



INC-01194-W1K1

# ALERTA DE SEGURIDAD



**CSIRT-RD**

Equipo Nacional de Respuestas a Incidentes  
Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 27 DE ENERO 2021

© Todos los derechos reservados





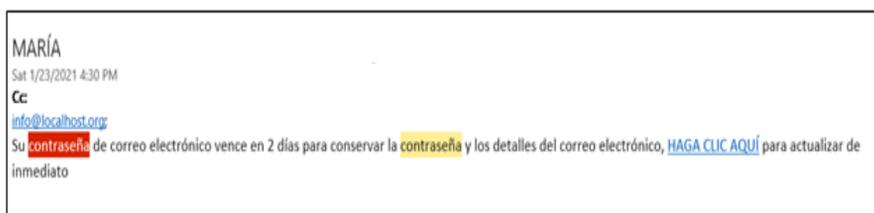
El presente documento es propiedad del Centro Nacional de Ciberseguridad (CNCS), y fue generado mediante el análisis de varias fuentes de terceras partes y una investigación del equipo CSIRT-RD.

## ALERTA DE SEGURIDAD

- ID INC-01194-W1K1
- TLP Blanco
- Tipo de incidente Ingeniería Social
- Categoría Robo de Información
- Fecha de incidente 19 de Enero 2021
- Fecha de reporte 26 de Enero 2021
- Nivel de peligrosidad **ALTO**

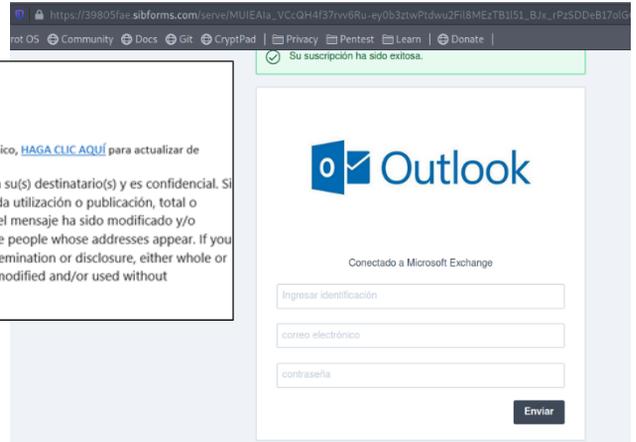
## DETALLES DE ALERTA

El Equipo Nacional de Respuesta a Incidentes CSIRT- RD ha recibido una notificación relacionada a una campaña de phishing que hace referencia a un enlace para realizar el **registro de credenciales** a los usuarios indicado que la contraseña de correo esta **próxima a vencer** y que requiere cambio.



ARATH i  
 Fri 1/22/2021 9:47 AM  
 Cc:  
 info@localhost.org  
 Su contraseña de correo electrónico vence en 2 días para conservar la contraseña y los detalles del correo electrónico, [HAGA CLIC AQUÍ](#) para actualizar de inmediato  
 \*\*\*\*\*Este mensaje (y sus adjuntos), en adelante "mensaje", ha sido enviado exclusivamente a su(s) destinatario(s) y es confidencial. Si usted recibe este mensaje por error, por favor bórralo y comuníquese inmediatamente al remitente. Toda utilización o publicación, total o parcial, queda prohibida salvo autorización expresa. La UTP no podrá ser considerada responsable si el mensaje ha sido modificado y/o utilizado sin autorización. This message (and any attachments), are confidential intended solely for the people whose addresses appear. If you have received this message by error, please delete it and immediately notify the sender. Any use, dissemination or disclosure, either whole or partial, without formal approval is prohibited. The UTP will not therefore be liable for the message if modified and/or used without approval.\*\*\*\*\*

Muestra de variante del correo de suplantación de identidad.



Suplantación de portal de credenciales de Outlook para verificar y cambio de contraseña.

