LOGICALIS
Architects of Change

Informe Técnico Contrato de Soporte

Confeccionado por Logicalis para la

Secretaría de Prevención del Lavado de Dinero o Bienes

Periodo 01/10/24 al 31/10/24

SECRETARÍA DE
PREVENCIÓN DE LAVADO DE DINERO O BIENES
UIF - UNIDAD DE INTELIGENCIA FINANCIERA

Alvaro León Silvano
Director de Infraestructura
SEPRELAD

Logicalis Paraguay S.A.
Av. Santa Teresa.
Torre 1 del Paseo La Galeria Piso 15
Asunción - Paraguay
Tel: +595 (21) 695636
Fax: +595 (21) 695636
www.la.logicalis.com

cesar miñarro
Logicalis Paraguay S.A.

LOGICALIS
Architects of Change

Contenidos

Sección 1. Objetivo 3
Sección 2. Actividades Realizadas. 4
Sección 3. Total de Horas 9
Sección 4. Conclusion 10

Logicalis Paraguay S.A.

Sección 1. Objetivo

El presente documento es redactado para dar a conocer detalles de las actividades realizadas en la Secretaría de Prevención del Lavado de Dinero o Bienes.

Describir:

1. Las actividades realizadas en el periodo indicado más arriba.

Logicalis Paraguay S.A.

Sección 2. Actividades Realizadas.

Identificador de Pedido: RITM1628341
Inicio: 07-10-2024 hora inicio 11:00 hs **Fin: 07-10-2024** hora fin: 13:00 hs
Descripción de la Solicitud: Realización de modificaciones en el servidor de correos Exchange
Solicitante: Alvaro León aleon@seprelad.gov.py>
Ingeniero asignado: Cesar Miñarro

En fecha 7/10/24

El servidor de correos Exchange no está enviando correos con TLS (Transport Layer Security) y esto está causando problemas de comunicación con otras entidades, como el Ministerio de Relaciones Exteriores.

Procesos realizados:

- Verificar la configuración de TLS en Exchange:
  Se verifica que está correctamente habilitado en los Conectores de recepción de Exchange. Todos los conectores creados cuentan con la opción TLS Habilitada.
- Actualizar certificados y configuraciones:
  Se verifica que los certificados SSL/TLS instalados en el servidor de Exchange estan actualizados y correctamente configurados.
- Registro de errores y logs:
  Se verifica los logs de transporte de Exchange para identificar errores relacionados con TLS, posterior a pruebas tomadas de envio de mails tanto interno como cuentas externas, no demostraba error en los logs. Identificador presentado *"A forced configuration update for Microsoft.Exchange.Transport.AcceptedDomainTable has successfully"*

Testing y Updates

- Se realizan testeos de envio y recepción de correos entre mails externos (cesar.minarro@la.logicalis.com ; cesarminarroz@gmail.com, aleon@seprelad.gov.py y administrator@seprelad.com.py) las recepciones y envíos se realizaron en 1 ocasión tuvo un tiempo de espera de 4 minutos.
- Reiniciaron servicios de TLS
  Servicio de Transporte de Microsoft Exchange (**MSExchangeTransport**): Este servicio maneja el flujo de correos entre servidores y garantiza que los correos se envíen a través de conexiones seguras con TLS.
  Reinicio: Reiniciar este servicio puede resolver problemas de conexión en el flujo de correo que involucre TLS.

  Servicio de FrontEnd de Microsoft Exchange (**MSExchangeFrontEndTransport**): Gestiona las conexiones SMTP entrantes y salientes en el servidor de Exchange y también es responsable de aplicar TLS en estas conexiones.
  Reinicio: Puede solucionar problemas de TLS en el flujo de correos.

Logicalis Paraguay S.A.

Posterior a lo modificado se realiza monitoreo de los envíos y recepción de correos, a **Hoy** por lo comentado por el Sr Alvaro **el inconveniente persiste**.
Se agenda sesión de reconfiguración de conector de envíos Miércoles 09/10/24 a las 9:00hs

Se procederá a realizar el forzado de utilización de TLS en conectores de envió.
Set-SendConnector -Identity "NombreConector" -RequireTLS $true
Get-SendConnector -Identity "NombreConector" | Format-List RequireTLS

Horas utilizadas: 2 horas (dos horas)

Estado Solicitud: Finalizado.

