

En la Sala de Juntas de la Dirección de Planeación, Evaluación e Información Institucional, ubicada en Avenida de las Telecomunicaciones S/N, Centro Telecomm I, Edificio "E", 2° piso, Colonia Leyes de Reforma, Código Postal 09310, Alcaldía Iztapalapa, Ciudad de México, siendo las 11:00 horas del día ocho de marzo de dos mil diecinueve, conforme a convocatoria emitida mediante oficios 5000-UT-143/2019, 5000-UT-144/2019 y 5000-UT-145/2019 de fecha 6 de marzo de 2019, se llevó a cabo la Sesión Extraordinaria número Ciento Sesenta y tres del Comité de Transparencia de Telecomunicaciones de México.

### **MIEMBROS DEL COMITÉ DE TRANSPARENCIA**

Lic. Alfonso A. Hernández Bocanegra, Director de Planeación, Evaluación e Información Institucional y Titular de la Unidad de Transparencia.

C. Guadalupe López López, Subdirectora de Recursos Materiales y Servicios Generales.

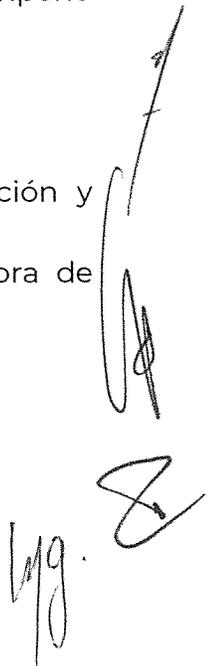
Lic. Felipe Urrutia Jiménez, Titular del Área de Auditoría Interna, en Suplencia del Titular del Área de Auditoría para el Desarrollo y Mejora de la Gestión Pública.

Lic. Mónica Vega Loza, Subdirectora de Control, Supervisión y Desempeño Institucional y Suplente del Titular de la Unidad de Transparencia.

### **INVITADOS.**

Lic. Roberto Ruiz Domínguez, Subdirector de Tecnologías de la Información y Comunicaciones.

C. María Guadalupe Guadarrama Anaya, Responsable del Área Coordinadora de Archivos en Telecomunicaciones de México.



Una vez verificado el quórum, el Licenciado Hernández Bocanegra somete a consideración de los presentes el siguiente:

### **ORDEN DEL DÍA**

1. Atención al Recurso de Revisión RRA 1933/19.

### **DESARROLLO DE LA SESIÓN.**

Una vez aprobado el Orden del Día por los Miembros del Comité, el Titular de la Unidad de Transparencia da por iniciada la sesión y se procede al desahogo de los asuntos, en los siguientes términos:

1. Atención al Recurso de Revisión RRA 1933/19.
  - a) El 14 de enero se recibió a través del Sistema INFOMEX la solicitud de información 0943700001819, que a la letra dice:

“Con fundamento en el artículo 6 constitucional, atentamente requiero que en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, me entregue a través de un medio gratuito derivado de los avances tecnológicos y en formato de documento portátil (PDF) comprimido o en diverso de naturaleza similar, la siguiente información pública documentada en ejercicio de las facultades, competencias y funciones previstas en las normas jurídicas aplicables. 1. Desglosado por numero de serie o numero de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado, nombre de los navegadores de internet que se encuentran instalados en dichos equipos de cómputo. 2. Motivos por los cuales son utilizados únicamente los navegadores de Internet a los que se haga referencia en relación al punto anterior. 3. Numero de serie o numero de parte de cada equipo de cómputo en posesión del sujeto obligado que tenga instalado el navegador de Internet denominado YANDEX BROWSER. 4. NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DE TODOS LOS PROVEEDORES DE SERVICIOS DE TELECOMUNICACIONES, ESPECIFICANDO AQUELLOS QUE PROVEAN

MG-2

ACCESO A INTERNET. 5. SERVIDORES DNS (Domain Name System) UTILIZADOS PARA EL ACCESO A INTERNET. 6. Cuáles son las redes sociales oficiales utilizadas como medios de comunicación. 7. Motivos por los cuales son utilizados únicamente las redes sociales a las que se haga referencia en el punto anterior. 8. Cuenta oficial en la red social de VK (Vkontakte). 9. Por numero de serie o numero de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado, la dirección MAC (por sus siglas en ingles Media Access Control) de cada tarjeta o adaptador de red (WIFI, BLUETOOTH, ETHERNET) de la que disponga cada equipo de cómputo". (SIC).

