POLÍTICA DE DIVULGACIÓN DE VULNERABILIDADES

CSIRT Global Technology

Tipo de documento		**POLÍTICA**	
Versión	**Estado**	**Fecha**	**Autor**
V.0.0	Borrador	23/06/2020	Área de GRC
V.1.0	Derogado	23/11/2020	Área de GRC
V.1.2	**Vigente**	13/05/2021	Área de Cumplimiento normativo

Uso Público

Índice de Contenido

1 OBJETO Y CAMPO DE APLICACIÓN....3

2 DOCUMENTACIÓN....3

2.1 Estándares y regulaciones externas 3

2.2 Principal legislación.... 3

2.3 Documentación de referencia 3

3 TÉRMINOS Y DEFINICIONES....3

4 DESCRIPCIÓN....3

4.1 Recepción de vulnerabilidades 4

4.2 Cumplimiento legal en la búsqueda de vulnerabilidades.... 4

4.3 Informes de Vulnerabilidades 4

4.4 Reconocimiento a informantes.... 5

4.5 Publicación de vulnerabilidades 5

4.6 Divulgación coordinada de vulnerabilidades 5

4.6.1 Comunicación al proveedor afectado.... 6

4.6.2 Comunicación a clientes.... 6

4.6.3 Comunicación a otros equipos, partes interesadas y CSIRT de referencia.... 6

5 ROLES Y RESPONSABILIDADES....7

1 OBJETO Y CAMPO DE APLICACIÓN

Es objeto del presente documento exponer la política que Global Technology implementa para la divulgación de las vulnerabilidades que el CSIRT Global Technology pueda identificar en el ejercicio de su actividad profesional. Así como plasmar los procedimientos a seguir en dicho caso.

Lo preconizado en este documento es de aplicabilidad a las actividades de divulgación de vulnerabilidades llevadas a cabo por todo el personal del CSIRT Global Technology.

2 DOCUMENTACIÓN

2.1 Estándares y regulaciones externas

- ISO/IEC 29147:2018 - Tecnología de la información - Técnicas de seguridad - Divulgación de vulnerabilidad.
- UNE-ISO/IEC 27001:2014 Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.

2.2 Principal legislación

- N/A

2.3 Documentación de referencia

- Contexto del Equipo CSIRT GT

3 TÉRMINOS Y DEFINICIONES

- **Vulnerabilidad:** es un comportamiento o un conjunto de condiciones presentes en un sistema, producto, componente o servicio que "viola un implícito o política de seguridad explícita ". En otras palabras, es una debilidad o exposición que permite una consecuencia de seguridad.
- **0-day** (Ataque de día 0): Una nueva vulnerabilidad para la cual no se han creado parches o soluciones, y que se puede emplear para llevar a cabo un ataque.

4 DESCRIPCIÓN

Global Technology consciente del daño que las vulnerabilidades 0-day pueden causar al entorno de las tecnologías de la información y consiente del deber que tiene de mantener informado a sus clientes de las amenazas y riesgos de seguridad de las que pudiesen ser víctimas, así como, del deber que asume con la sociedad en general de contribuir con la seguridad de la información. En virtud de promover un marco de acción, que permita una divulgación coordinada de las posibles vulnerabilidades detectadas y con el objetivo principal y último de minimizar los riesgos de divulgar

dichas vulnerabilidades, además de ofrecer la oportunidad de actuar como puente para la recepción y escalado de vulnerabilidades detectadas por terceros, implementa la siguiente política para la divulgación de vulnerabilidades:

4.1 Recepción de vulnerabilidades

Global Technology pone a disposición de la comunidad en general su buzón de recepción de informes de vulnerabilidades, para aquellas personas que deseen compartir información de cualquier vulnerabilidad detectada tanto en sus sistemas como en otros que puedan afectar a sus clientes y la sociedad en general. Actuando como organización de contacto y facilitando el anonimato del informador, si así lo desease, (salvo requerimiento legal), o publicitando sus capacidades si así lo requiriese.