Obs: Las horas utilizadas en esta asistencia corresponden al BANCO_HORAS_SEPRELAD_OV998_SOPORTE_MICROSOFT

Identificador de Pedido: **RITM1628341**

Inicio: 09-10-2024 hora inicio 09:00 hs

Fin: 09-10-2024 hora fin: 12:00 hs

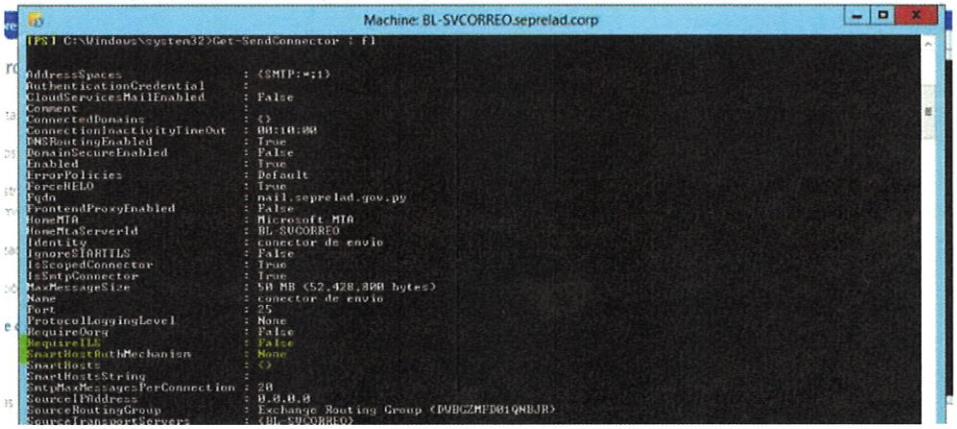
Descripción de la Solicitud: Solicitud de soporte técnico

Solicitante: Alvaro León aleon@seprelad.gov.py>

Ingeniero asignado: Cesar Miñarro

Según lo agendado y coordinado se procedió a la verificación del uso del TLS en los conectores de envío, a continuación los procedimientos realizados.

- Se verifica que el uso del TLS para el conector de envío se encontraba inhabilitado: Estado -> False



- Se procede a ejecutar el comando de solicitud de activación del protocolo TLS al conector de envio.

- Se ejecuta comando de verificación que muestre el cambio de estado del TLS.

Logicalis Paraguay S.A.

```
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>Get-SendConnector -Identity "conector de envio" | Format-List *

[PS] C:\Windows\system32>Get-SendConnector -Identity "conector de envio" | Format-List RequireTLS

RequireTLS : True

[PS] C:\Windows\system32>_
```

- Se observa luego de la aplicación de los comandos por PowerShell el estado de **RequireTLS** se encuentra en **True**

```
Machine: BL-SVCORREO.seprelad.corp

[PS] C:\Windows\system32>Get-SendConnector | fl

AddressSpaces                : {SMTP:*;1}
AuthenticationCredential     :
CloudServicesMailEnabled     : False
Comment                      :
ConnectedDomains             : {}
ConnectionInactivityTimeOut  : 00:10:00
DNSRoutingEnabled            : True
DomainSecureEnabled          : False
Enabled                      : True
ErrorPolicies                : Default
ForceHELO                    : True
Fqdn                         : mail.seprelad.gov.py
FrontendProxyEnabled         : False
HomeMTA                      : Microsoft MTA
HomeMtaServerId              : BL-SVCORREO
Identity                     : conector de envio
IgnoreSTARTTLS               : False
IsScopedConnector            : True
IsSmtpConnector              : True
MaxMessageSize               : 50 MB (52,428,800 bytes)
Name                         : conector de envio
Port                         : 25
ProtocolLoggingLevel         : None
RequireOorg                  : False
RequireTLS                   : True
SmartHostAuthMechanism       : None
SmartHosts                   : {}
```

- De igual manera se procedió a generar un nuevo conector exclusivo para Gmail con las siguientes especificaciones.

  Configuración del Conector
  Nombre: "Gmail TLS Connector".
  Tipo de Conector: Internet.
  Smart Hosts: gmail-smtp-in.l.google.com
  Dominio: Gmail.com

Queue Viewer - BL-SVCORREO.seprelad.corp

Queues | Messages | gmail.com

Create Filter

Next Hop Domain	Delivery Type	Status	Message Count
bourbon.com.py	DnsConnectorDelivery	Listo	2
db01	Entrega SMTP a buzón	Listo	0
gmail-smtp-in.l.googl...	SmartHostConnectorDelivery	Listo	0

- Resultado del comando Test-Mailflow luego de las actualizaciones en conectores.

```
[PS] C:\Windows\system32>Test-Mailflow

RunspaceId          : 959ade7e-1191-45ae-bdcc-52e411c60b43
TestMailflowResult  : Success
MessageLatencyTime  : 00:00:01.5331392
IsRemoteTest        : False
Identity            :
IsValid             : True
ObjectState         : New
```

Mensaje:
testMailflowResult: Success
IsRemoteTest: false
Identity: (no especificado)
IsValid: True
ObjectState: New

Logicalis Paraguay S.A.