ACTA ADMINISTRATIVA
CUMPLIMIENTO OBLIGACIONES MENSUALES – ENERO 2023
CONTRATO 2778 DE 2023

ACTA 0001.1

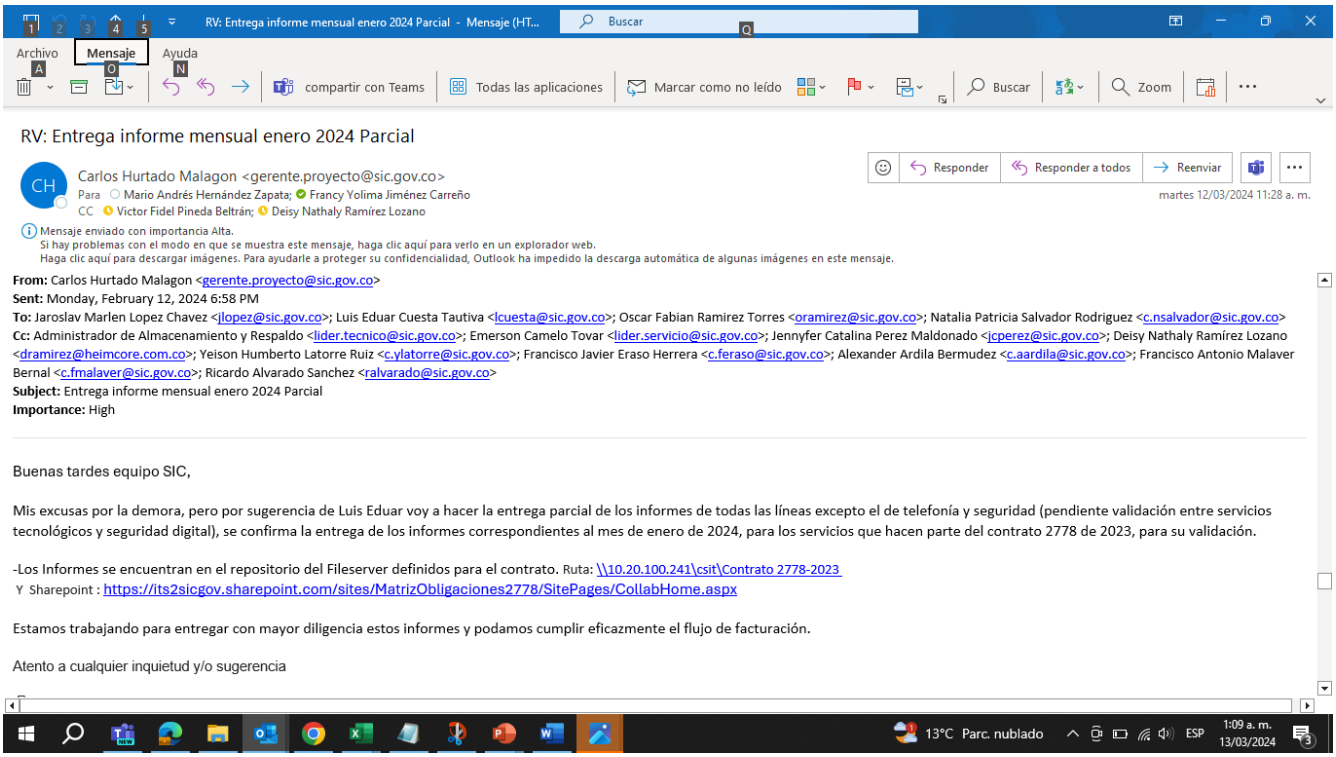
CIUDAD Y FECHA: Bogotá, 19 de marzo de 2024

PROCESO: Centro de Servicios Integrado de Tecnología. Matriz de cumplimiento SharePoint: https://its2sicgov.sharepoint.com/sites/MatrizObligaciones2778/SitePages/CollabHome.aspx

OBJETIVO: Validar cumplimiento a las obligaciones de contrato 2778 de 2023 para el mes de enero de 2024.

