Aprobación Documental

Revisó: Ricardo Cespedes **Rol**: Gerente de Servicios Ciberseguridad **Fecha**: septiembre 2023	**Aprobó:** Carlos Bustos **Rol:** director Corporativo Ciberseguridad **Fecha:** septiembre 2023

Contenido

1. INFORMACIÓN DEL DOCUMENTO

Este documento contiene una descripción de los equipos CSIRT de SONDA S.A. de acuerdo con el RFC 2350. Adicionalmente proporciona información básica sobre el **Defense Center**, canales de comunicación, roles y responsabilidades.

1.1. FECHA DE LA ÚLTIMA ACTUALIZACIÓN

25 de septiembre de 2023.

1.2. LISTA DE DISTRIBUCIÓN PARA NOTIFICACIONES

Todo cambio realizado al documento será notificado y publicado mediante el sitio oficial

https://www.sonda.com/soluciones/ciberseguridad y el detalle de sus modificaciones estarán disponibles en la plataforma de GRC interna de Sonda.

1.3. UBICACIÓN DEL DOCUMENTO

La versión actual del documento está disponible en el sitio web interno Sonda GRC y Sitio Oficial de Sonda

1.4. AUTENTICACIÓN DEL DOCUMENTO

Este documento ha sido firmado mediante la clave PGP por CSIRT- Sonda.

2. INFORMACIÓN DE CONTACTO

2.1. NOMBRE DEL EQUIPO

CSIRT- SONDA, equipo de respuestas a incidentes del Centro de Operaciones de Ciberseguridad de SONDA S.A.

2.2. DIRECCIÓN

Teatinos # 500. Región Metropolitana. Santiago de Chile.

CARRERA 106 15 A 25 23 LT IN 135 ED ZF TOWERS SERVICE AND, Bogotá Colombia

2.3. ZONA HORARIA

UTC-GMT -3 Chile

GMT-5 Colombia

2.4. NÚMEROS DE CONTACTO

(+562) 26576035 SOC Chile

(+569) 54800979 SOC Chile

+573167491946 SOC Colombia

2.5. NÚMERO DE FAX

No aplica

2.6. OTRAS COMUNICACIONES

defensecenter.cl@sonda.com

2.7. DIRECCIÓN DE CORREO ELECTRÓNICO

Contacto primer nivel Chile: defensecenter.cl@sonda.com

Contacto primer nivel Colombia: defensecenter.co@sonda.com

Contacto CSIRT regional: CSIRT@sonda.com

2.8. LLAVES PÚBLICAS Y CIFRADO DE INFORMACIÓN

Las llaves públicas para el cifrado de información serán compartidas a través de los canales establecidos con los equipos de respuesta incidentes, clientes, socios de negocio y terceros que requieran hacer uso de ellas.

2.9. MIEMBROS DEL EQUIPO

Por razones de privacidad el listado de personal perteneciente al equipo no se publica en este documento.

2.10. MAS INFORMACIÓN

Para obtener información adicional, relacionada a los servicios prestados por CSIRT-Sonda, consultar el sitio web:

https://www.sonda.com/soluciones/ciberseguridad

2.11. HORARIO DE ATENCIÓN

El CSIRT de Sonda opera en horario estándar de 8 horas al día, de lunes a viernes, considerando las zonas horarias respectivas de Chile y Colombia.

Para garantizar la disponibilidad de respuesta ante situaciones de crisis las 24 horas del día, los 7 días de la semana, el CSIRT cuenta con turnos rotativos de personal de guardia.

El horario disponible para la activación del equipo CSIRT es 24x7x365 días sin excepción.

2.12. PUNTOS DE CONTACTO PARA CLIENTES

La comunicación entre el equipo SCIRT-Sonda y la comunidad a la que presta servicio, se realiza mediante el siguiente listado de escalamiento:

- Primera instancia:
  Correo electrónico CSIRT: csirt@sonda.com
  Correo electrónico SOC Chile: defensecenter.cl@sonda.com
  Correo electrónico SOC Colombia: defensecenter.co@sonda.com

- Segunda Instancia:
  (+562) 26576035 SOC Chile
  (+569) 54800979 SOC Chile
  +573167491946 SOC Colombia

3. CONSTITUCIÓN

A partir del 17 de abril de 2019, junto con la inauguración del equipo SOC en Colombia, inician las operaciones de Ciberseguridad de Sonda para sus clientes. En la actualidad cuenta, además, con un equipo de SOC en Chile y presta servicios de Respuesta a Incidentes, desde su equipo CISRT regional.

3.1. MISIÓN

Ser reconocidos como uno de los principales proveedores de servicios de Ciberseguridad gestionados en las Américas, estableciendo un nivel de seguridad que lleve al cliente, a lograr la confianza que le permita aumentar su ventaja estratégica.

Propuesta de valor con los clientes en el centro:

Construimos los niveles de confianza que nuestros clientes requieren para sus procesos de transformación digital, preparando, previniendo, detectando y respondiendo a los diferentes incidentes de ciberseguridad.

