1. OBJETIVO

La presente Normativa es parte de la POLÍTICA DE DISCLOSURE VULNERABILITY RESEARCH de SONDA (la "Política") cuyo objeto es definir aspectos relacionados con su cumplimiento, en el marco de las buenas practicas globales sobre la divulgación de vulnerabilidades coordinadas, denominada CVD, definidas en el "Global Forum on Cyber Expertise" (GFCE), celebrado en la Haya el 16 de abril de 2015, y de esta manera contribuir en el desarrollo de la ciberseguridad mediante la comunicación de conocimientos y resultados de evaluaciones de los investigadores, especialistas de ciberseguridad y/o cazadores de bugs (en conjunto como los "Especialistas".

2. ALCANCE

Esta normativa se aplica a todos los Especialistas externos, excluyendo los casos en que legislación y/o jurisdicción lo prohíba, sea por la vía de su aplicación territorial o derivado de normativa aplicable a los nacionales o ciudadanos del país investigador. Tanto la Política como la presente Normativa se hacen extensivas a nuestros clientes para que evalúen nuestras soluciones propietarias de uso comercial privado, respetando siempre la debida custodia y confidencialidad de la información, en estricta observancia de la Ley, el principio de buena fé y la formalización de acuerdos de confidencialidad celebrado por las partes para este ejercicio especifico.

3. TERMINOLOGIA

- **CVE / Common Vulnerabilities and Exposures**: Es un identificador estándar para vulnerabilidades de seguridad informática conocidas públicamente en la industria.
- **Research o Investigador:** Especialista en Ciberseguridad, responsable de analizar, investigar, evaluar y buscar fallas de seguridad de día cero, tanto de infraestructura como de aplicaciones.
- **Hacker Ético:** Especialista en ciberseguridad que posee un conjunto de principios morales y éticos, responsable de realizar pruebas de intrusión en un sistema de forma controlada y autorizada, con el fin de evaluar los controles de seguridad existentes, mediante diferentes técnicas para identificar y reportar vulnerabilidades de seguridad.
- **GFCE:** Global Forum on Cyber Expertise, es un foro para que los países, organizaciones internacionales y empresas privadas intercambien las mejores prácticas y la experiencia en el desarrollo de capacidades cibernéticas.
- **CVD o Coordinated Vulnerability Disclosure:** Es un acuerdo para la transparencia de la adopción de políticas de divulgación de vulnerabilidades de forma coordinada.
- **POC o Proof of Concept:** Para la seguridad informática, está definido como pruebas de concepto para explicar cómo se puede explotar una vulnerabilidad.
- **Día Cero o Zero Day attack:** Es un ataque a un sistema o aplicación, por medio de técnicas donde se exploran fallas desconocidas para el fabricante o para el público, sin corrección, debido a que no existe registro anterior del evento.

6. NORMATIVA

6.1. REPORTE DE VULNERABILIDADES A SONDA S.A

6.1.1. REPORTAR VULNERABILIDADES A SONDA S.A

SONDA a dispuesto la casilla de correo electrónico report.a.bug[*]sonda.com para reportar vulnerabilidades. Para lo anterior se deberá proceder de acuerdo a la Normativa, lo cual será presumido por SONDA en aplicación del principio Buena Fé, cumpliendo, entre otros, con lo siguiente:

- Se deberán adjuntar los detalles del reporte, cifrando su contenido con password.
- El informe debe contener la descripción del tipo error, problema o falla.
- Se deberá entregar detalles por medio de un POC (Prueba de Concepto) donde se demuestre la exploración de la vulnerabilidad y su funcionamiento.
- Aceptamos recomendaciones de mitigación o corrección a la vulnerabilidad, las cuales serán evaluadas de forma interna si corresponden, no siendo obligados a aplicar tales recomendaciones.

6.2. CONSIDERACIONES DE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN

6.2.1. AUDITORIAS E INVESTIGACIÓN NO PERMITIDAS

Son contrarios a la Ley, si no hay autorización expresa de SONDA, las investigaciones y actividades de los Especialistas que:

(i) Produzcan la negación o degradación de los servicios que SONDA provee a sus clientes, de cualquier naturaleza (DDoS o DoS).

(ii) Realicen cambios en los sistemas de información y afecten su integridad. En este caso la autorización de SONDA además deberá ser específica para realizar dichos cambios durante un proceso de investigación y evaluación de vulnerabilidades.

(iii) Utilicen fallas o ataques por medio de una vulnerabilidad que tenga una Identidad “Common Vulnerabilities and Exposures” (CVE ID) o que afecten a otros proveedores de servicios con los cuales los de SONDA o sus sistemas relacionen o integren de cualquier manera de manera que puedan verse afectados o degradados.

6.2.2. AUDITORIA E INVESTIGACIÓN EXTERNA PERMITIDA

Los sistemas de información de SONDA, pueden ser objeto de auditorías externas por Especialistas en ciberseguridad, quienes deberán respetar la confidencialidad, disponibilidad e integridad de los mismos y de la información que en ellos se procese o almacene, además de dar estricta observancia a la ley aplicable y los procedimientos y regulaciones de SONDA para procesos de Auditoría, lo que incluye la presente Normativa.

6.2.3. INVESTIGACIÓN DE VULNERABILIDADES POR UN CLIENTE

Los sistemas de información de SONDA S.A de uso privado y comercial, solamente pueden ser auditados bajo un acuerdo firmado por las partes interesadas que contenga los procedimientos y regulaciones de SONDA para procesos de Auditoría, así como las obligaciones de confidencialidad correspondientes.

6.2.4. INVESTIGACIÓN DE VULNERABILIDADES POR SONDA S.A

Todos los colaboradores de ciberseguridad, los desarrolladores y especialistas que lleguen a evaluar algún producto, servicio de aplicación o sistema de terceros, deberán dar estricto cumplimiento a la Ley aplicable y se comprometen a cumplir con los programas de comunicación de vulnerabilidades de forma transparente.

6.3. CUMPLIMIENTOS LEGALES

6.3.1. LEGISLACIÓN APLICABLE

La legislación aplicable será la del país donde se encuentren los activos objeto de investigación por los Especialistas, sin perjuicio de la aplicación de normativa de derecho internacional privado, convenios internacionales y/o alcance extraterritorial de normativa extranjera. Las acciones necesarias para adecuarse a la legislación vigente se coordinarán con el área legal de SONDA.

6.3.2. CUMPLIMIENTO DE LA POLÍTICA DE CONFIDENCIALIDAD

Al realizar un reporte de vulnerabilidades a SONDA S.A, los Especialistas que identifique una vulnerabilidad, se comprometen a aceptar y suscribir un acuerdo de confidencialidad de forma inmediata durante la corrección de la falla reportada, la cual obliga a no divulgarla durante todo el periodo de análisis y corrección al público y hasta dos años posteriores a su finalización.

6.3.3. DERECHOS DE PROPIEDAD INTELECTUAL (DPI)

SONDA tiene derechos de propiedad intelectual (Copyright), y otros derechos de propiedad industrial, incluida aquella desarrollada por sus empleados como parte de las actividades como colaboradores de la compañía. Todo desarrollo y mejora ejecutada por empleados de SONDA son de propiedad de esta, así como aquellos derivados de contratos con prestadores de servicio, consultorías u otras, cuyos resultados ceden en beneficio exclusivo de SONDA, sin perjuicio de los derechos de propiedad intelectual de terceros, derechos de uso asociados y limitaciones que puedan contemplar los acuerdos suscritos por la compañía.