ACUSE

COMUNICACIONES

Telecomm. TELECOMUNICACIONES DE MÉXICO

130 AÑOS SECRETARÍA DE COMUNICACIONES Y TRANSPORTES

México 2021 Año de la Independencia

SECRETARÍA DE COMUNICACIONES Y TRANSPORTES
TELECOMM TELEGRAFOS
DIRECCIÓN TÉCNICA
SUBDIRECCIÓN DE SISTEMAS DE INFORMÁTICA
19 MAR 2021
12:34 hrs
GERENCIA DE CENTROS DE COMPUTO Y EQUIPAMIENTO INFORMÁTICO

Dirección de la Red de Sucursales
Subdirección de procesos de Supervisión
Gerencia de Implementación de procesos de Servicios
OF.- 4120 / CNSD019 / 2021
Ciudad de México, a 18 de marzo del 2021

GRENTES ESTATALES Y REGIONALES
Presente

En atención al oficio No. 64000/171/2021, enviado el día 03 de marzo del 2021, por la Subdirección de tecnología de la Información y Comunicaciones, derivado de la auditoria que realizo el banco Santander a TELECOMM con respecto al siguiente hallazgo:

ID	hallazgos	Actividades
81569	Corrección de fallas identificadas en la operación de sucursales: - Falla de seguridad en los equipos de las sucursales y las operaciones realizadas por corresponsales.	2.- Deshabilitar las teclas que permiten un dispositivo de Booteo diferente al predeterminado desde BIOS y Configurar una contraseña segura para que solo los administradores o personal autorizado tengan acceso a este sistema. 3.- Configurar las sesiones en las que trabajan los operadores de la oficinas Telegráficas como un Usuario sin Privilegios, quitando todos los permisos para realizar cambios en el equipo, instalar o desinstalar aplicativos de cualquier tipo.

Con respecto a la especificación del punto 3 el cual corresponde al aplicativo denominado SymetryBus, el cual permite la comunicación a la plataforma del SIGITEL y los Dispositivos PinPad, usados en las sucursales Telegráficas para la operación del día a día.
Al respeto le comento, este aplicativo requería de privilegios como administrador para el correcto funcionamiento. Sin embargo, derivado del hallazgo identificado por los auditores de Santander, se generó un procedimiento(manual) que se anexa para revocar esto privilegios.
Por lo anterior solicito girar sus apreciables instrucciones a quien corresponda para que se genere y entregue un calendario de aplicación del procedimiento a todos los equipos de ventanilla de la Red de Sucursales Telegráficas, para realizar las actividades 2 y 3 que se entregarán a la Gerencia de Seguridad Informática y Comunicaciones para poder cerrar el hallazgo de manera satisfactoria
Sin otro particular, aprovecho la oportunidad para enviarle un cordial.

Atentamente

C.P. Alejandro López Carranza.
Gerente de Implementación de Procesos de Servicios.

Telecomm. TELECOMUNICACIONES DE MÉXICO
RECIBIDO
FIRMA 19 MAR 2021 12:37 HORA
GERENCIA DE CENTROS DE COMPUTO Y EQ. INF
SUBDIRECCIÓN DE BIENES INFORMÁTICOS

RECIBIDO 19 MAR 2021 11:0

RECIBIDO
FIRMA 19 MAR 2021 12:16 HORA
SUBDIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

C. c. p. Maestra Ma. del Carmen Moncada Soto. - Subdirectora.
Rafael Balboa Bravo. - Subdirector de Tecnología de Información y Comunicaciones.
C. Anselmo Alvarado Resendiz. - Gerente de Centros de Cómputo y Equipamiento Informático,
Lic. Jose Gerardo Villela Valencia. -Coordinador de Bienes Informáticos

ALC/gmp

Centro TELECOMM | Av. de las Telecomunicaciones [illegible]
Alcaldía Iztapalapa, CDMX.

Dot 229

COMUNICACIONES
SECRETARÍA DE COMUNICACIONES Y TRANSPORTES | Telecomm. TELECOMUNICACIONES DE MÉXICO | 130 AÑOS

Dirección de Administración
Subdirección de Tecnologías de la Información y Comunicaciones
OF.- 6400.- 171/2021

Ciudad de México, a 3 de marzo del 2021

Dr. Edgar Horacio Esquivel Martínez
Director de la Red sucursales
Presente

Derivado de la Auditoria realizada por Banco Santander a Telecomm y en especifico a la Red de Sucursales, a continuación, se describe el hallazgo identificado.

