INFORMACIÓN DE COINSOC

RFC 2350

Julio de 2023

1. Información sobre el documento

1.1 Versión 1: Publicada en Julio de 2023

1.2 Lista de distribución:

No hay una lista de distribución para notificación del cambio de versión de este documento, en caso de nueva versión, será publicada en la página de COINSA S.A.S., sección CoinSOC.

1.3 Ubicación del documento:

Español:

https://coinsasas.com/wp-content/uploads/COINSOC_RFC_2350_ESP.pdf

Inglés:

https://coinsasas.com/wp-content/uploads/COINSOC_RFC_2350_ENG.pdf

1.4 Autenticación del documento:

El documento es firmado desde el usuario autorizado por COINSA S.A.S.

2. Información de contacto

2.1 Nombre del equipo:

COINSOC, Centro de Operaciones de Seguridad, que hace parte de la Compañía de Ingenieros de Sistemas Asociados - COINSA S.A.S.

2.2 Dirección:

Sede Administrativa: Carrera 35 No. 46-48 - Bucaramanga

Sede Operativa: Avenida Carrera 45 # 100-12, piso 4 Edificio Panorama 100 - Bogotá

2.3 Zona Horaria:

América / Bogotá (GMT-5), en ésta zona horaria no hay horario de verano.

2.4 Números de contacto:

(57) 3157750178 - (57) 3174276422

2.5 Dirección de correo electrónico:

- Para intercambiar información de incidentes: analistasoc@coinsalt.com
- Información general: info@coinsalt.com

2.6 Claves públicas PGP

Para enviar correo cifrado a la cuenta de atención de incidentes analistasoc@coinsalt.com, descargue la llave pública que se encuentra al final de la página, en el enlace: https://coinsasas.com/why-us/ y descargarla en el link:

https://coinsasas.com/wp-content/uploads/CSIRTCoinsa_public.asc

2.7 Miembros del equipo:

No se publican los nombres de los integrantes del equipo por seguridad. En un proceso formal de revisión de CoinSOC o en un proceso contractual con los clientes, puede ser suministrada esta información.

2.8 Horas laborales de SOC:

7 días a la semana, 24 horas del día, 365 días del año, línea directa las 24 horas

2.9 Información sobre COINSOC:

La información general sobre SOC de COINSA S.A.S, puede ser consultada en el enlace https://coinsasas.com/why-us/

2.10 Puntos de contacto para la comunidad:

La comunicación entre COINSOC y los clientes o interesados en los servicios se realiza mediante:

- Los números celular (57) 3157750178 - (57) 3174276422
- Envío de correo electrónico a analistasoc@coinsalt.com

3. Constitución

3.1 Misión

COINSA SAS.[1], es una empresa que provee bienes y servicios informáticos, ofreciendo una solución íntegra, real y efectiva a las necesidades de sistematización y actualización tecnológica de nuestros clientes, buscando incrementar la competitividad empresarial de los mismos mediante la efectiva apropiación de la tecnología.[2]

CoinSOC (NOC-SOC de COINSA) brinda a los clientes y a la compañía los servicios horizontales de ciberseguridad, seguridad de la información y monitoreo de las operaciones tecnológicas, de forma más ágil y oportuna.

3.2 Comunidad a la que brinda servicios[3]

La comunidad a la que se brindan los servicios son: cliente interno objetivo COINSA S.A.S. y en los diferentes clientes externos de la compañía que requieren el servicio, definidos en un contrato.

3.3 Alcance

Mediante la gestión de ciberseguridad, seguridad de la información y monitoreo de las operaciones tecnológicas, se busca aplicar medidas de contención o mitigación y respuesta a las amenazas, eventos e incidentes, los cuales son realizados con los servicios ofrecidos por COINSOC:

[1] COMPAÑIA DE INGENIEROS DE SISTEMAS ASOCIADOS - COINSA S.A.S.

[2] SC-O-PL-22-007_PLANEACIÓN ESTRATEGICA

[3] A quien brinda los servicios (distrito electoral)

- Gestión y monitoreo de Eventos de TI e Incidentes de Seguridad – SOC
- Vigilancia Digital
- Inteligencia de Amenazas / Cacería de Amenazas
- Análisis Forense Informático
- Evaluación de Vulnerabilidades, Pruebas de Intrusión e Ingeniería Social
- Desarrollo, Investigación y Educación de Ciberseguridad e Infraestructura Tecnológica

3.4 Organización patrocinadora

CoinSOC, pertenece a Compañía de Ingenieros de Sistemas Asociados - COINSA S.A.S y forma parte de la Vicepresidencia de Operaciones.

4. Políticas

4.1 Gestión de incidentes y nivel de soporte

Los clientes: externos (con contrato suscrito) cómo el cliente interno (COINSA S.A.S. a través de CoinSOC (NOC/SOC) reporta los eventos o incidentes de seguridad que se presenten junto con los registros o soportes que se tengan, para así poder realizar una correcta identificación, recolección, adquisición y preservación.[4]

COINSA S.A.S, cómo patrocinador de COINSOC (NOC/SOC), establece los responsables y canales para la gestión de los incidentes de seguridad de la información (Ver los numerales del presente documento: “2.5 Dirección de correo electrónico” y “2.10 Puntos de contacto para la comunidad”).

