativo: hackers que espían a empresas para obtener información sobre ellas.

-Guerra informática: países o entidades políticas que espían o atacan la infraestructura cibernética de otro país.

De: kinsta.com/es/blog/exploit-de-zero- day

-Organizaciones con mala ciberseguridad

-Organizaciones que manejan datos personales (DATOS PERSONALES, BASES DE CLIENTES DE EMPRESAS)

-Organizaciones que tienen información confidencial

-Organizaciones que crean software o hardware para clientes (ya que pueden utilizar la tecnología para hackear a los clientes)

-Organizaciones que trabajan en el ámbito de la defensa

EJEMPLO PRÁCTICO

En la actualidad aproximadamente el 78% de los portales web están escritos en PHP, según las estadísticas de w3techs.Daremos un ejemplo de código malicioso el cual queremos insertar en el sistema web de un banco.

Primero ocultamos nuestra ip al mundo simulando que estamos en EEUU Nueva York con "atlas VPN".

BLANCOS DE UN EXPLOIT

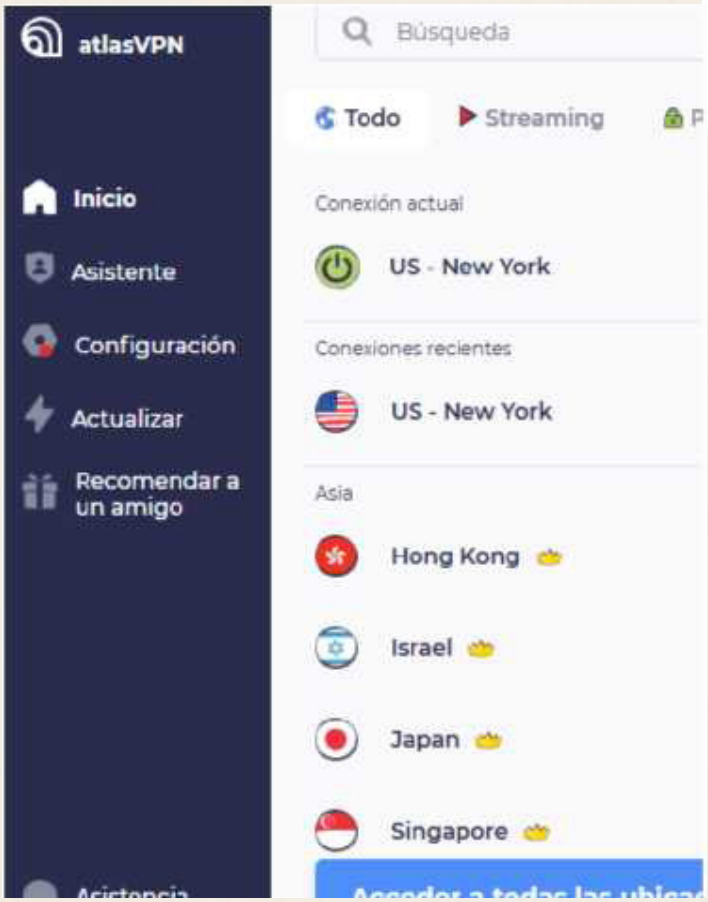
Un hackeo de día cero puede aprovechar vulnerabilidades en una variedad de sistemas, como los siguientes:

Identificamos el Ip a atacar identificamos ello mediante un simple comando Dos.

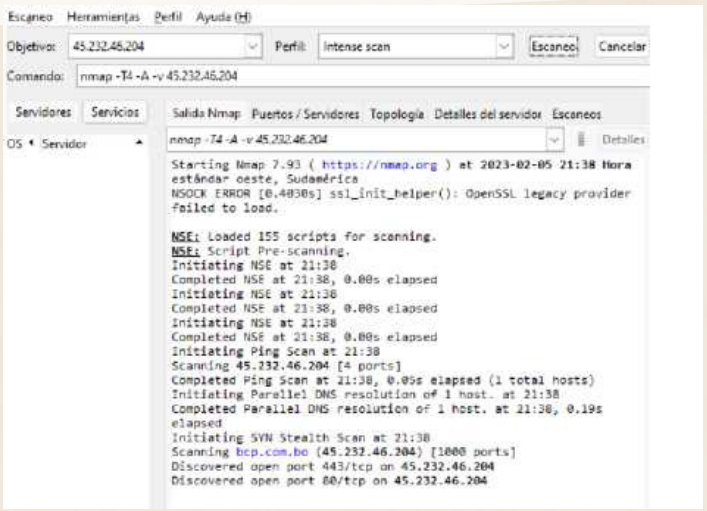
Figura: 2. Identificación de Ip objetivo FUENTE: Elaboración propia

Identificamos el objetivo a scanear para ver si tiene fallos de seguridad con la herramienta Zenmap la cual verifica si hay puertos abiertos en la red del sistema web por el que podamos ingresar.

Figura: 1 ocultamiento de Ip del Hacker



FUENTE: Elaboración propia




```
C:\Windows\system32>ping www.bcp.com.bo

Haciendo ping a www.bcp.com.bo [45.232.46.204] con 32 b
Respuesta desde 45.232.46.204: bytes=32 tiempo=19ms TTL
Respuesta desde 45.232.46.204: bytes=32 tiempo=16ms TTL
Respuesta desde 45.232.46.204: bytes=32 tiempo=14ms TTL
Respuesta desde 45.232.46.204: bytes=32 tiempo=14ms TTL

Estadísticas de ping para 45.232.46.204:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 14ms, Máximo = 19ms, Media = 15ms
```

deseado no funcionarla, como información nos avisa que sistema operativo utiliza, pero podemos identificar el tipo de encriptado realizado en esta comunicación que son:

MD5:

da977d79eb119c705084dcc8f2bd170 6

SHA-1:

3a60bade116299e0c6f9aca5ecf10176 db5e9398

Verificamos los ficheros accesibles e ingresamos mediante algún host ip del sitio atacado e insertamos un archivo para llamarlo desde donde nos encontremos usando el host de la víctima para sacar información.

Por razones solo-didácticas llegaremos hasta este punto poniendo en claro que lo realizado no es confines maliciosos solo con el fin de identificar vulnerabilidades que podamos detectar de forma solo educativa.

Podemos identificar dos fallos de seguridad por la red, usaremos los fallos para poder ingresar y tratar de revisar datos del disco duro del servidor y ver el nivel de seguridad colocando un formulario falso para algún usuario y obtener las contraseñas utilizando el puerto 443 de la red.

Figura: 4 puerto abierto

```
|_  Supported Methods: GET HEAD POST OPTIONS
443/tcp open  ssl/https
|_ssl-date: TLS randomness does not represent time
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 301 Moved Permanently
|     Content-Type: text/html; charset=UTF-8
|     Location: https://www.bcp.com.bo/
|     X-Xss-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Referrer-Policy: no-referrer
|     X-Permitted-Cross-Domain-Policies: none
|     X-Frame-Options: SAMEORIGIN
|     Strict-Transport-Security: max-age=31536000;
includeSubDomains
```

FUENTE: Elaboración propia

Podemos ver que los resultados obtenidos de análisis del puerto en resumen es la conexión cifrada con seguridad, además de tener actualizada la versión del servidor, la versiones PHP es superior a 7.1 por lo que el código

Podemos ver que nuestro fichero esta activo en el host de la victima

De modo que llamando al host de la víctima desde cualquier navegador

Conclusión

La seguridad de la información muchas veces se pasa por alto sin prevenir que hay personas preparadas para usar la tecnología que esta a mano con fines delincuenciales mismos que en nuestro país aún no tienen fuertes penalizaciones con la ley actual Boliviana, existen softwares gratuitos y de paga por los cuales se pueden insertar exploits a los sistemas , debido a que algunos desarrolladores no toman en cuenta la seguridad de la información , ello rebajaría las vulnerabilidades de un sistema, aplicar las buenas practicas aplicando una norma de calidad como el ISO 27001 en la cual se puede ver los siguientes puntos

Creación de un plan SGSI el cual consta de:

-Políticas de seguridad en todas las áreas (hardware y software), -metodologías de seguridad.