ID	Hallazgos	Actividades
81569	Corrección de fallas identificadas en la operación de sucursales: -Fallas de seguridad en los equipos de las sucursales y las operaciones realizadas por corresponsales	2. Deshabilitar las teclas que permiten seleccionar un dispositivo de booteo diferente al predeterminado desde BIOS y configurar una contraseña segura para éste para que solo los administradores o personal autorizado tengan acceso a este sistema. 3. Configurar las sesiones en las que trabajan los operadores de las oficinas telegráficas como un usuario sin privilegios, quitando todos los permisos para realizar cambios en el equipo, instalar o desinstalar aplicativos de cualquier tipo

Con base a lo anterior y en específico al punto numero 3 el cual corresponde al aplicativo denominado SymetryBus, el cual permite la comunicación de la plataforma SIGITEL y los dispositivos Pinpad, usados en las sucursales telegrafiadas para la prestación de servicios y operaciones diarias, comento a usted que anteriormente dicho aplicativo requería privilegios elevado como administrador para su correcto funcionamiento, sin embargo y derivado del hallazgo identificado se realizaron pruebas en la Ventanilla de Centro Telecomm II, al igual que se elaboró un procedimiento incluido como anexo para revocar estos privilegios, entre la Gerencia de Seguridad en Informática y Comunicaciones y personal Técnico de la Gerencia de la Ciudad de México

Recibí.
10.03.21
10:00
Recibí original para las Direcciones de la Red de Sucursales
13:15

México 2021 Año de la Independencia

TELÉGRAFOS
Telecomm

Dirección de Administración
Subdirección de Tecnologías de la Información y Comunicaciones
Gerencia de Seguridad en Informática y Comunicaciones

MANUAL DE CONFIGURACIÓN DE SYMETRYBUS EN CUENTAS DE USUARIOS LIMITADOS

27 de enero de 2020

A continuación, se enlistan los pasos para la configuración de SymetryBus en cuentas de usuarios limitados al igual que el arranque automático en el inicio de sesión.

Asignar privilegios de administrador para ejecución de SymetryBus.

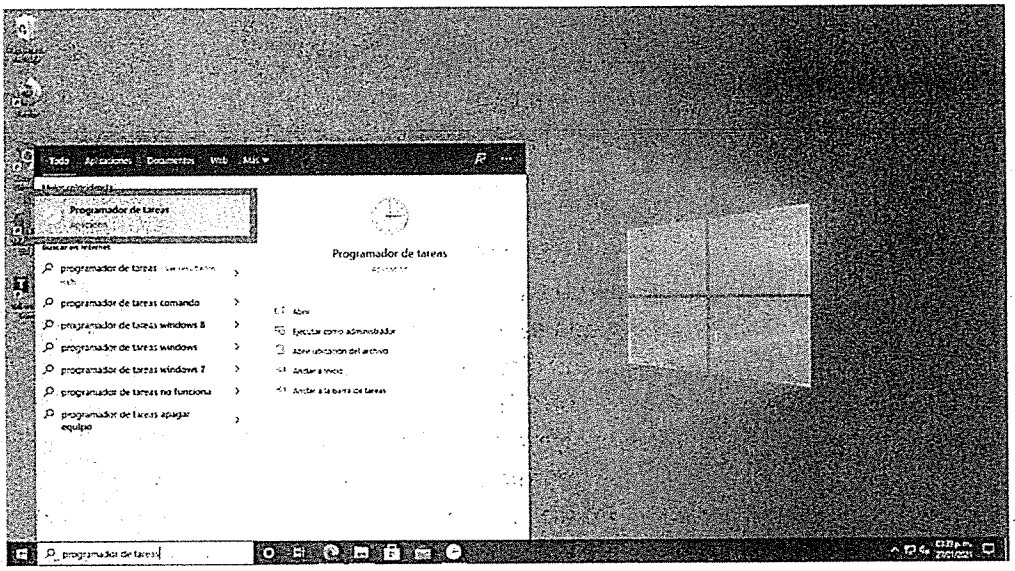
1. Iniciar sesión en el equipo con alguna cuenta con privilegios de administrador.
2. Habilitar la cuenta "Administrador" del sistema.
3. Establecer una contraseña robusta a la cuenta "Administrador":
    a. Usar 8 caracteres como mínimo.
    b. Alfanumérica.
    c. Al menos una letra mayúscula.
    d. Al menos un caracter especial (Ej. *.-_+/).
4. Cerrar la sesión del sistema donde se encuentre.
5. Crear y/o Iniciar la sesión del usuario limitado.
6. Generar un acceso directo en escritorio a SymetryBusTelecomm.exe (la ruta habitual es: C:\SymetryBusTelecomm\SymetryBusTelecomm.exe).
7. Abrir las propiedades del acceso directo.
8. En la pestaña "Acceso directo" en el campo "Destino" insertar lo siguiente: C:\Windows\System32\runas.exe /user:Administrador /savecard C:\SymetryBusTelecomm\SymetryBusTelecomm.exe
9. Abrir el acceso directo.
10. En la ventana CMD teclear la contraseña establecida para la cuenta "Administrador" y presionar enter.
11. Verificar que SymetryBus esté en ejecución.