ENTREGA DE INFORMES

El día 12 de febrero de 2024 se realiza la entrega, por parte de UT INFOCH, los informes definidos generados por los servicios prestados durante el mes de enero de 2024, como evidencia del cumplimiento de las obligaciones contractuales.



RV: Entrega informe mensual enero 2024 Parcial - Mensaje (HT...

Archivo | Mensaje | Ayuda

compartir con Teams | Todas las aplicaciones | Marcar como no leído | Buscar | Zoom

RV: Entrega informe mensual enero 2024 Parcial

Carlos Hurtado Malagon <gerente.proyecto@sic.gov.co>
Para Mario Andrés Hernández Zapata; Francy Yolima Jiménez Carreño
CC Victor Fidel Pineda Beltrán; Deisy Nathaly Ramírez Lozano

Responder | Responder a todos | Reenviar
martes 12/03/2024 11:28 a. m.

Mensaje enviado con importancia Alta.
Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.
Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática de algunas imágenes en este mensaje.

From: Carlos Hurtado Malagon <gerente.proyecto@sic.gov.co>
Sent: Monday, February 12, 2024 6:58 PM
To: Jaroslav Marlen Lopez Chavez <jlopez@sic.gov.co>; Luis Eduar Cuesta Tautiva <lcuesta@sic.gov.co>; Oscar Fabian Ramirez Torres <oramirez@sic.gov.co>; Natalia Patricia Salvador Rodriguez <c.nsalvador@sic.gov.co>
Cc: Administrador de Almacenamiento y Respaldo <lider.tecnico@sic.gov.co>; Emerson Camelo Tovar <lider.servicio@sic.gov.co>; Jennyfer Catalina Perez Maldonado <jcperez@sic.gov.co>; Deisy Nathaly Ramírez Lozano <dramirez@heimcore.com.co>; Yeison Humberto Latorre Ruiz <c.ylatorre@sic.gov.co>; Francisco Javier Eraso Herrera <c.feraso@sic.gov.co>; Alexander Ardila Bermudez <c.aardila@sic.gov.co>; Francisco Antonio Malaver Bernal <c.fmalaver@sic.gov.co>; Ricardo Alvarado Sanchez <ralvarado@sic.gov.co>
Subject: Entrega informe mensual enero 2024 Parcial
Importance: High

Buenas tardes equipo SIC,

Mis excusas por la demora, pero por sugerencia de Luis Eduar voy a hacer la entrega parcial de los informes de todas las líneas excepto el de telefonía y seguridad (pendiente validación entre servicios tecnológicos y seguridad digital), se confirma la entrega de los informes correspondientes al mes de enero de 2024, para los servicios que hacen parte del contrato 2778 de 2023, para su validación.

-Los Informes se encuentran en el repositorio del Fileserver definidos para el contrato. Ruta: \\10.20.100.241\csit\Contrato 2778-2023
Y Sharepoint : https://its2sicgov.sharepoint.com/sites/MatrizObligaciones2778/SitePages/CollabHome.aspx

Estamos trabajando para entregar con mayor diligencia estos informes y podamos cumplir eficazmente el flujo de facturación.

Atento a cualquier inquietud y/o sugerencia

13°C Parc. nublado | ESP | 1:09 a. m. 13/03/2024

Resultado Evaluación:

Las siguientes obligaciones presentan observaciones sobre el servicio con su respectiva subsanación. Las obligaciones no relacionadas en este ítem se encuentran cumplidas.

Resultado Evaluación:

1. **PONDERABLES**

1.1 SERVICIOS SOC

Las siguientes obligaciones presentan observaciones sobre el servicio con su respectiva subsanación. Las obligaciones no relacionadas en este ítem se encuentran cumplidas.

Obligación 1: Monitoreo del dominio https://www.sic.gov.co/
Subsanación: 05-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación. 19-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación.

Obligación 2: Monitoreo de los subdominios de la SIC.
Subsanación: 05-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación. 19-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación.

Obligación 3: Monitoreo de las apps móviles de la entidad.
Subsanación: 05-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación. 19-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación.