-creación de un cuadro de evaluación de riesgos.

-informes de los resultados.

-Acciones correctivas.

-plan de tratamiento.

-plan de formación.

La norma nos generara un plan de contingencias ante posibles ataques Día Cero, minimizando el impacto en la empresa u organización.

, también se recomienda la actualización de versiones de plataformas de desarrollo o sistemas operativos que se manejen 30.

Bibliografía

Día Cero https://kinsta.com/es/blog/exploit-de- zero-day/

-Revista Ciencia Unemi, Universidad Estatal de Milagro 2011

Código fuente Exploit https://github.com/80vul/php-codz/blob /master/research/pch-009.md

www.hackplayers.com

Normas ISO 27001

latam.kaspersky.com

kinsta.com/es/blog/exploit-de-ze ro- day

Artículo Recibido: 14/03/2023

Artículo Aceptado: 12/05/2023

INSTRUCCIONES PARA LOS AUTORES

ILUMINATE

REVISTA DE INVESTIGACIÓN DE LA CARRERA DE INGENIERÍA DE SISTEMAS

UNIVERSIDAD LA SALLE EN BOLIVIA

MISIÓN

Nuestra Misión es publicar, divulgar trabajos de investigación generados en el ámbito académico de Las Ciencias de la Computación a nivel nacional e internacional, elaborado principalmente por estudiantes e investigadores para aportar a la producción científica de nuestra universidad y de nuestro país.

POLÍTICA EDITORIAL

Iluminate, es una publicación editada por la Carrera de Ingeniería de Sistemas de la Universidad La Salle de Bolivia, con **frecuencia de publicación anual**, busca divulgar trabajos de investigación del area de las ciencias de la computación generados en el ambiente Universitario por estudiantes y en entornos colaborativos con otras universidades. Se reciben contribuciones en español e inglés. El Artículo candidato a publicación debe cumplir con las normas que aparecen en las instrucciones para los autores. Luego de su recepción, el artículo se somete a evaluación por pares, los que recomiendan su aceptación o rechazo.

La revista solicita a los autores con preferencia remitir artículos originales u originales cortos, artículos inéditos en español o inglés con carácter científico, que serán valorados por el comité editor.

La revista se divulga en forma impresa y electrónica, esta ultima para ampliar el espectro de difusión, nos interesa que profesionales, pequeñas, medianas y grandes empresas, organismos, tomadores de decisiones, otros investigadores, docentes y estudiantes universitarios, puedan acceder a sus páginas y establecer referencias para potenciar el desarrollo local y regional.

LICENCIAMIENTO

Los artículos que sean seleccionados para formar parte de la revista deberán ser autorizados por su autores o autores, para su difusión a través de

cualquier medio, mediante formato establecido para dicho fin. Los artículos de la revista, permanecen en acceso abierto disponibles en la página web institucional como en los diferentes índices y bases de datos a los cuales la revista está suscrita.

INSTRUCCIONES PARA LA PRESENTACIÓN DE ARTÍCULOS

1. La entrega de artículos y afiliación

Los artículos, serán recibidos y registrados en Dirección Académica de la Universidad La Salle:

Editor en Jefe - Revista Iluminate

oyokosaki@ulasalle.edu.bo;

Instituto de Investigaciones, Universidad La Salle

Calle Jorge Carrasco, esquina Las Palmas, No. 450, zona Bolognia- La Paz, Bolivia

Tel: 591-2-2723588 - 2723598 / Fax: 591-2-2723588

http://www.ulasalle.edu.bo/Iluminate

La universidad entregará, en este caso, acuse de recepción por la misma vía.

Se entregarán en formato digital en una versión actualizada de Word. Las fechas de recepción y aceptación del artículo son importantes, y deberán ocupar un lugar en el artículo de acuerdo con el formato para la presentación de artículos.

En caso de ser el primer aporte de la revista, el autor deberá presentar en formato digital, nombres y apellidos completos, grado académico, lugar y fecha de nacimiento, lugar de trabajo actual, cargo actual y dirección correo electrónico, para su respectiva afiliación.

