HEIMCOREISOC-CSIRT RFC 2350

1. INFORMACIÓN DEL DOCUMENTO

1.1 Fecha de Ultima Actualización: Versión 1.0, publicada el 20 de Febrero 2023.
1.2 Listas de Distribución: No Existe un canal de distribución para notificar cambios en este documento. Los cambios son anunciados por medio de notificación en:
- https://heimcore.com.co/solucion/heimcore-csirt/
- SGSI 27001 del proceso SOC Heimcore (Control Interno)

1.3 Ubicación del Documento: La ultima versión del documento se encuentra publicada en:
https://heimcore.com.co/solucion/heimcore-csirt/
- SharePoint SGSI 27001 SOC NOC Heimcore

1.4 Autenticación del Documento: Este Documento ha sido firmado físicamente por el representante de la Alta Gerencia en el SGSI y por la Dirección Ejecutiva de Heimcore.

2 INFORMACIÓN DE CONTACTO

2.1 Nombre del Equipo: HeimcoreISOC-CSIRT, CERT Heimcore Centro de Operación de Seguridad Inteligente (ISOC).
2.2 Dirección:
Heimcore-ISOC-CSIRT, ISOC de Heimcore, Calle 98 #70-91 Ofc.203
Bogota Colombia.
2.3 Zona Horaria: GMT-5
2.4 Número de Teléfono: +57 601 5804352 – Opción 2 – Celular: 3042218925.
2.5 Numero de Fax: No Existente
2.6 Otras Comunicaciones: No Existente
2.7 Direcciones de Correo Electrónico:
- Intercambio de Información relativa a incidentes o eventos: csirt@heimcore.com.co
- Consultas de carácter general: mercadeo@heimcore.com.co
- Otras direcciones de correo electrónico para contactar con el HeimcoreISOC-CSIRT:
  - https://www.heimcore.com.co/Contacto

2.8 Claves Publicas y cifrado de información: Los correos de contacto y claves PGP asociadas se encuentran bajo administración del ISOC de Heimcore, con cada uno de sus clientes tanto internos como externos.
2.9 Miembros del Equipo: Analistas Monitoreo SOC - CSIRT nivel 1, Analistas SOC - CSIRT nivel 2, Ingeniero Especialista SOC, Coordinador de SOC - CSIRT y Directora de Operaciones.

2.10 Mas Información: La Información general sobre los servicios proporcionados y ofrecidos por nuestro HeimcoreISOC-CSIRT y sobre el propio organismo se encuentra publicado en nuestra página WEB oficial corporativa:

- https://heimcore.com.co/solucion/heimcore-csirt/

2.11 Horario de Atención: El equipo de HeimcoreISOC-CSIRT esta disponible en los siguientes horarios:

- Consulta sobre los servicios o catalogo: horario de Oficina 8:00 AM – 5:00 PM
- Requerimientos, Eventos o Incidentes clasificados como prioridad Baja: horario de 8x5 L-V
- Incidentes clasificados como prioridad Media, Alta o Muy Alta: 24X7X365

2.12 Puntos de contacto para la comunidad: La comunicación entre el equipo HeimcoreISOC-CSIRT y los organismos a los que da soporte se realiza principalmente a través de:

- Correo Electrónico: csirt@heimcore.com.co/ soporte.soc@heimcore.com.co
- Pagina WEB: https://heimcore.com.co/solucion/heimcore-csirt/
- Correo Mercadeo: mercadeo@heimcore.com.co
- Teléfonos proporcionados a los clientes en la entrega oficial de los ANS.

3 CONSTITUCIÓN

3.1 Misión: Su misión principal es poder contribuir con el mejoramiento continuo de la Ciberseguridad en Colombia y Latinoamérica, siendo uno de los ISOC/CSIRT más importantes y reconocidos a nivel nacional e internacional y que permita ayudar a las organizaciones tanto públicas como privadas, en su gestión y respuesta a los ciberataques que puedan tener y afrontar de forma activa las ciber amenazas, incluyendo la coordinación a nivel nacional de distintas capacidades de respuesta a incidentes de seguridad o de centros de operación de seguridad reconocidos, para incidentes de especial relevancia.

Lo anterior, con el fin de conseguir mas tranquilidad en las organizaciones y un ciberespacio mas seguro y confiable, preservando siempre la Confidencialidad, Integridad y Disponibilidad de la información, permitiendo aplicar marcos de trabajo de éxito, últimas tendencias tecnologicas y políticas de seguridad, que de alguna manera blinden a las organizaciones de nuestros clientes.

3.2 Comunidad a la que se brinda el Servicio:
Organizaciones de todos los sectores nacionales, tanto públicas como privadas.
3.3 Patrocinio / Afiliaciones: El HeimcoreISOC-CSIRT, se encuentra actualmente certificado en la norma Internacional ISO 27001:2013 e ISO 9001:2015 con el Ente Internacional Bureau Veritas, por otro lado, cuenta con una afiliación con el centro cibernético de la Policía Nacional, para el escalamiento de Incidencias de seguridad informática críticas y reporte de amenazas identificadas, ademas de vínculos con otros Csirt de la región y uno de la Unión Europea.