Obligación 4: Monitoreo de cuentas comprometidas del personal VIP de la SIC.
Subsanación: 05-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación. 19-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación.

Obligación 5: Monitoreo de DNS.
Subsanación: 05-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación. 19-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación.

Obligación 6: Monitoreo de redes sociales.
Subsanación: 05-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación. 19-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación.

Obligación 7: Detección de contenidos publicados en las redes sociales sobre marcas o productos, opiniones dañinas o usuarios conflictivos que pueden producir una crisis o poner en riesgo a la SIC.
Subsanación: 05-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación. 19-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación.

Obligación 8: Identificación de fugas de información Deep y Dark Web.
Subsanación: 05-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación. 19-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación.

Obligación 9: Detección de nuevos sitios phishing.
Subsanación: 05-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación. 19-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación.

Obligación 10: Detección y eliminación de ataques o amenazas a sus activos digitales, información y/o bases de datos.
Subsanación: 05-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación. 19-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación.

Obligación 11: Uso no autorizado de imágenes, logos y marca.
Subsanación: 05-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación. 19-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación.

Obligación 12: Detección pasiva de las vulnerabilidades de la superficie de ataque expuesta a internet
Subsanación: 05-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación. 19-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación.

Obligación 13: Detección de información de la SIC expuesta en repositorios públicos.
Subsanación: 05-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación. 19-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación.

Obligación 14: Protección de la marca contra posibles abusos y daños reputacionales, piratería, falsificaciones, entre otros.
Subsanación: 05-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación. 19-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación.

Obligación 15: Alertar sobre certificados SSL vencidos o próximos a vencer.
Subsanación: 05-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación. 19-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación.

Obligación 16: Apoyo a la entidad en la realización de los takedown, en caso de que se requiera y sea procedente.
Subsanación: 05-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación. 19-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación.

Obligación 17: Deberá realizar la gestión de las vulnerabilidades detectadas, informando, presentando las recomendaciones correspondientes, y haciendo el seguimiento a su mitigación.
Subsanación: 05-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación. 19-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación.

Obligación 18: El SOC que se ofrezca debe tener certificación ISO 27001 teniendo en cuenta los procesos de seguridad que se deben tener para este tipo de gestión.
Subsanación: 05-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación. 19-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación.

Obligación 19: Este servicio le debe permitir a la Entidad conocer su estado de Ciber Exposición y vulnerabilidades a nivel de: activos de red, servidores, equipos de seguridad y aplicaciones web. Este debe tener como cobertura 500 activos y deberá permitir:

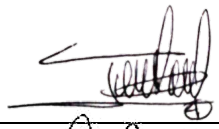
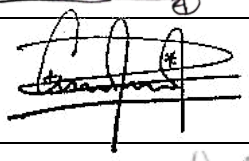
- ✓ Escaneo de vulnerabilidades priorizado mediante Vulnerability Priority Rating en cualquiera de sus niveles

✓ Generación periódica de reportes sobre las vulnerabilidades detectadas.
✓ Identificación de vulnerabilidades en aplicaciones web
✓ Monitoreo de Ataques al directorio activo.

Subsanación: 05-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación

Obligación 20: Deberá suministrar el servicio de escaneo de vulnerabilidades de mínimo tres (3) veces al año.
Subsanación: 05-03-2024 Se carga el informe actualizado, para dar cumplimiento con la obligación

REVISORES

Nombre	**Cargo / Dependencia**	**Entidad**	**Firma**
Luis Eduar Cuesta Tautiva	Coordinador Servicios Tecnológicos / Supervisor Contrato	SIC	
Oscar Ramírez Torres	Coordinador Seguridad Digital y LIF / Supervisor Contrato	SIC	
John Alexander Acuña Ramírez	Arquitecto Informática Forense y Seguridad Digital	SIC	
Carlos Hurtado Malagon	Gerente de Proyecto	UT INFOCH	
Daniel Andrés Pico Moreno	Lider del NOC- SOC	UT INFOCH	