Los autores publicados en Iluminate se afiliarán automáticamente a la publicación para recibir periódicamente la revista en formato impreso.

2. Proceso de arbitraje

Una vez recibido el artículo y que se ha comprobado que cumple con los requisitos de forma indicados en las instrucciones para el autor, se acusará recibo mediante correo electrónico y se iniciará el proceso de selección.

Los revisores evaluadores serán designados por el Comité Editorial. Se empleará la metodología "revisores ciegos", quienes evaluarán los aspectos propios de la especialidad tratada.

Los artículos recibidos y admitidos por el Comité Editorial serán enviados, con la información de los autores a dos (2) evaluadores de reconocido prestigio en el área y materia del artículo remitido, también se remitirá el formulario de evaluación.

Los evaluadores tendrán cuatro semanas para revisar el artículo y entregar el formulario de evaluación lleno. Los árbitros evaluadores pueden sugerir modificaciones al artículo original que deben ser realizados por el autor para la aceptación de su artículo. El autor tiene (15) días

hábiles para entregar el artículo reformulado. En caso de existir diferencia de opinión entre los dos árbitros evaluadores, se procederá a enviar el artículo a un tercer evaluador o al Editor que dirimirá la controversia.

La evaluación negativa se podrá justificar en los siguientes casos:

a) La clasificación propuesta no concuerda con el desarrollo del artículo.

b) Si presenta deficiencias en la redacción o el desarrollo científico.

c) Si la información contenida no respeta los derechos de autor.

d) Si el artículo no corresponde al eje temático de la revista.

3. Conflicto de Interés

Iluminate aplicará mecanismos internos de resguardo y cautela, para evitar conflicto de interés que afecte a la objetividad en todo el proceso editorial y que involucren al comité editorial y a los evaluadores anónimos en el proceso de arbitraje.

4. Aceptación de artículos

Una vez concluida la etapa de evaluación, será comunicada al autor la decisión sobre la aceptación o rechazo del artículo por parte del Comité Editorial.

El artículo deberá presentar la fecha de entrega y aceptación, éstas serán impresas de acuerdo con las instrucciones para los autores. Adicionalmente el autor deberá llenar el formulario de autorización para la publicación del artículo o revista escrita y/o digital

El comité editorial, declara que las opiniones y comentarios expresados en los artículos son de responsabilidad exclusiva de sus autores.

La revista Iluminate comunicará al autor, el informe final de evaluación. Dicha Comunicación tendrá lugar en un plazo máximo de seis (6) meses, a contar desde la fecha de recepción del artículo.

5. Publicación

El artículo aceptado será publicado en el siguiente número de revista disponible de espacio para el efecto.

6. Afiliación de Evaluadores

Un árbitro evaluador será parte de la base de datos de Iluminate al momento de ser nombrado por el comité editorial y haber aceptado la primera solicitud de evaluación de un artículo. Para su registros será necesario ingresar el curriculum vitae del evaluador con los siguientes datos: nombres y apellidos completos, lugar de estudio, y dirección correo electrónico.

7. Conformación del Comité Editorial

El comité editorial será conformado por disposición de Consejo de la carrera de Ing. de Sistemas de la

Universidad La Salle en Bolivia, nombrando para el efecto los siguientes estamentos; Editor, Editor responsable, Consejo editorial, Consejo de Arbitraje, Colaboradores, Diseño y Diagramación.

El Consejo Editorial aprobará la incorporación de nuevos evaluadores.

8. Compromisos y Responsabilidades éticas

Cada autor presentará una declaración responsable de autoría y originalidad respecto de los siguientes aspectos:

- Inédito. No ce acepta material previamente publicado. Los autores son responsables de obtener los oportunos permisos para reproducir parcialmente (texto, tablas o figuras) de otras publicaciones y de citar su procedencia correctamente. Las opiniones expresadas en los artículos publicados son responsabilidad del autor/es

- Autoría. En la lista de autores firmantes deben figurar únicamente aquellas personas que han contribuido intelectualmente al desarrollo del trabajo. Haber colaborado en la recolección de datos no es, por si mismo, criterio suficiente de autoría. Iluminate declina cualquier responsabilidad sobre posibles conflictos derivados de la autoría de los trabajos que se publiquen.

- Consentimiento informado. Los autores deben mencionar que los procedimientos empleados en sujetos de experimentación han sido realizados con consentimiento informado.

INSTRUCCIONES PARA LOS AUTORES

Todos los artículos serán publicados en español, con título en español e inglés, con resúmenes en español e inglés.

1. Instrucciones respecto al tipo de artículo

Los trabajos se estructurarán de acuerdo con las secciones y normas que a continuación se exponen:

a) ***Artículos originales (investigación científica).*** Documento que presenta, de manera detallada, los resultados originales de proyectos terminados de investigación.

Los **artículos originales**, de **reporte de caso** y **cortos**, deben cumplir con la siguiente estructura: la **introducción** debe resaltar la importancia de la investigación, presentar la literatura relacionada y entregar antecedentes necesarios para comprender la hipótesis de los autores, terminando con un párrafo que indique claramente los objetivos de la investigación. El **Método** debe tener suficiente información que permita a otro investigador replicar el ensayo y lograr los mismos resultados, así como la inclusión del diseño experimental, el análisis estadístico y las referencias de los métodos ya publicados.

Los **resultados y discusión** se deben presentar en forma clara, apoyados con cuadros y figuras, con el análisis estadístico y los antecedentes

de otros investigadores. Las **conclusiones** deben redactarse de acuerdo con los objetivos de la investigación explicando claramente los principales resultados de la investigación. Las **referencias** deben contener todos los documentos consultados.

b) ***Artículo de reflexión.*** Documento que presenta resultados de investigación terminada desde una perspectiva analítica, interpretativa o crítica del autor, sobre un tema específico, recurriendo a fuentes originales. Los **artículos de reflexión** deben mostrar: a)intención analítica; b)propósito interpretativo; c)posición crítica. La estructura: **Resumen, Introducción, Desarrollo del tema, Conclusiones y referencias**.

c) ***Artículo de revisión.*** **Documento resultado de una investigación terminada donde se analizan, sistematizan e integran los resultados de investigaciones publicadas o no publicadas, sobre un campo en ciencia o tecnología, con el fin de dar cuenta de los avances y las tendencias de desarrollo. Se caracteriza por presentar una cuidadosa revisión bibliográfica de por lo menos** 40 referencias. Los **artículos de revisión** deben tener: **Resumen, Introducción, Desarrollo del tema, Conclusiones y referencias**.

d) Artículo original corto. Documento breve que presenta resultados originales preliminares o parciales de una investigación científica o tecnológica, que por lo general requieren de una pronta difusión. Tiene la misma estructura de los artículos originales.

e) Reporte de caso. Documento que presenta los resultados de un estudio sobre una situación particular con el fin de dar a conocer las experiencias técnicas y metodológicas consideradas en un caso específico. Incluye una revisión sistemática comentada de la literatura sobre casos análogos.

f) Revisión de tema. Documento resultado de la revisión crítica de la literatura sobre un tema en particular.

g) Cartas al editor. Posiciones críticas, analíticas o interpretativas sobre los documentos publicados en la revista, que a juicio del Comité Editorial constituyen un aporte importante a la discusión del tema por parte de la comunidad científica de referencia.

h) Editorial. Documento escrito por el editor, un miembro del comité editorial o un investigador invitado sobre orientaciones en el dominio temático de la revista.

i) Traducción. Traducciones de textos clásicos o de actualidad o transcripciones de documentos históricos o de interés particular en el dominio de publicación de la revista.

j) Documento de reflexión no derivado de investigación. Reflexión sobre un tema en particular, el cual no requiere ser derivado de una investigación científica o tecnológica

k) Reseña bibliográfica.

l) Otros

En todos los casos el artículo debe presentar aspectos de originalidad y contener las referencias bibliográficas.

Adicionalmente el autor deberá llenar el formulario de autorización para la publicación de artículos y/o revistas en formatos impresos y digitales.

