GUÍA DE USO DEL PROTOCOLO TLP

TLP (Traffic Light Protocol o Protocolo de Semáforos)

Es un protocolo de comunicación que proporciona un esquema simple e intuitivo, para que quien origina la información, indique cuándo y cómo se puede compartir información sensible y confidencial; y, cuán ampliamente quiere que su información se distribuya más allá del destinatario inmediato.

Está diseñado para mejorar el flujo de información entre individuos, organizaciones o comunidades de forma controlada y confiable. Es importante entender y respetar las reglas del protocolo, ya que sólo entonces se puede establecer la confianza entre los involucrados.

El TLP se basa en el concepto de etiquetado, con el cual quien comparte la información, utiliza uno de los cuatro (4) colores definidos por este protocolo, para indicar el alcance de la difusión que el destinatario deberá dar a la información. La información de etiquetado consiste simplemente en agregar "TLP: COLOR" a un documento o parte de él.

A continuación se detalla los cuatro (4) colores utilizados en este protocolo:

Color	¿Cuándo utilizar?	¿Cómo debe ser compartida la información?	Ejemplo
	**DIFUSIÓN RESTRINGIDA** Cuando la información está limitada a personas concretas, debido a que su difusión a terceras personas podría tener un impacto en la privacidad, reputación u operaciones si es mal utilizada.	Los destinatarios no pueden compartir información de TLP: ROJO con nadie fuera del intercambio, reunión o conversación específica en la que se reveló originalmente. En caso de que se necesite dar a conocer a otra persona se deberá pedir autorización al emisor de la información. En la mayoría de los casos, TLP:ROJO debe intercambiarse de manera verbal o en persona. Los destinatarios no pueden compartir información con nadie, incluso en un nivel jerárquico superior.	1. Información compartida en una reunión o conversación. 2. Correo electrónico directo. (Con etiqueta TLP:ROJO)

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

 TLP:ÁMBAR	**DIFUSIÓN LIMITADA** Cuando la información requiere apoyo para que se actúe de manera efectiva, pero conlleva riesgos para la privacidad, la reputación o las operaciones, si se comparte fuera de las organizaciones involucradas.	Los destinatarios solo pueden compartir información de TLP:ÁMBAR con miembros de su propia organización, y otros actores que necesiten conocerla para protegerse o evitar daños mayores. Las fuentes tienen la libertad de especificar límites adicionales para compartirla.	Acuerdos de confidencialidad entre Centros de Respuesta a Incidentes Informáticos.
 TLP:VERDE	**DIVULGACIÓN LIMITADA DENTRO DE LA COMUNIDAD** Cuando la información es útil para el conocimiento de todas las organizaciones participantes.	La información recibida con etiqueta TLP:Verde puede circular libremente dentro de una comunidad en particular, pero no implica que sea información pública. Los beneficiarios pueden compartir la información con sus compañeros y organizaciones asociadas dentro de su sector o comunidad, pero no fuera de ella o a través de canales accesibles públicamente.	Compartir un análisis de malware dentro de una comunidad objetivo determinada.
 TLP:BLANCO	**DIVULGACIÓN SIN RESTRICCIÓN** Cuando la información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.	Se debe tener en consideración que al momento de su difusión, se deben respetar los derechos de autor.	

CONSIDERACIÓN FINAL

Aunque pueda ser tentador usar TLP:Red para algo sensible, esto puede evitar que sus destinatarios realicen una investigación adecuada o alertas en su entorno, ya que evitaría que sus destinatarios traten esta información con su equipo o personal técnico para un análisis posterior, ya que NO puede ser utilizada por quienes no estuvieron presentes durante la divulgación.

Se puede usar TLP:Red para obtener información sobre una amenaza, pero una mayor investigación (y comentarios) será bastante limitada, por lo que se sugiere el uso de

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

TLP: Ámbar con una restricción de constituyentes, por ejemplo: solo comparta esto con su equipo del CSIRT.

REFERENCIAS:

1. https://www.first.org/tlp/
2. https://www.ecucert.gob.ec/tlp.html
3. https://www.incibe-cert.es/tlp
4. https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/considerations-on-the-traffic-light-protocol
5. https://www.us-cert.gov/tlp
6. https://www.vanimpe.eu/2015/08/21/use-traffic-light-protocol-tlp/

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec