https://repository.uaeh.edu.mx/revistas/index.php/sahagun/issue/archive

Ingenio y Conciencia Boletín Científico de la Escuela Superior Ciudad Sahagún

Publicación semestral, Vol. 8, No. 16 (2021) 26-30

ISSN: 2007-784X

Encriptación a la medida, mediante Cálculos Matemáticos, para la Seguridad de Datos de una Microempresa

Customized encryption, through Mathematical Calculations, for the Security of Data of a Microenterprise

Yira Muñoz-Sánchez [a], María A. Alonso-Lavernia [b], Iliana Castillo-Pérez [c], Verónica Martínez-Lazcano [d], Fabián Gálvez-González [e], Cuitláhuac Alamilla-Cintora [f]

Abstract:

The data that they handle from micro to macro companies are stored in databases for storage, processing and presentation that allows decision-making. However, data is one more resource that must be protected for what it represents, especially those of a vulnerable type, since they can suffer damage that puts the future of the company at risk. Encryption is an option to protect this data and in this work the development of a mathematical procedure to encrypt and decrypt the vulnerable data of a micro-company is shown, also ensuring that these processes are transparent to end users but ensuring the integrity of the information stored in the database.

Keywords:

Encryption, database, data security.

Resumen:

Los datos que manejan desde las micro hasta las macroempresas son guardados en bases de datos para su almacenamiento, procesamiento y presentación que permita la toma de decisiones. Sin embargo, los datos son un recurso más que debe ser protegido por lo que representan, sobre todo aquellos de tipo vulnerable, ya que pueden sufrir daños que ponen en riesgo el futuro de la empresa. La encriptación es una opción para proteger estos datos y en el presente trabajo se muestra el desarrollo de un procedimiento matemático para encriptar y desencriptar los datos vulnerables de una microempresa, asegurando además que estos procesos sean transparentes a los usuarios finales pero asegurando la integridad de la información almacenada en la base de datos.

Palabras Clave:

Encriptación, base de datos, seguridad de datos.

[a] Autor de Correspondencia, Universidad Autónoma del Estado de Hidalgo, Escuela Superior de Ciudad Sahagún, https://orcid.org/0000-0002-4876-2747, Email: yira@uaeh.edu.mx

[b] Universidad Autónoma del Estado de Hidalgo, Instituto de Ciencias Básicas e Ingeniería, https://orcid.org/0000-0002-9839-8250, Email: marial@uaeh.edu.mx

[c] Universidad Autónoma del Estado de Hidalgo, Instituto de Ciencias Básicas e Ingeniería, https://orcid.org/0000-0002-8130-9231, Email: ilianac@uaeh.edu.mx

[d] Universidad Autónoma del Estado de Hidalgo, Instituto de Ciencias Básicas e Ingeniería, https://orcid.org/0000-0003-2172-4000, Email: vlazcano@uaeh.edu.mx

[e] Universidad Tecnológica del Valle del Mezquital, https://orcid.org/0000-0003-4073-6525, Email: faglvz@gmail.com

[f] Universidad Tecnológica del Valle del Mezquital, https://orcid.org/0000-0002-0221-231X, Email: cuitlahuacalamillacintora@gmail.com

Fecha de recepción: 21/03/2021, Fecha de aceptación: 20/05/2021, Fecha de publicación: 05/07/2021

Introducción

Desde hace algunas décadas, las empresas han considerado controles de seguridad para los datos, pero no todos incluyen políticas y planes para lograr una seguridad informática.
La seguridad de los datos se considera como la protección a ellos contra pérdidas de tipo accidental o intencional, su destrucción o un mal uso que se haga de ellos (Cuadra, 2010; Narang, 2011).

De forma específica, de acuerdo con Hoffen, Prescott y McFadden (2007), los daños que pueden sufrir los datos son:

- Pérdidas accidentales, incluyendo errores humanos y daños en el hardware.
- Robo y Fraude.
- Pérdida de la privacidad y confiabilidad.
- Pérdida de la integridad de los datos.
- Pérdida de la disponibilidad de los datos.