2. Instrucciones respecto al formato del artículo

Los artículos seleccionados serán el centro de la revista, por lo que deben ajustarse a las siguientes especificaciones de forma:

a) Título del artículo (en español e inglés) no debe tener más de 15 palabras. El título estará escrito con letras minúsculas y en negritas con tipo Times New Román de 12 puntos y centrado, este debe contener máximo 15 palabras. (En español e inglés).

b) Lista de Autores: Con los nombres completos y apellidos en el orden que deben aparecer. Adicionalmente el autor principal anotará su correo electrónico, para la correspondencia de editores y lectores; lugar y fecha de investigación y financiamiento si la tuvo.

c) Resumen y palabras clave: Se presenta un resumen en español y en inglés máximo de 100 palabras. Palabras clave en español e inglés (hasta un máximo de diez palabras).

d) Texto del artículo: Cuando los artículos son originales y original corto deberán tener las siguiente partes:

Introducción: El autor debe establecer el propósito del estudios, resumir su fundamento lógico.

Materiales y métodos: Incluye la selección de procedimientos para el trabajo experimental, y se indentifican los métodos y equipos con suficiente detalle.

Resultados y Discusión: Debe presentarse en secuencia lógica con sus re4spectivas tablas y gráficas y los comentarios de los principales hallazgos. En la Discusión enfatizar los aspectos más importantes del estudio.

Conclusiones: Anotar una o más conclusiones.

Los demás artículos deberán tener como mínimo resúmen, palabras clave, el desarrollo del tema y las conclusiones.

e) El artículo debe estar capturado electrónicamente en una versión actualizada de Word, su extensión no debe exceder las doce (15) páginas en una columna y espacio sencillo, letras Times New Roman de 10 puntos, en hojas tamaño carta.

f) Los títulos principales deberán siempre ser precedidos de una línea en blanco, salvo que con ellos se comience una nueva página. Los títulos principales se escribirán centrados utilizando

letras mayúsculas y en negritas con tipo Times New Román de 10 puntos. Se dejará una línea en blanco después de cada título principal. Cada título tendrá al menos dos líneas de texto que le continúen al final de cada hoja.

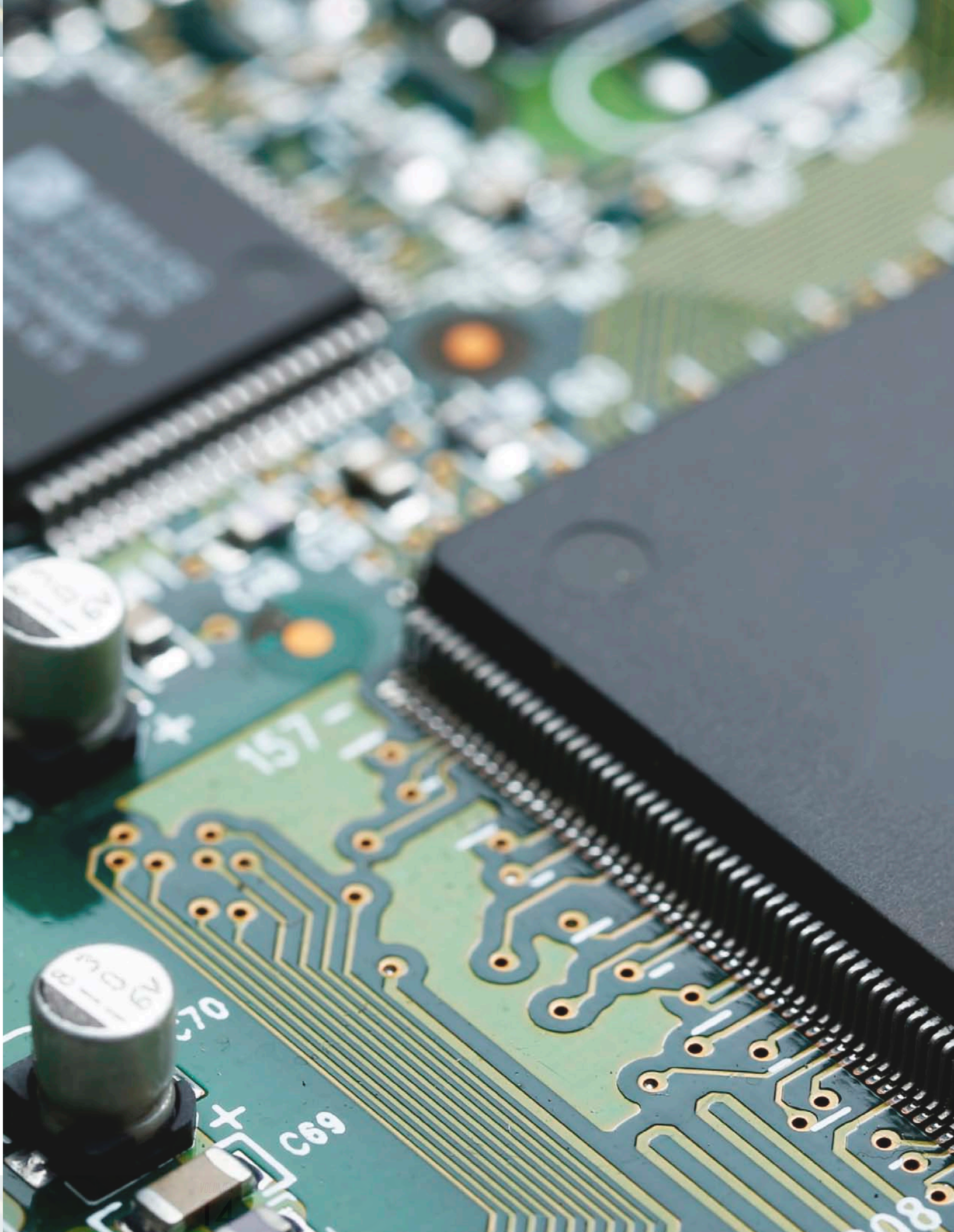
g) Las tablas deberán intercalar en el texto, ubicándose lo más cerca posible a la sección de texto que las refiere, pero no será aceptable, por fines de uniformidad, dividir la página en varias columnas para intercalar tabla en el texto. Se deberán centrar con respeto al formato del texto y deberá existir por lo menos una línea en blanco antes y después de cada tabla. La numeración de tablas deberá hacerse de forma secuencial. Los títulos de las tablas deberán ir en su parte inferior.

h) Las figuras se deberán intercalar con el texto, ubicándose lo más cerca posible a la sección de texto que las refiere, pero no será aceptable, por fines de uniformidad, dividir la página en varias columnas para intercalar figuras con el texto. Se deberán centrar con respecto al formato del texto y deberá existir por lo menos una línea en blanco antes y después de cada figura. La numeración de figuras deberá hacerse de forma secuencial. Los títulos tendrán como máximo una extensión de dos líneas. Las figuras no deberán enmarcarse, salvo que se trate de gráficas donde esto último se justifique. Asimismo, en la instrucción de formato de imagen de Word, deberá asegurarse que la figura se defina como un objeto en línea con el texto, con la finalidad de que el control de la posición de la imagen en el mismo sea fácil de manipular por los editores en caso que se requiera algún ajuste menor en el artículo.

i) Si desea incluir una sección de agradecimientos, esta se ubicará después de la sección de conclusiones y antes de la sección de referencias, utilizando el mismo formato que para títulos y secciones principales.

j) Las fuentes bibliográficas deben ser citadas a lo largo del texto, en formato APA.

k) Cualquier tema no cubierto en lo anterior será resuelto por el editor coordinador en el Consejo editorial y deberán ser consultados al siguiente correo electrónico: oyokosaki@ulasalle.edu.bo ■


C70
C69

La Salle
Universidad
Bolivia

INGENIERÍA DE SISTEMAS

Campus Universitario Bolognia Av. Jorge Carrasco esq. Las Palmas
Teléfono: 591-2-2723588 - 2723732 - 2744650
www.ulasalle.edu.bo
La Paz - Bolivia