- b) Mediante oficios números 5000-UT-023/2019 y 5000-UT-025/2019, la Unidad de Transparencia solicitó la información a la Dirección de Administración y a la Gerencia de Innovación e Imagen Institucional en el ámbito de sus competencias.
- c) Con oficios 6400.-037/2019, y 5210-002/2019, de fecha 21 de enero de 2019, firmados por el Subdirector de Tecnologías de la Información y Comunicaciones y la Gerente de Innovación e Imagen Institucional, respectivamente, responden cada uno en el ámbito de sus competencias lo siguiente:
1. *Anexo a este documento, en CD, se envía la información en formato Excel.*
  2. *El navegador de Internet Explorer es el navegador predeterminado ya que al instalar el Sistema Operativo Windows en cualquiera de sus versiones y al ser este el nativo del sistema operativo se convierte en el navegador institucional, aunado a que este navegador permite interactuar con bibliotecas de enlace dinámico (DLL) necesarias para la operación de los servicios financieros básicos y telegráficos en sucursales telegráficas.*
  3. *El navegador Yandex Browser, no se encuentra instalado en los equipos de cómputo de la institución.*
  4. *Operbes, S.A. de C.V. y Teléfonos de México S.A.B. de C.V.*
  5. *El servidor DNS es Interno y propio de la Institución.*
  6. *Las redes sociales utilizadas por el Organismo son Facebook, Twitter e Instagram.*

7. *Se utilizan las redes sociales anteriores por considerarse las más efectivas para comunicar las actividades del Organismo y que nos pueden brindar retroalimentación de nuestros usuarios. No se utilizan otras redes ya que los contenidos que maneja Telecomm no son aplicables a esta.*
8. No se cuenta con la red social VK (Vkontakte).
9. *No es viable entregar esta información, debido a que la MAC es el identificador único de cualquier equipo de cómputo en el mundo, este dato no puede ser compartido por razones de seguridad, ya que por medio de esta información se podrían realizar acciones como suplantación de identidad, aunado a que Telecomm al ser corresponsal bancario debe garantizar la confidencialidad de la información con la que operan los servicios financieros básicos y telegráficos y es auditado por los bancos y la Comisión Nacional Bancaria y de Valores.*
- d) Con fecha 5 de febrero de 2019 a través del Sistema INFOMEX, la Unidad de Transparencia envió la información solicitada al requirente. Información que fue proporcionada por las áreas responsables de la misma.
- e) El 28 de febrero de 2019, la Unidad de Transparencia recibió a través del Sistema de Comunicaciones con los Sujetos Obligados el **Recurso de Revisión RRA 1933/19**, derivado de la solicitud de información 0943700001819, con el que el recurrente presenta las razones y motivos de su inconformidad:

"AGRAVIO PRIMERO. - Violación a la garantía de máxima publicidad de la información.

ARTÍCULOS TRANSGREDIDOS: 6° DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, 4°, 11 Y 12 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, 3° DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.

Inicialmente es oportuno señalar que por disposición del artículo 6° constitucional, el derecho fundamental de acceso a la información deberá interpretarse en función del principio de máxima publicidad. Asimismo, en atención a lo establecido en el artículo 1° constitucional y en la Ley reglamentaria del artículo 6° del mismo ordenamiento, en todo momento debe prevalecer la protección más amplia para la persona.

El principio de máxima publicidad enunciado en los artículos 11 y 12 de la Ley General de Transparencia y Acceso a la Información Pública (en lo subsecuente referida como Ley General), vincula a todo sujeto obligado a efecto de que permita el acceso y entregue todo tipo información generada, obtenida, adquirida, transformada o en su defecto se encuentre en su posesión; con exclusión de aquella que por disposición de Ley actualiza algún supuesto de excepcionalidad.

... Ahora bien, como se evidenciará a priori en las subsecuentes líneas, la clasificación de información efectuada por el sujeto obligado en atención a la solicitud 0943700001819 transgrede el principio de máxima publicidad de la información. Sin embargo, es de advertirse antes que en función de lo dispuesto en el artículo 20 de la Ley General, la carga de la prueba recae directamente sobre el sujeto obligado.

... Como se mencionó en líneas anteriores, el principio de máxima publicidad únicamente puede verse limitado por la actualización de algún supuesto previsto en el régimen de excepciones, es decir, ante la presencia de información clasificada como confidencial o reservada.

Los artículos 113 de la Ley General y 110 de la Ley Federal de Transparencia y Acceso a la Información Pública (en lo subsecuente Ley Federal) establecen que información será considerada como reservada.