Una alternativa para evitar los daños, antes listados, a los datos de una empresa es el uso de la encriptación, la cual consiste en la codificación o cifrado de los datos para que las personas no las puedan leerlos, ya que se convierten en una secuencia de caracteres ilegibles, entonces de esta manera se puede garantizar la confidencialidad y la integridad de la información, así como el aseguramiento de la privacidad de los datos. (García, 2020; Hoffen, Ramesh y Topi, 2019).
La encriptación debe incluir rutinas para decodificar y es un recurso que ha tomado relevancia en la actualidad, ya que permite asegurar la transferencia de los datos y éstas rutinas también deben tener medidas de seguridad, de lo contrario no tiene validez la codificación, sobre todo cuando existe una comunicación en red, y se deben administrar y mantener seguros los datos como la administración de contraseñas, autógrafos analógicos, etc., en donde se requieren algoritmos para encriptar (García, 2020; Piattini, Marcos, Calero y Vela, 2006; Rob y Coronel, 2005).
Si bien existen diversos tipos de algoritmos para encriptar datos, como los de clave secreta, clave pública o de resumen, en ocasiones resulta complicado determinar en la práctica el desempeño de ellos y pueden resultar frágiles ante los ataques que pudieran sufrir los datos, además de que algunos trabajan bajo combinaciones de variadas longitudes (Cabrera, H. J., 2018; Chmel y Mužný, 2019).
La diferencia entre las microempresas y las macroempresas es que éstas últimas cuentan con la tecnología suficiente para la protección de los datos e información que en ellas se maneja.
Además de que es necesario fomentar el desarrollo de sistemas con un funcionamiento adecuado, de acuerdo con las necesidades de las organizaciones y a bajo costo (Montenegro, 2020).
En el presente trabajo se plantea la solución a una microempresa, para dar seguridad a los datos más vulnerables que en ella se manejan, a través de la encriptación, usando un algoritmo matemático desarrollado a la medida, que satisfaga sus necesidades de transferencia y lectura de datos en congruencia a sus condiciones de infraestructura.

Metodología

Para implementar el proceso de encriptación sobre los datos más vulnerables de la base de datos de la microempresa, para proporcionar seguridad, se siguió la siguiente metodología.

1. Identificar los datos más importantes o vulnerables de la empresa que requieren ser encriptados o cifrados. Las contraseñas de los usuarios porque en este caso son los datos más importantes que se manejan en la base de datos.
2. Desarrollar la interfaz gráfica para el almacenamiento de los datos encriptados.
3. Conectar la base de datos a la aplicación.
4. Seleccionar el procedimiento de encriptación. En este punto se desarrolló un algoritmo a la medida, de acuerdo con las necesidades de seguridad e infraestructura de la empresa.
5. Programación del algoritmo de cifrado.
6. Desarrollar la interfaz para el descifrado de los datos.
7. Programar el procedimiento de descifrado.
8. Realizar pruebas a los procesos desarrollados.

Resultados y Discusión

Una de las tablas consideradas para aplicar el proceso de encriptación se presenta en la Figura 1.

Figura 1. Tabla con datos vulnerables
Fuente: Creación Propia

Los datos de los usuarios de la base deben ser capturados y los datos identificados como vulnerables con la clave y la contraseña de los usuarios que son los datos que deberán encriptarse y son los que se muestran en la Figura 1.

El proceso de almacenamiento de los datos debe ser transparente al usuario final, así como el proceso de encriptación, por lo tanto, se generó una interfaz gráfica, que aparece en la Figura 2, para que dicho usuario capture los datos requeridos.

La Figura 2 muestra la interfaz para capturar los datos que serán almacenados en la base, una vez encriptados, a través del botón *Encriptar.*

Figura 2. Interfaz para almacenar los datos encriptados
Fuente: Creación Propia

Antes de programar el algoritmo de encriptación, es necesario realizar la conexión a la base de datos, en donde se almacenarán los datos no vulnerables y los vulnerables, éstos últimos se almacenarán encriptados. La conexión de la base de datos se realizó a través de la interfaz del servidor, con la opción de Agregar módulo, tal como se muestra en la Figura 3.

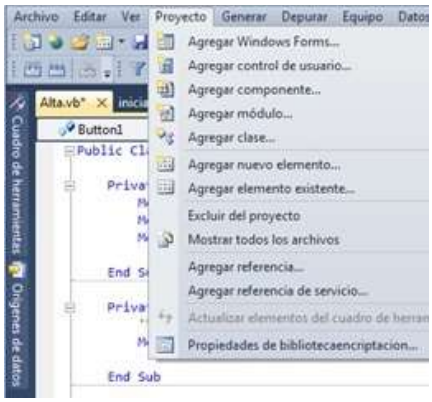

Figura 3. Conexión a la base de datos
Fuente: Creación Propia

En la opción de *Agregar módulo* se programó la conexión, mediante Visual Basic, que es una herramienta de Visual Studio para programación con bases de datos (Microsoft, 2021), usando el código que se muestra a continuación.

```
Imports System.Data.SqlClient
Imports System.Data
Module conexion
    Public con As New
SqlConnection("Integrated
Security=true;Server=ROKE-
PC\SQLEXPRESS;Database=NombreBaseDatos")
'Conexión a la base de datos

    Sub Main()
        Dim flogin As New iniciar
        If flogin.ShowDialog() =
System.Windows.Forms.DialogResult.OK Then
            flogin.Close()
            Application.Run(New Alta)
        End If
    End Sub
End Module
```