Nota1: Los pasos 6,7, 8 y 9 se pueden omitir ejecutando la siguiente instrucción desde una ventana CMD:
runas /user:Administrador /savecard C:\SymetryBusTelecomm\SymetryBusTelecomm.exe

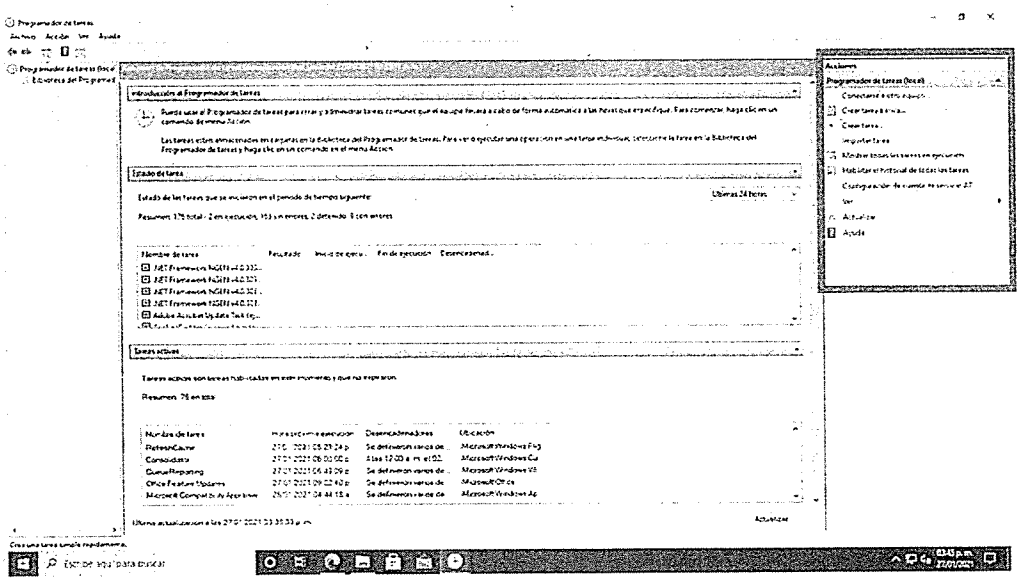
Nota2: Todas las sesiones de usuarios de los equipos deben de contar con inicio de sesión protegido por contraseñas seguras (debe de contar con 8 caracteres como mínimo, Alfanumérica, Al menos una letra mayúscula, Al menos un caracter especial).

Crear tarea para ejecutar SymetryBusTelecomm.exe en el arranque del usuario limitado:

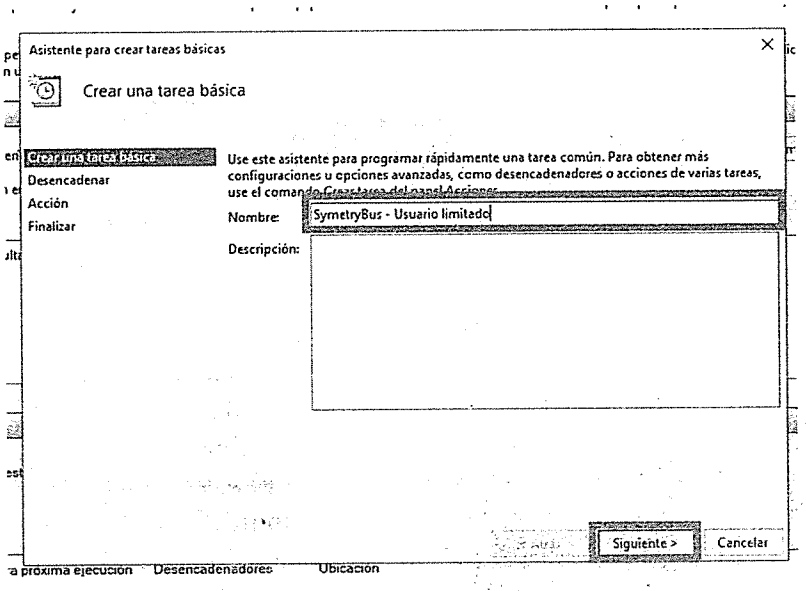
1. Iniciar sesión en la cuenta de usuario limitado.
2. Abrir "Programador de tareas".



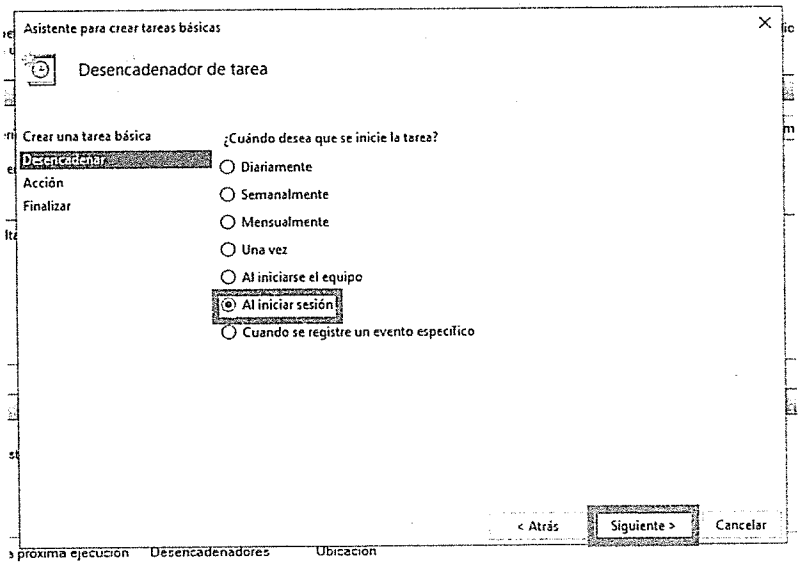
3. En la sección "Acciones" al lado derecho seleccionar "Crear tarea básica..."



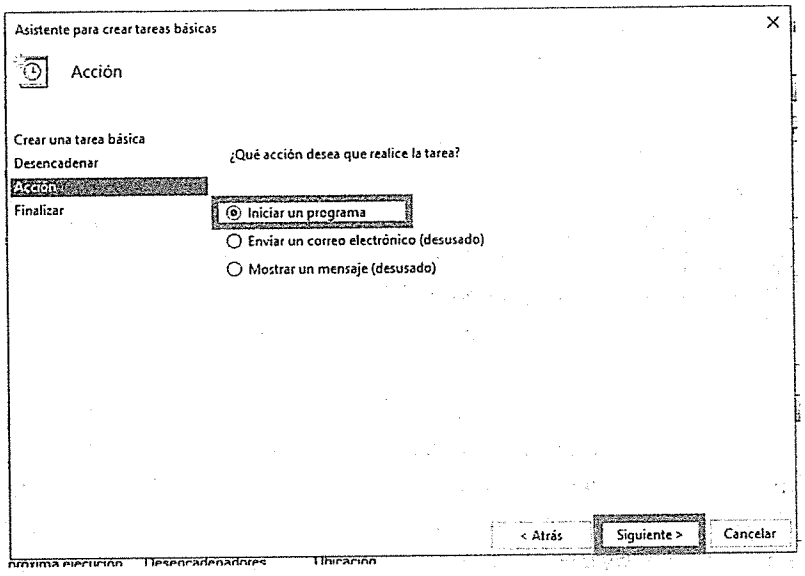
4. En el campo "Nombre" teclear el nombre que se desee para la tarea y dar clic en el botón "Siguiente".



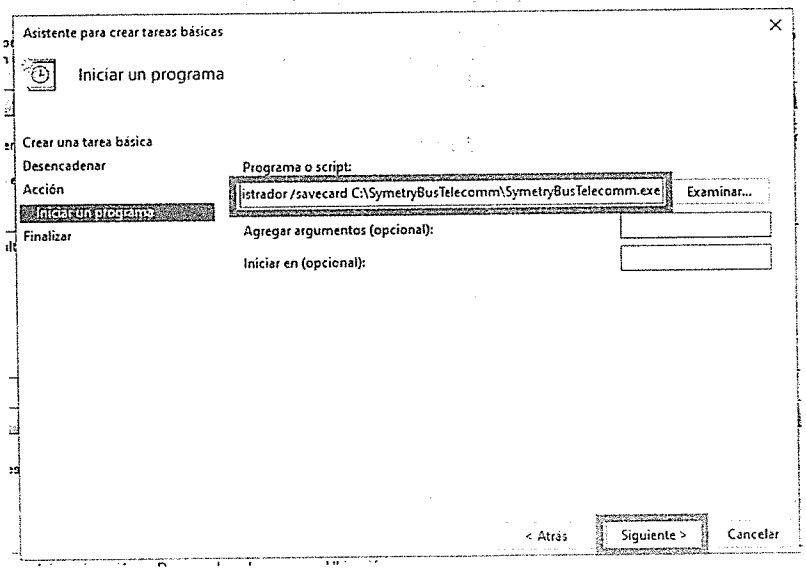
5. En la sección "Desencadenador de tarea" seleccionar "Al iniciar sesión" y dar clic en el botón "Siguiente".



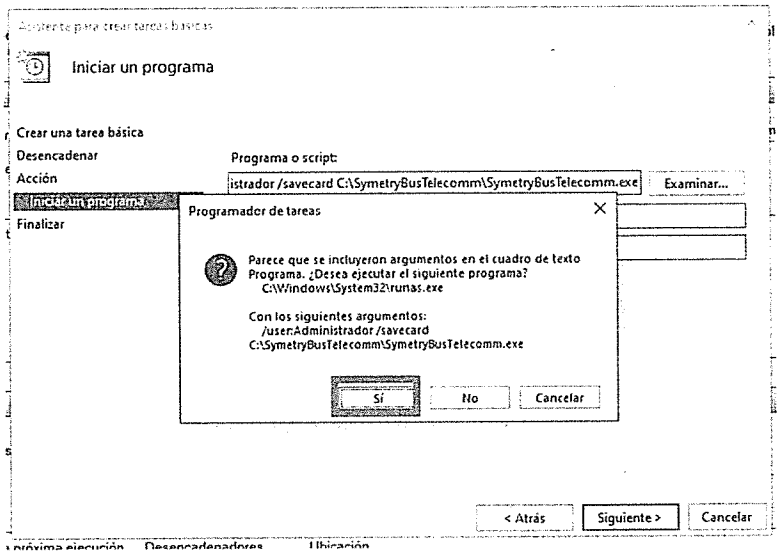
6. En la sección "Acción" seleccionar "Iniciar un programa" y dar clic en el botón "Siguiente".



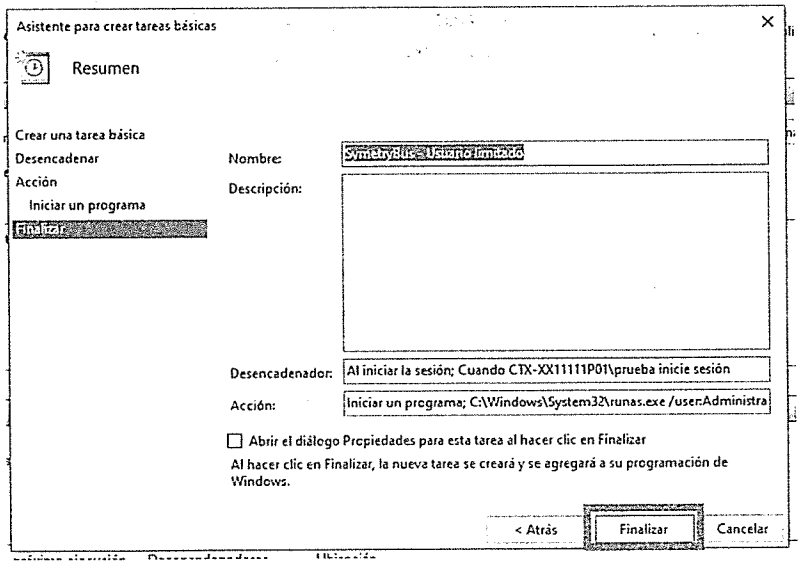
7. En la sección "Iniciar un programa" en el campo "Programa o script" teclear la siguiente instrucción: **C:\Windows\System32\runas.exe /user:Administrador /savecard C:\SymetryBusTelecomm\SymetryBusTelecomm.exe** y dar clic en el botón "Siguiente".



8. En la ventana emergente de confirmación dar clic en el botón "Sí".



9. Dar clic en el botón "Finalizar".



10. Reiniciar el equipo de computo.
11. Iniciar sesión en la cuenta de usuario limitado.
12. Verificar que SymetryBus se encuentre ejecutando.