... Ahora bien, la información precisada en la solicitud 0943700001819 no actualiza algún supuesto previsto en los artículos antes transcritos, tal y como lo hace aparentar la clasificación efectuada por el sujeto obligado.

Lo anterior, toda vez que lo petitionado en el numeral 9 de la solicitud 0943700001819, se trata de información que de ninguna forma compromete la seguridad nacional, la seguridad pública o la defensa nacional; y menos aún vulnerar o alterar el normal desarrollo de las funciones desempeñadas por el sujeto obligado. Sino por el contrario, son datos públicos y accesibles a cualquier persona; ya que por disposición de los artículos 68 de la Ley Federal y 70 fracción XXXIV de la Ley General, estos deben formar parte del inventario de los bienes muebles en posesión o propiedad el sujeto obligado.

... La divulgación de la dirección MAC de cada tarjeta o adaptador de red, de ninguna manera debe vulnerar o interrumpir el normal desarrollo de las atribuciones encomendadas al sujeto obligado; esto puesto que el sujeto obligado debe contar con diversas herramientas o medios (programas informáticos) que le permitan hacer frente a cualquier ataque cibernético, intentado a partir de las direcciones MAC requeridas.

Además, resulta ilógico que al publicitar la dirección MAC de cada tarjeta o adaptador de red, dato con el que cuenta tanto el fabricante del equipo de cómputo, el fabricante de la tarjeta o adaptador de red, y que incluso puede conocer el proveedor del servicio de acceso a Internet, se vean vulneradas o interrumpidas las funciones y actividades desempeñadas por el sujeto obligado, y en última instancia la seguridad pública.

En suma, la clasificación efectuada por el sujeto obligado resulta violatoria del principio de máxima publicidad, y en última instancia del derecho fundamental de acceso a la información reconocido constitucional y convencionalmente en beneficio del hoy recurrente; ya que como se argumentó en líneas anteriores, lo requerido en la solicitud 0943700001819 no actualiza algún supuesto de reservada previsto en la Ley Federal o en la Ley General.

AGRAVIO SEGUNDO.- Falta de notificación de la Resolución del Comité de Transparencia, por la cual se clasifico la información requerida.

ARTÍCULOS TRANSGREDIDOS: 137, EN RELACIÓN CON EL 132 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, 140 EN RELACIÓN CON EL 135 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.

... Ahora bien, en contravención a los preceptos jurídicos antes citados, el sujeto obligado omite notificarme la resolución signada por cada uno de los integrantes del Comité de Transparencia, a través de la cual se clasifico la información requerida en la solicitud 0943700001819." (SIC)

- f) Con oficio 5000-UT-111/2019 de fecha 28 de febrero de 2019, El Titular de la Unidad de Transparencia solicita al Titular de la Dirección de Administración ratificar o rectificar la respuesta del oficio número 6400-037/2019, de fecha 21 de enero del presente emitida por el Subdirector de Tecnologías de la Información y Comunicaciones.
- g) Con oficio 6000.-0239/19, de fecha 4 de marzo de 2019, el Titular de la Dirección de Administración responde lo siguiente:

***"Al respecto, ratifico que no es viable entregar la información requerida, debido a que la MAC es el identificador único de cualquier equipo de cómputo en el mundo, este dato no puede ser compartido por razones de seguridad, ya que por medio de esta información se podrían realizar acciones como suplantación de identidad, aunado a que Telecomm al ser corresponsal bancario debe garantizar la confidencialidad de la información con la que operan los servicios financieros***

*básicos y telegráficos y es auditado por los bancos y la Comisión Nacional Bancaria y de Valores.” (SIC)*

*Asimismo, el Director de Administración envía documento con el que motiva porqué esta información debe ser considerada como Reservada.*

## **Relevancia de la MAC Address en Telecomm**

### **¿Qué es la MAC Address o Dirección MAC?**

Es un Identificador único asignado a las tarjetas de la red de los dispositivos electrónicos que accesan a una red de datos o al mismo Internet, dicho identificador es asignado por el fabricante de las mismas; al ser un identificador único es imposible encontrar dos dispositivos con la misma MAC en el mundo, sin embargo, eso no quiere decir que ésta no pueda ser duplicada en otra tarjeta de red por medio de procedimientos que afectan la memoria RAM en la que ésta fue grabada, a esta técnica se le conoce como MAC Spoofing.

Una analogía clara a la definición anterior es el caso de la Credencial de Elector, la cual es única para cada uno de los Ciudadanos mayores de 18 años, sin embargo, alguna persona con fines maliciosos puede clonar la identificación y utilizarla como si fuera la credencial original.

### **¿Cómo puede afectar a Telecomm el exponer o entregar a terceros la Dirección MAC?**

Hoy en día Telecomm cuenta con controles de seguridad implementados para el uso del Sistema SIGITEL, estos controles atienden las diversas regulaciones establecidas por la Comisión Nacional Bancaria y de Valores para la operación de corresponsalía bancaria y para la operación de remesas nacionales e internacionales; el sistema SIGITEL identifica la Dirección MAC de cada uno de los equipos de cómputo de la red de Sucursales Telegráficas y la asocia a cada uno de los operadores, de esta manera identifica si el equipo de cómputo o el operador son válidos para la operación del Sistema.

Exponer o entregar el listado de las direcciones MAC de cada uno de los equipos puede ser utilizada para hacer pasar un equipo de cómputo externo como un equipo válido para la operación del Sistema SIGITEL por medio de MAC Spoofing, por citar solo un ejemplo, entre otros casos puede ser utilizada para evadir el filtrado MAC en los equipos de seguridad de red perimetral y de esta manera puedan acceder a la red de datos interna como un equipo de confianza.

*Wg* 7

### **Cómo prevenir intentos de ataque informático?**

Uno de los factores más importantes para evitar ser blanco de ataques informáticos, y más aún, que estos se ejecuten de forma exitosa, es la discreción del personal en el uso de la información a la que tiene acceso por sus actividades, así como evitar la divulgación de los controles de seguridad que se tienen implementados y la de los activos informáticos, ya que de lo contrario es abrirle la puerta a cualquier persona o institución mal intencionada para que esta pueda ejecutar un ataque.

- h) En alcance al oficio número 6400.-0037/2019, de fecha 21 de enero del 2019, El Subdirector de Tecnologías de la Información y Comunicaciones mediante oficio número 6400-0203/2019, de fecha 7 de marzo del presente, realiza las siguientes precisiones:

En relación con la prueba de daño con respecto a la información considerada como reservada, la cual tiene fundamento en los artículos 110 Fracciones IV y VII y 113, Fracciones I y II de la Ley Federal de Transparencia y Acceso a la Información Pública, si bien a través del derecho de acceso a la información cualquier persona puede tener acceso a la información en posesión de los sujetos obligados, existen restricciones al respecto, mismas que se refieren a la información reservada. Por lo que en cumplimiento al Artículo 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, a continuación, se fundamenta y motiva, través de la aplicación de la prueba de daño, la solicitud de clasificación como información reservada, por un plazo de cinco años, de los datos correspondientes a las direcciones MAC de los equipos de cómputo en posesión de Telecomunicaciones de México.

Por cuestiones de seguridad de la información de la institución (confidencialidad, disponibilidad e integridad), la información del direccionamiento MAC no puede ser entregada o hacerse del conocimiento de terceros, ya que esta forma parte de las configuraciones internas de la Institución, aunado a que esta información no contribuye a la transparencia ni a la rendición de cuentas, pues no documentan la gestión pública.

Es deber de la Institución salvaguardar la seguridad de la información que se genera, procesa, transmite y almacena derivado de las actividades sustantivas de esta, por medio de la implementación de controles de seguridad de la información, entregar esta información potencializa el riesgo de que los equipos conectados a la red de datos interna sean vulnerados a partir de la

ejecución de ataques cibernéticos, basados en Spoofing, ARP Spoofing, Suplantación de dirección IP y Ataque de fuerza bruta, solo por citar algunas de las técnicas utilizadas por delincuentes cibernéticos y grupos hacktivistas; los cuales han ido en aumento a nivel global y muchas veces los blancos principales son las Instituciones de la Administración Pública Federal.

No se omite señalar que Telecomunicaciones de México tiene dentro de sus actividades sustantivas la operación de servicios operados a nombre y por cuenta de terceros y ser trasmisor de dinero autorizado por la Comisión Nacional Bancaria y de Valores, por lo que Telecomunicaciones de México, maneja información de datos personales, razón por la que exponer la dirección MAC de los equipos no se considera viable, toda vez que esto revela información de los equipos de cómputo que se encuentran conectados a la red de datos interna, los cuales podrían ser atacados para afectar la seguridad de la información.

De acuerdo con el principio de proporcionalidad, se concluye que la afectación que podría traer la divulgación de las direcciones MAC, es mayor que el interés público de que se difundan, por lo que se considera que en este caso debe prevalecer la reserva, por cinco años, de las direcciones MAC de los equipos de cómputo de Telecomunicaciones de México.