## INDICADORES DE COMPROMISO (IoC)

### Conexiones

- 104[.]18[.]174[.]17

### Soluciones de Dominio DNS

- c8679251[.]sibforms[.]com
- 39805fae[.]sibforms[.]com
- f17ca927[.]sibforms[.]com

### Peticiones HTTP

- [https://f17ca927\[.\]sibforms.com/serve/MUIEAFrh8U0eVUP-zsY7FZA3Yx7rEp9xVSV-UmsHgZ2zX9n4PT3kmDb-pmAWvtVv29sfU08amkyz7D496QdoOBm4wYUAsfMjK9KmThagc8uHhRSKsCQmAS98qRpDt1iLgNBrJEAwWySO\\_724iyAkqY7FAKUNt6XlCh77nO4SXbcBlaO\\_bQjkU-e7H0pCgntxtiunfadBzey6iepq](https://f17ca927[.]sibforms.com/serve/MUIEAFrh8U0eVUP-zsY7FZA3Yx7rEp9xVSV-UmsHgZ2zX9n4PT3kmDb-pmAWvtVv29sfU08amkyz7D496QdoOBm4wYUAsfMjK9KmThagc8uHhRSKsCQmAS98qRpDt1iLgNBrJEAwWySO_724iyAkqY7FAKUNt6XlCh77nO4SXbcBlaO_bQjkU-e7H0pCgntxtiunfadBzey6iepq)
- [https://39805fae\[.\]sibforms\[.\]com/serve/MUIEAla\\_VCcQH4f37rvv6Ru-ey0b3ztwPtdwu2FiI8MEzTB1I51\\_BJx\\_rPzSDDeB17olGG1kFD79Q5dDbcmjAvpT5mSY9MxljKcF5f38U3IONpfwWKHUT5Zu67rcliTXYj3aF6ggGVPk3KDmG-r4ih8F1NxLGTswLBGqffdLr6HSnp-6w8pk2Qa8thLrDSweqpXTb9RjG2vZ12JE](https://39805fae[.]sibforms[.]com/serve/MUIEAla_VCcQH4f37rvv6Ru-ey0b3ztwPtdwu2FiI8MEzTB1I51_BJx_rPzSDDeB17olGG1kFD79Q5dDbcmjAvpT5mSY9MxljKcF5f38U3IONpfwWKHUT5Zu67rcliTXYj3aF6ggGVPk3KDmG-r4ih8F1NxLGTswLBGqffdLr6HSnp-6w8pk2Qa8thLrDSweqpXTb9RjG2vZ12JE)
- [https://c8679251\[.\]sibforms\[.\]com/serve/MUIEABbP69ghhZbV1Ti2WfJS330e3zMO9etXG339pHQlxuLHsGeAW0j453TcK3089iQ1SywYzhIA\\_CbOYNm4MPFNS5jT8Gr16u2EBqD2YBgMfIEEjgR6Acrt\\_x3zbZB-LVPE3-GHvgDNbBu58rRQYheDJjH\\_gGZzRR0I7v-avVZ04z1gJ9KOOZo40pnAg7ytNGI0ST0s79-J4w00C](https://c8679251[.]sibforms[.]com/serve/MUIEABbP69ghhZbV1Ti2WfJS330e3zMO9etXG339pHQlxuLHsGeAW0j453TcK3089iQ1SywYzhIA_CbOYNm4MPFNS5jT8Gr16u2EBqD2YBgMfIEEjgR6Acrt_x3zbZB-LVPE3-GHvgDNbBu58rRQYheDJjH_gGZzRR0I7v-avVZ04z1gJ9KOOZo40pnAg7ytNGI0ST0s79-J4w00C)

# RECOMENDACIONES

1. Realizar el análisis correspondiente para el bloqueo a los indicadores de compromiso expuestos, indicados en este documento.
2. Recomendamos tener precaución al momento de acceder a enlaces suministrados mediante medios de mensajería.
3. Mantener actualizadas las plataformas y sistemas de información.
4. Realizar campañas de concientización periódica a todos los usuarios de la institución.
5. No introducir los datos personales en portales web sin antes verificar los controles de seguridad de la misma.