4.2 Cumplimiento legal en la búsqueda de vulnerabilidades

Es importante tener en cuenta que la búsqueda de vulnerabilidades no puede, ni debe ser una excusa para vulnerar las leyes establecidas en la materia. Y que el respeto a la ley en todo momento debe ser primordial. por ello, en la búsqueda de vulnerabilidades no se permiten llevar a cabo las siguientes acciones:

- Comprometer el sistema y mantener acceso persistente a los mismos.
- Hacer uso de malware.
- Hacer uso de ingeniería social.
- Utilizar y/o explotar la vulnerabilidad de cualquier modo que implique mayores acciones que demostrar su existencia haciendo uso de métodos no agresivos.
- Hacer uso de ataques de fuerza bruta o DoS o DDoS.
- Compartirla con terceros.

4.3 Informes de Vulnerabilidades

Los informes de vulnerabilidades deberán como mínimo contener, sin limitarse a ella, la siguiente información:

- Descripción clara y detallada de la vulnerabilidad
- Información clara y detallada de cómo se ha llegado a descubrir la vulnerabilidad. El objetivo es poder reproducirla.

Además,

- Pruebas de la existencia de la vulnerabilidad (captura de pantalla, enlace, etc.)
- Timeline o información temporal sobre el momento en el que se descubrió la vulnerabilidad.
- Cualquier tipo de información que considere necesaria para localizar y resolver la vulnerabilidad de la forma más rápida y eficaz posible.

En ningún caso los informes de vulnerabilidades compartidos con terceras partes incluirán datos de que faciliten la identificación de la infraestructura en la que ha sido detectada o explotada (si fuese el caso) a excepción de aquellos en los que se incurra en un requerimiento legal o a petición del afectado.

4.4 Reconocimiento a informantes

Global Technology reconoce el trabajo y el talento necesario para identificar dichas vulnerabilidades, así como la buena fe del informante al realizar la acción de informar, por ello, publicitará las cualidades del mismo, si así este lo desease, entre su entorno. Del mismo modo, si la organización afectada por la vulnerabilidad ofreciese compensaciones económicas, se posicionará como de punto de contacto entre los implicados.

4.5 Publicación de vulnerabilidades

Con el objetivo de evitar su posible explotación, Global Technology ***no divulgará por medio de ninguna red pública*** (web corporativa, ni redes sociales) las vulnerabilidades de 0-day detectadas en el ejercicio de sus funciones hasta pasado al menos un periodo de 60 días desde la comunicación a las partes interesadas de la identificación de la vulnerabilidad. Plazo que se estima oportuno en función de las premisas establecidas por el INCIBE-CERT para el tratamiento y reporte de vulnerabilidades.

No obstante, llevará a cabo los pasos que se desarrollan en los siguientes apartados, dejando el tiempo optimo que se estime oportuno, si así se considerase, en virtud de cada casuística y el desarrollo de los acontecimientos.

4.6 Divulgación coordinada de vulnerabilidades

Cuando en el ejercicio de sus funciones el CSIRT Global Technology identificase una vulnerabilidad 0-day, realizará las acciones oportunas para asegurar la completa cooperación con las partes interesadas con el objetivo de remediar la vulnerabilidad y minimizar el daño. Para ello:

- **Comunicará al proveedor afectado** el hallazgo, identificando, además del tipo de vulnerabilidad, toda aquella información relevante que haya recopilado sobre el comportamiento de la misma o su posible solución. Coordinará con el mismo los plazos para la publicación de la vulnerabilidad detectada, con el margen suficiente para que el proveedor actúe en consecuencia colaborando en la resolución de la vulnerabilidad si este lo solicitase.
- **Comunicará a los clientes afectados y los posibles clientes vulnerables** el hallazgo, bajo la premisa de confidencialidad y discreción, concienciándoles con las posibles consecuencias, para ellos y el entorno de la seguridad de la información, de la divulgación no controlada de este tipo de vulnerabilidades. Así como, recomendará las acciones oportunas para suprimir o mitigar el riesgo y apoyará a sus clientes, si así lo demandasen, en la implementación de las mismas.
- **Comunicará a otros equipos de seguridad de la información, otros CSIRT de referencia y otras partes interesadas** el hallazgo, con el objetivo de promover un ambiente de colaboración a la seguridad de la información, difundiendo las medidas llevadas a cabo para solventar o mitigar la amenaza.

Para realizar las diferentes comunicaciones Global Technology utilizará los medios técnicos y los flujos de comunicación a su disposición para proteger en todo momento la confidencialidad de la información.