A su vez, el artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública, respecto de la información que puede clasificarse como reservada, en sus fracciones IV y VII de la establece que:

IV. Pueda afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pueda poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, pueda comprometer la seguridad en la provisión de moneda nacional al país, o pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal;

VII. Obstruya la prevención o persecución de los delitos;

En relación con lo anterior, en el capítulo II "Acceso ilícito a sistemas y equipos de informática" del Código Penal Federal dispone lo siguiente:

mg 9

Artículo 211 Bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días de multa.

Al que sin autorización conozca o copie Información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días de multa

Artículo 211 Bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos informáticos del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días de multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado; protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientas días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 Bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

En este sentido, revelar las direcciones MAC de los equipos de cómputo permitiría que terceros contarán con elementos para intentar algún tipo de ataque cibernético para ingresar, sin autorización, a todos y cada uno de los equipos de cómputo de Telecomunicaciones de México. No se omite señalar que Telecomunicaciones de México tiene dentro de sus actividades

sustantivas la operación de servicios operados a nombre y por cuenta de terceros, es un transmisor de dinero, por lo que se aplica el último párrafo del Artículo 95 Bis del Capítulo II “de los delitos” de la Ley General de Organizaciones y Actividades Auxiliares de Crédito, que a la letra dice:

Los servidores públicos de la Secretaría de Hacienda y Crédito Público y el Servicio de Administración Tributaria, las sociedades financieras de objeto múltiple, las personas que realicen las actividades a que se refiere el artículo 81-A y los transmisores de dinero, sus miembros del consejo de administración, administradores, directivos, funcionarios, empleados, factores y apoderados, deberán abstenerse de dar noticia de los reportes y demás documentación e información a que se refiere este artículo, a personas o autoridades distintas a las facultadas expresamente en los ordenamientos relativos para requerir, recibir o conservar tal documentación e información. La violación a estas obligaciones será sancionada en los términos de las leyes correspondientes.)

Por lo anteriormente expuesto, se concluye que la información es reservada con fundamento en los artículos 110 fracciones IV y VII, 113 fracciones I y II de la Ley Federal de Transparencia y Acceso a la Información Pública y del Artículo 95 Bis del Capítulo II “de los delitos” de la Ley General de Organizaciones y Actividades Auxiliares de Crédito.

Una vez desahogado el tema a tratar por el Comité, se emite el siguiente:

**ACUERDO**

**163.1** Con fundamento en el Art. 65, Fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública, el Comité de Transparencia de Telecomunicaciones de México confirma por unanimidad en términos de los Artículos 110 Fracciones IV y VII y 113, Fracciones I y II de la misma Ley, así como del Artículo 95 Bis del Capítulo II “de los delitos” de la Ley General de Organizaciones y Actividades Auxiliares de Crédito, la clasificación de reserva por un periodo de 5 años para el resguardo de la confidencialidad de la información que contiene la red de datos de Telecomunicaciones de México, la que administra y transmite información relativa a datos personales y servicios que se operan a cuenta y nombre de terceros, de instituciones financieras, transmisores de dinero, instancias de seguridad nacional e información relativa a la prevención o persecución de probables faltas

administrativas, lo que corresponde al punto 9 de la solicitud de información número 0943700001819, referente al número de serie o número de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado, la dirección MAC (por sus siglas en inglés Media Access Control) de cada tarjeta o adaptador de red (WIFI, BLUETOOTH, ETHERNET) de la que disponga cada equipo de cómputo.

Al no haber más asuntos por tratar, se da por concluida la Sesión Extraordinaria número 163 del Comité de Transparencia de Telecomunicaciones de México, siendo las 13:20 horas del día de su inicio, firmando al calce los que en ella intervinieron.

Titular de la Unidad de Transparencia

LIC. ALFONSO A. HERNÁNDEZ BOCANEGRA

Titular del Área de Auditoría Interna, en  
Suplencia del Titular del Área de Auditoría  
para el Desarrollo y Mejora de la Gestión  
Pública

LIC. FELIPE URRUTIA JIMENÉZ

Subdirector de Tecnologías de la  
Información y Comunicaciones

LIC. ROBERTO RUIZ DOMINGUEZ

Subdirectora de Recursos Materiales y  
Servicios Generales y Miembro del Comité  
de Transparencia

C. GUADALUPE LOPEZ LÓPEZ

Subdirectora de Control, Supervisión y  
Desempeño Institucional y Suplente del  
Titular de la Unidad de Transparencia

LIC. MÓNICA VEGA LOZA

Responsable del Área Coordinadora de  
Archivos

MARÍA GUADALUPE GUADARRAMA ANAYA