4 POLITICAS

4.1 Tipo de Incidentes y de soporte

La clasificación de incidentes sobre los que esta alineado el HeimcoreISOC-CSIRT, están definidas y organizadas de acuerdo con el procedimiento de Gestión de Incidentes del SGSI 27001 de Heimcore, procedimiento documentado como **HC-SER-PRO-012.**

HeimcoreISOC-CSIRT, como CERT nacional, esta enfocado en colaborar y apoyar cuando se requiera, a todos los organismos públicos y privados en la detección, notificación, análisis, respuesta y aprendizaje de los diferentes incidentes de seguridad que puedan ocurrir, teniendo una trazabilidad detallada en todo el ciclo de vida del incidente de seguridad materializado, alimentando continuamente la base de conocimiento interna del HeimcoreISOC-CSIRT.

A nivel de soporte o apoyo que realizará el HeimcoreISOC-CSIRT, estará alineado con unos ANS programados en la plataforma de soporte Aranda, y dichos tiempos de respuesta están sujetos a los siguientes criterios de evaluación:

- Identificación del tipo de amenaza (Malware, Denegación de Servicios, Ransomware, acceso abusivo al sistema, etc.)
- Origen de la Incidencia de Seguridad o Amenaza identificada
- Activos críticos afectados en el incidente de seguridad
- Perfilamiento de los usuarios afectados o usados en el incidente de seguridad
- Arquitectura de seguridad informática actual del cliente afectado
- Plan de Continuidad de negocio del cliente actualizado
- El impacto que genera o generó el incidente de seguridad en la organización
- Los requisitos legales y regulatorios del cliente actualizado

Por otro lado, el HeimcoreISOC-CSIRT pone a disposición de sus clientes, información relacionada con las últimas tendencias de ataques informáticos en la región, alienados con otros CSIRT y entidades de ciberseguridad reconocidas a nivel mundial, esto con el fin de poder reducir vulnerabilidades tanto de tipo hardware como de software, de los usuarios internos y externos de la organización y en una arquitectura técnica ideal de acuerdo con el CORE de la Organización. Para esto, notifica o crea un alertamiento periódico con la siguiente información:

- Alertas o Aviso de amenazas o vulnerabilidades detectadas por el HeimcoreISOC-CSIRT o por otro CSIRT que trabaja alineado con la Organización del cliente.
- Alertamiento de eventos y de incidentes que se consideren de prioridad baja, media o alta.
- Reporte de Vulnerabilidades actualizadas y de fuentes muy confiables
- Informes o reportes de código malicioso que esta circulando en la red de la región
- Informes o reportes de las mejores practicas de seguridad del momento

- Informes o reportes de las amenazas identificadas en la actualidad, con sus respectivas recomendaciones

4.2 Divulgación, Interacción o Cooperación de la Información

Es importante tener claro que la información que maneje el HeimcoreISOC-CSIRT es tratada con absoluta confidencialidad e integridad de acuerdo con las políticas y procedimientos establecidos en el Sistema de Gestión de Seguridad de la Información ISO 27001 y las diferentes normas de protección de la información clasificada y tratamiento de datos personales.

4.3 Plan de Comunicación y Autenticación del HeimcoreISOC-CSIRT

Los medios disponibles para la comunicación con el HeimcoreISOC-CSIRT son los siguientes:

- Correo Electrónico cifrado con llaves publicas y privadas que están dedicadas para el paso de información critica o confidencial, previamente clasificada por el SOC NOC de Heimcore. (Las llaves serán entregadas y organizadas entre el HeimcoreISOC-CSIRT y cada uno de sus clientes o stakeholders del CSIRT)
- Teléfonos o PUC que se entregaran a los clientes del SOC NOC y CSIRT en la activación del servicio
- Plataforma de Gestión de Incidentes y requerimientos de servicios Aranda del SOC NOC de Heimcore.

5 SERVICIOS

5.1 PREVENCIÓN

El HeimcoreISOC-CSIRT con todos sus clientes activos, realiza un plan de sensibilización y comunicación con cada cliente, esto con el fin de poder crear conciencia y prevenir a las organizaciones de los clientes, evitando la materialización de diferentes tipos de incidentes de seguridad que pongan en riesgo la información, algunas actividades se destacan las siguientes:

- Puesta en marcha y confirmación de las políticas de seguridad establecidas en el HeimcoreISOC-CSIRT, las cuales están alineadas al SGSI 27001 vigente de Heimcore.
- Soporte y apoyo en el tratamiento de las vulnerabilidades identificadas en cada organización cliente.
- Entrega periódica de informes con la gestión de Incidentes o eventos trabajados desde el HeimcoreISOC-CSIRT y el SOC NOC de Heimcore.
- Entrega de ultimas noticias en materia de ciberseguridad a cada uno de los clientes del HeimcoreISOC-CSIRT.
- Apoyo constante en actualizar temas de requisitos legales y normativos de la Región en cada organización.
- Entrega de insumos de formación y sensibilización relacionados con ciberseguridad.
- Organización y participación constante en eventos o seminarios de ciberseguridad.
- Apoyo en auditorias relacionadas con ciberseguridad de los clientes, siendo más consultivos y preventivos.
- Capacitación constante al equipo de Ingenieros del HeimcoreISOC-CSIRT brindando confianza en el conocimiento idóneo y actualizado de ciberseguridad.

5.2 RESPUESTA A LOS INCIDENTES

El HeimcoreISOC-CSIRT brinda apoyo especializado técnico y operativo, al momento de identificar un incidente de seguridad, estando alineado en las diferentes etapas del proceso de gestión de incidentes mundialmente conocidos, como lo son la detección, el análisis, la notificación, la contención, la erradicación y recuperación. En el procedimiento de gestión de incidentes también se tiene en cuenta una evaluación para poder medir el nivel de criticidad del incidente de seguridad materializado, esto con el fin de aplicar los tiempos de respuesta que correspondan, posterior a esto viene todo el tema de validación y verificación del incidente y finalmente la toma de evidencias necesarias, para poder mas adelante construir un documento de trazabilidad de la misma.

Finalmente, el SOC NOC junto con el HeimcoreISOC-CSIRT, escalaran de ser necesario el incidente con sus grupos de apoyo, con el fin de poder tener mas conocimiento del incidente y el paso a seguir que permita controlar la situación, adicionalmente se construye un documento tipo reporte que permita mostrar un seguimiento y análisis detallado del tipo de incidente que se está contrarrestando.

5.3 COORDINACIÓN DE LOS INCIDENTES

El HeimcoreISOC-CSIRT coordina los incidentes y ejerce además la coordinación a nivel nacional como centro de respuesta a incidentes tipo CSIRT/CERT y tiene en su estructura también un equipo de trabajo que actúa como centro de operaciones de seguridad Inteligente tipo SOC, tanto del sector público como privado, siempre en constante actualización de tendencias de nuevos ciberataques y mecanismos de defensa, siempre alienado con otros CSIRT y equipos SOC, nacionales como internacionales.

5.4 PROCESO DE MONITOREO

HeimcoreISOC-CSIRT cuenta con plataformas especializadas en el monitoreo en tiempo real de activos de Infraestructura tecnológica, que permiten validar la disponibilidad y funcionamiento de cada activo monitoreado, con unas alertas y reglas de notificación configuradas, para avisar en tiempo real cualquier eventualidad que genere impacto en el activo monitoreado, los activos pueden ser equipos físicos, equipos virtuales o servicios específicos que hacen parte del CORE de una determinada organización.

5.5 PLATAFORMAS Y HERRAMIENTAS DE CIBERSEGURIDAD

El HeimcoreISOC-CSIRT tiene en su estructura técnica, una serie de herramientas de seguridad informática que permiten garantizar la seguridad de los sistemas de información y que brindan una mejor gestión de ciberseguridad para los clientes, todas las herramientas utilizadas son alineadas al ciclo de la NIST, donde se detecta, analiza, audita y transfiere la información de los clientes, que ha sido afectada o amenazada por un incidente de seguridad.

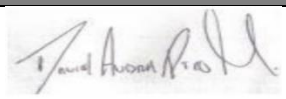
5.6 INFORMATICA FORENSE Y DE ANALISIS DE MALWARE

HeimcoreISOC-CSIRT cuenta con un equipo de profesionales capacitados en análisis forense y de malware, mediante herramientas muy especializadas en informática forense, permitiendo atender y dar respuesta a incidentes de seguridad complejos.
Por otro lado, cuenta con alianzas estratégicas con equipos muy especializados en todo lo que es la informática forense y requisitos legales vigentes.

6 CANALES DE NOTIFICACIÓN DE INCIDENTES AL HEIMCOREISOC-CSIRT

La notificación de incidentes por parte de los clientes o stakeholders del HeimcoreISOC-CSIRT se puede hacer de la siguiente manera:

- Plataforma de Gestión de Incidentes Aranda del Soc Noc de Heimcore
  - https://www.heimcore.com.co/soporteti
- PUC (Punto Único de Contacto)
  - 6015804352 opción 2
  - Celular 3042218925
- Correos Electrónicos
  - soporte.soc@heimcore.com.co
  - csirt@heimcore.com.co

1. Control de aprobación de documentos		
Nombre	**Cargo**	**Firma**
Daniel Andres Pico	Coordinador SOC – NOC	
Anahis Cabello	Directora de Operaciones	
Danny Pineda	Director Ejecutivo	