3.1.1 Objetivos:

- Entregar Servicios Avanzados de Ciberseguridad con personal certificado en 4 idiomas.
- Tener servicios de SOC que nos permita trabajar en forma competitiva en 7 husos horarios.
- Contar con un laboratorio de investigación que innova y desarrolla técnicas de detección avanzadas que son incorporadas a nuestra plataforma de servicios.
- Aportar técnicas en ciberseguridad a la comunidad internacional
- Ser el partner top 3 de Ciberseguridad de las multilatinas y multinacionales en la región.

3.2. COMUNIDAD A LA QUE BRINDA SERVICIOS

El CSIRT brinda servicios tanto a la organización SONDA y sus filiales, como a clientes externos a ella que cuenten con servicios de Ciberseguridad suscritos o requieran de ellos.

3.3. PATROCINIO / AFILIACIÓN

CSIRT- Sonda nace de la necesidad de la compañía, de contar con un equipo que permita dar respuesta a las demandas actuales respecto a ciberseguridad de la organización y sus clientes. Se crea entonces, desde una visión estratégica, la división de servicios de ciberseguridad como ente autónomo, con la opción de ampliar su alcance de servicios a clientes externos a SONDA.

3.4. AUTORIDAD

Dependiendo en cada caso, la autoridad del equipo depende del nivel de responsabilidades acordadas con cada cliente y definidas por contrato. De acuerdo con esto, El equipo CSIRT-Sonda cuenta con capacidades tanto de asesoramiento y consultoría especialista, como de implementación de medidas, lo que define también, el nivel de autoridad y responsabilidad a la hora de aplicar las acciones correctivas correspondientes.

4. POLÍTICAS

4.1. TIPO DE INCIDENTES Y NIVEL DE SOPORTE

Con el fin de proporcionar una respuesta coherente y oportuna y, manejar la información de una manera adecuada, se establece la Política Manejo de incidentes de ciberseguridad, la cual define y proporciona las pautas necesarias para que el CSIRT-Sonda clasifique cada caso de acuerdo con la categoría, nivel de criticidad y prioridad que corresponda. A su vez, entrega los lineamientos para la notificación y tiempos de respuesta para cada tipo de incidente.

4.2. COOPERACIÓN, INTERACCIÓN Y DIVULGACIÓN DE LA INFORMACIÓN

Durante el ciclo de prestación de sus servicios, el CSIRT-Sonda puede interactuar con otras organizaciones y equipos CSIRT, proveedores, Partners etc.

Con el objeto de facilitar la cooperación en temas específicos o servicios técnicos, el SCIRT-Sonda interactúa con grupos relacionados a la respuesta a incidentes tanto de manera interna como externa. En la política de difusión de información Ciberseguridad, se especifica quiénes son los destinatarios del informe CIRT en cada circunstancia.

A la fecha de publicación de este documento, los grupos relacionados con los que interactúa el CSIRT-Sonda son los siguientes:

- CSIRT Gobierno Chile
-

4.3. COMUNICACIÓN Y AUTENTICACIÓN

El CSIRT- Sonda garantiza principalmente la seguridad de las comunicaciones mediante el uso de PGP. Se podrían usar otros medios acordados dependiendo del nivel de sensibilidad y el contexto de la información intercambiada entre las partes.

5. SERVICIOS

El amplio portafolio de soluciones y servicios de ciberseguridad de Sonda, permite entregar un enfoque integral, incluyendo dentro de su alcance los procesos, personas y tecnologías para resguardar los entornos TI, además de procedimientos. Nuestra plataforma de Servicios, nuestros profesionales y nuestros procesos permiten contar con niveles de escala mundial. (Acotado al DF)

5.1 Detección de amenazas y vulnerabilidades

- Gestión de Eventos
- Administración de Identidades
- Revisión de código
- Business Hardening: Gobierno de Vulnerabilidades
  Aseguramiento de la Red de Infraestructura

5.2 Servicios avanzados de ciberseguridad

- Threat Hunting
- Respuesta a Incidentes
- Análisis Forense
- Automatización y Orquestación: Administración de playbooks
  Integración Continua

5.3 Seguridad Ofensiva

- Breach and Attack Simulation (RedTeam)
- Ethical Phishing
- Ethical Hacking: Internos/Externos
  Específicos (WebApps, apps)

5.4 Consultoría

- Evaluación de madurez CIS/NIST/ISO27K
- Compliance Continuo CIS/NIST/ISO27K
- Compliance Específico (Finanzas, OT)
- Awareness Corporativo
- Evaluación Integral de proceso de Negocio

El detalle de los servicios, se encuentran disponibles en el siguiente link:
https://www.sonda.com/soluciones/ciberseguridad

6. FORMAS DE NOTIFICACIÓN DE INCIDENTES

- Primera instancia:
  Correo electrónico CSIRT: csirt@sonda.com
  Correo electrónico SOC Chile: defensecenter.cl@sonda.com
  Correo electrónico SOC Colombia: defensecenter.co@sonda.com

- Segunda Instancia:
  (+562) 26576035 SOC Chile
  (+569) 54800979 SOC Chile
  +573167491946 SOC Colombia

7. DISCLAIMER

El Equipo **CSIRT- SONDA de SONDA S.A.** no se hace responsable daños resultantes del mal uso de la información contenida en este documento.