Una vez que se conectó la base de datos se procedió a programar la acción de guardar en la base de datos, mediante el botón de *Encriptar*, a través de la interfaz de la Figura 2. La codificación e invocación del algoritmo de encriptación se realiza dentro de este proceso, tal cual se muestra en el código siguiente.

```
Private Sub Button1_Click(ByVal sender As
System.Object, ByVal e As System.EventArgs)
Handles Button1.Click
        Dim caracter As Char
        Dim i As Integer
        Dim m As Integer
        TextBox2.Text = TextBox1.Text()
        TextBox2.Text = ""

        If TextBox1.Text.Length <= 0 Then
            MsgBox("No hay datos para
encriptar")
            TextBox1.Focus()
        Else
            m = TextBox1.Text.Length
            For i = 0 To m - 1
                caracter =
Chr(AscW(TextBox1.Text.Substring(i, 1)) + ((i
* 2) + AscW(TextBox1.Text.Substring(i, 1))))
'Encriptación
                TextBox2.Text = TextBox2.Text
& caracter
```

```
            Next
        End If

    End Sub
End Class
```

A través de la validación de cada usuario con su contraseña, que son los datos que fueron almacenados encriptados, se hace necesario el proceso de desencriptación, ya que este proceso debe ser transparente para él. La interfaz a través de la cual los usuarios realizan dicha validación se muestra en la Figura 4.

Figura 4. Interfaz con proceso de desencriptar
Fuente: Creación propia

A través del botón de Ingresar, que se muestra en la Figura 4, se invoca el proceso de desencriptación y validación de los datos previamente encriptados.

```
Imports System.Data.SqlClient
Imports System.Data
Public Class iniciar
    Private Sub Button1_Click(ByVal sender As
System.Object, ByVal e As System.EventArgs)
Handles Button1.Click
        Dim cmd As SqlCommand
        Dim dr As SqlDataReader
        Dim caracter As Char
        Dim i As Integer
        Dim m As Integer
        If TextBox2.Text.Length <= 0 Then
            MsgBox("No hay datos para
encriptar")
        Else
            m = TextBox2.Text.Length
            For i = 0 To m - 1
                caracter =
Chr(Asc(TextBox2.Text.Substring(i, 1)) + ((i
* 2) + Asc(TextBox2.Text.Substring(i, 1))))
                TextBox3.Text = TextBox3.Text
& caracter
            Next
        End If

        TextBox2.Text = TextBox3.Text
        Try
            'abrir la conexion
            con.Open()
            cmd = New SqlCommand("sesion",
con)
            cmd.CommandType = 4
            With cmd.Parameters
                .AddWithValue("@nombre",
TextBox1.Text.ToString)
                .AddWithValue("@contraseña",
TextBox2.Text.ToString)
            End With
            dr = cmd.ExecuteReader
            If dr.HasRows = True Then
                MsgBox("Bienvenido....",
vbInformation)
                Alta.Visible = True
                Me.Visible = False
            Else
                MsgBox("Datos
Incorrectos...!!!", vbInformation)
                TextBox1.Text = ""
                TextBox2.Text = ""
                TextBox1.Focus()
            End If
        Catch ex As Exception :
MsgBox(ex.Message)
        End Try
        con.Close()
    End Sub
End Class
```

Conclusiones

Si duda, la encriptación es una solución apropiada para proteger los datos vulnerables, aunque no es la única, pero en el caso abordado es una oportunidad para que la empresa asegure la integridad y confiabilidad de su información y se fortalezca el proceso de toma de decisiones.

Gracias a las opciones que ofrece el campo amplio de las matemáticas, con la combinación de diferentes operaciones matemáticas, fue posible la creación de un algoritmo a la medida, para el caso de la microempresa. Esto permitió generar una solución a la medida, y sin costo alguno, a la necesidad sobre seguridad de datos que presentaba la microempresa.

Referencias

Cabrera, H. J. (2018). *Estudio comparativo de los algoritmos de encriptación Advanced Encryption Standard (AES) y Rivest, Shamir & Adleman (RSA)* (Tesis). Universidad Nacional Jorge Basadre Grohmann – Tacna. Tacna, Perú.

Cuadra, D. (2010). Desarrollo de Bases de Datos. México: alfaomega Ra-Ma.

Chmel, M. y Mužný, V. (2019). SQL Server 2019 Administrator's Guide. USA: Microsoft.

García, J. D. (2020). *Prototipo De Encriptación De Streaming De Video Mediante Python* (Tesis de grado). Universidad Tecnológica Israel. Quito, Ecuador.

Hoffen, J., Prescott, M. y McFadden, F. (2007). Modern Database Management. U.S.A.: Prentice Hall College Div.

Hoffen, J., Ramesh, V. y Topi, H. (2019). *Modern Database Management*. U.S.A.: Pearson Education.

Microsoft. (2021). *Documentación de Visual Studio*. Recuperado de https://docs.microsoft.com/es-es/visualstudio/get-started/visual-basic/?view=vs-2019

Montenegro, B. (2020). *Comparación de algoritmos de encriptación para la transferencia de archivos en mensajeria instantánea* (Tesis). Universidad Señor de Sipan. Pimentel, Perú.

Narang, R. (2011). *Database Management Systems*. Nueva Delhi: PHI Learning Private Limited.

Piattini, M., Marcos, E., Calero, C. y Vela, B. (2006). Tecnología y Diseño de Bases de Datos. México: RA-MA.

Rob, P. y Coronel, C. (2005). Sistemas de Bases de Datos. Diseño, Implementación y Administración. México: Thomson