d

Montevideo, 23 de setiembre de 2024.

Desde Datasec felicitamos por todo el proceso llegado adelante para construir una estrategia de ciberseguridad nacional. Agradecemos a su vez esta instancia, y el haber sido invitados para participar y realizar aportes en instancias previas.

En este momento, y sobre la base de un borrador escrito disponible, y los plazos establecidos, quisiéramos hacer unos aportes finales puntuales.

Hay una idea central sobre las cuales quisiéramos trabajar este último aporte:

- **Una infraestructura tecnológica robusta proporciona la base necesaria para implementar medidas de ciberseguridad efectivas. Sin una infraestructura sólida, cualquier esfuerzo en seguridad puede ser insuficiente o fácilmente vulnerable.**

Esta idea central, basada en la experiencia que observamos en el día a día, nos llega a sugerir los siguientes aspectos:

1) Gobernanza de la IIC

Las Infraestructuras de Información Críticas (IIC) pueden tener en ciertos casos debilidades de Gobernanza, Gestión, y ausencia de objetivos de TI y Ciberseguridad.

Sugerimos entonces, establecer con mayor claridad la relación entre Pilar 1 y 5, específicamente en lo que refiere a las Organizaciones Relevantes y la IIC.

- Establecer que todas aquellas organizaciones que administran o gestionan IIC deben ser consideradas Organizaciones Relevantes, y por ende aplicarles las Líneas y acciones establecidos en el Pilar 1.

2) Infraestructura de TI Segura.

Las IIC, tanto en el sector público o privado, pueden estar corriendo en Infraestructura de TI obsoletas o significante inseguras por diversas razones. Establecer medidas de ciberseguridad en estos contextos es significativamente más complejo o inviable sin antes atacar la causa raíz del problema a nivel de sistemas o aplicaciones obsoletas o diseños inseguros.

Sugerimos entonces incluir acciones en la Línea 5.2 Proteger las IIC, que podrían ser adaptadas en las ya establecidas de esta forma:

- Promover la cultura de la ciberseguridad y la capacitación en todos los niveles, concientizando y capacitando a los diferentes actores involucrados en la gestión de las IIC sobre la importancia de contar con una Infraestructura de TI robusta y segura, su ciberseguridad y las mejores prácticas para protegerlas.
- Establecer mecanismos de financiamiento adecuados para garantizar la implementación de: Infraestructuras de TI robustas y seguras por diseño, la remediación de vulnerabilidades o debilidades relevantes, así como otras medidas de ciberseguridad en las IIC.
- ** En este mismo punto se podría establecer que las organizaciones involucradas en la administración o gestión de IIC serán considerados Organizaciones Relevantes para cumplir con lo establecido en el Pilar 1, en especial a nivel de Objetivos de Gestión.

3) Promover el uso de soluciones de TI y ciberseguridad robustas.

En el contexto del Pilar 6, entendemos que sería valioso sumar otras acciones que empoderen a las personas de mejor forma para hacer frente a las amenazas.

Por ejemplo:

- Promover el uso de soluciones de TI actualizadas, antimalware robustos, así como otras herramientas fundamentales para proteger los dispositivos..."
- Estudiar mecanismos para el desarrollo de programas de acceso a servicios y herramientas de ciberseguridad con foco en las personas.

Nuevamente agradecemos por la oportunidad de seguir aportando, y quedamos a las órdenes como siempre.