4.6.1 Comunicación al proveedor afectado

Global Technology con el objetivo de contribuir a una solución rápida y eficaz de las vulnerabilidades detectadas, informará del hallazgo en primera instancia y tan pronto como sea posible al proveedor afectado. Coordinando con el mismo los pasos a seguir y las acciones necesarias para colaborar con la resolución de la vulnerabilidad, por medio de un informe detallado del hallazgo, tal y como se establece en el punto 4.3 del presente procedimiento.

Algunos proveedores cuentan con medios habilitados para la recepción de informes de vulnerabilidades, lo cual facilita enormemente la labor. No obstante, existen otros que, por su magnitud, internacionalidad, secretismo u cualquier otro motivo imposibilitan la comunicación. En este caso se pasará en primera instancia a remitir el informe de vulnerabilidad al INCIBE-CERT como principal CSIRT de referencia dentro del ámbito de actuación de Global Technology.

4.6.2 Comunicación a clientes

Dado que para Global Technology la seguridad de sus clientes es su principal preocupación, se informará a los mismos de las vulnerabilidades detectadas en sus sistemas en el mismo momento en que el equipo técnico las detecte.

Global Technology utilizará los medios seguros habilitados de comunicación para el envío de informe de vulnerabilidades a sus clientes. Esta comunicación se podrá llevar a cabo por diferentes canales en función de los procedimientos operativos acordados con el cliente:

- Correo electrónico seguro.
- Herramienta de comunicación de incidentes (ticketing)
- Repositorio compartido de información.
- Otros.

El equipo CSIRT Global Technology tratará los informes de vulnerabilidades con la confidencialidad y discreción que merece, en función de los requisitos legales y contractuales, y la gravedad de los mismos. Sin perjuicio del deber de notificar e informar a la autoridad competente a través del CSIRT de referencia de los incidentes que tengan efectos perturbadores significativos o los sucesos o incidencias que puedan afectar a las redes y sistemas de información empleados para la prestación de los servicios esenciales, pero que aún no hayan tenido un efecto adverso real sobre los mismos.

Si en el ejercicio de sus funciones, el equipo CSIRT GT topase con una vulnerabilidad no conocida hasta el momento, comúnmente denominadas 0-day, transmitiría dicha información a todos los clientes que pudiesen ser víctima de la misma por los medios atribuidos por este fin y siempre salvaguardando la confidencialidad de la información.

4.6.3 Comunicación a otros equipos, partes interesadas y CSIRT de referencia

Con el objetivo de contribuir a un aumento en la seguridad de la información general, en el contexto de la organización, Global Technology mantiene, promueve y fomenta el trabajo en equipo y la colaboración con otros equipos de seguridad de la información. dicha colaboración además de contribuir a un aumento general de la

seguridad contribuye a mantener un amplio espectro en la observación y detección de vulnerabilidades que ayuda a eliminar o mitigar estas de una forma más rápida y eficaz.

A su vez, Global Technology podrá servir de enlace técnico con el principal CSIRT de referencia a petición de sus clientes encargándose de las comunicaciones y notificaciones necesarias.

Global Technology podrá compartir información relativa a las características de las vulnerabilidades identificadas y medios de resolución con otras partes interesadas dentro del contexto de su organización, como pueden ser empresas colaboradoras, otros CSIRT y partners en función de las necesidades identificadas, bajo la premisa de necesidad de conocer y siempre sujetos al compromiso adquirido con la confidencialidad de la información. La información compartida en ningún caso contendrá datos del cliente o ninguna alusión que permita a terceros identificar el origen de la vulnerabilidad, salvo expresa autorización de este o requerimiento legal.

5 ROLES Y RESPONSABILIDADES

- La organización velará por la seguridad de sus clientes, así como por la confidencialidad de sus datos.
- La organización proporcionará los medios adecuados para la transferencia de información y las comunicaciones seguras con sus clientes.
- La organización fomentará un marco de trabajo colaborativo y participativo con otros CSIRT.
- La organización comunicará al CSIRT de Referencia las vulnerabilidades relevantes que pueda detectar en el ejercicio de sus funciones.
- La organización protegerá la identidad de los informantes salvo requerimiento legal, o publicitará sus capacidades en función de los deseos de los mismos.