El personal responsable debe atender de manera inmediata los eventos reportados, luego de analizar los eventos, determinar si estos son categorizados como incidente

[4] SC-O-PR-22-003_PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

de ciberseguridad y/o de seguridad de la información y realizar el escalamiento correspondiente de acuerdo con su nivel de criticidad, determinado mediante los niveles de impacto descritos en la sección “6.2.2 Niveles de impacto”, que hace parte del SC-O-PR-22-003_PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

Los incidentes reportados a COINSOC son catalogados de acuerdo a la taxonomía de clasificación de los incidentes, descrita en el documento SC-O-PR-22-003_PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, en la sección “6.2.1 Taxonomía de clasificación de incidentes”

CoinSOC (NOC-SOC) tiene la autoridad y es el responsable de garantizar que los posibles incidentes de ciberseguridad y de seguridad de la información se identifiquen analicen, defiendan, investiguen e informen correctamente.

Periódicamente desde CoinSOC se envían boletines de seguridad con la descripción de vulnerabilidades, su impacto, el nivel en el cual puede ser explotado, recursos de software afectado, riesgos, remediación y la información de contacto con COINSOC.

4.2 Cooperación, interacción y divulgación de la información

En la divulgación de la información, desde CoinSOC (NOC-SOC) de COINSA S.A.S. se determina que se debe mantener bajo reserva y no propagar, divulgar o usar en beneficio propio o de terceros la totalidad o parte de la información confidencial.

Proteger la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.[5]

Compartir con la comunidad los eventos e incidentes identificados en temas de monitoreo tecnológico, seguridad en la operaciones y seguridad de la información con el fin de crear sinergias de conocimiento en estas áreas.

5. Servicios

[5] SC-O-MO-22-002_MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION

Desde CoinSOC (NOC-SOC) de COINSA S.A.S., se ofrecen los siguientes servicios:

SERVICIO DE COINSOC	DESCRIPCIÓN
Gestión y monitoreo de Eventos de TI e Incidentes de Seguridad – SOC	Monitoreo permanente de la actividad de los activos de información orientado a identificar eventos o incidentes que puedan impactar la seguridad, integridad, disponibilidad, identidad y el acceso a los procesos de negocio del cliente A fin de realizar alertas tempranas, así aplicar acciones de contención y/o de prevención, realizar mejoras en los procesos en función de las lecciones aprendidas, y documentar la base de conocimiento.
Vigilancia Digital	Se realizan actividades para la detección proactiva de abusos que atenten contra la marca y la reputación de la empresa. Identificación de eventos digitales con el fin evitar disrupciones en el negocio Las líneas de capacidad del SOC de COINSA para el servicio de vigilancia digital son: a) Investigación de Contenido digital: Todo el contenido relacionado con abuso de propiedad intelectual, patentes, derechos de autor, marca registrada. b) Afectación a la reputación: Eventos de (conductas delictivas, amenazas, calumnia), ofuscación de manifestaciones, protestas, huelgas divulgadas, todos los eventos o sujetos identificados en entornos digitales que puedan afectar la integridad de nuestros clientes. c) Fuga de información: Toda la información y/o datos personales y/o institucionales encontrados en entornos públicos digitales.

SERVICIO DE COINSOC	DESCRIPCIÓN
	d) Suplantación: Evidencia de engaño o fraude informático de la infraestructura tecnológica o de los activos digitales del cliente. e) Seguridad Tecnológica: Exposición de activos de digitales o de infraestructura tecnológica del cliente
Inteligencia de Amenazas/Cacería de Amenazas	Con la recopilación de la información detallada sobre las amenazas de ciberseguridad que han sido dirigidas a las organizaciones, descritas en informes de Inteligencia de amenazas cibernéticas, por sus siglas en inglés: CTI[6], se realiza el análisis y filtrado con el fin de identificar posibles amenazas en la infraestructura y aplicar medidas de contención y/ o mitigación del impacto y así reducir los riesgos en los sistemas
Análisis Forense Informático	Es un conjunto de técnicas destinadas a extraer información valiosa de los sistemas, sin alterar el estado de los mismos (cadena de custodia). Estas permiten identificar datos que son conocidos previamente, para encontrar un patrón o comportamiento determinado, o descubrir información que se encontraba oculta Información que es parte de un proceso de fraude informático o delito cibernético y que se entrega para procesos disciplinarios o legales.
Evaluación de Vulnerabilidades, Pruebas de Intrusión e Ingeniería Social	Es el ejercicio de identificar las debilidades de las tecnologías, personas o procesos.
Desarrollo, Investigación	Realizar laboratorios para la simulación de amenazas,

[6] Cyber Threat Intelligence

SERVICIO DE COINSOC	DESCRIPCIÓN
y Educación de Ciberseguridad e Infraestructura Tecnológica	revisión de vulnerabilidades y verificación de afectación e impacto en las tecnologías.

6. Notificación de incidentes

- **Correo electrónico:** analistasoc@coinsalt.com
- **Número celular:** + 57 3157750178

7. Descargo de responsabilidad

COINSA S.A.S. no se hace responsable por el posible mal uso de la información contenida en este documento.

Firmado digitalmente por Analista SOC
Nombre de reconocimiento (DN):
cn=Analista SOC, o=Coinsa SAS,
ou=CoinSOC,
email=analistasoc@coinsalt.com, c=CO
Fecha: 2023.08.02 12:20:27 -05'00'