Montevideo, 4 de marzo de 2021.

Señora Presidenta de la
Cámara de Senadores
Esc. Beatriz Argimón

De mi mayor consideración:

De acuerdo con lo dispuesto por el artículo 118 de la Constitución de la República, solicito se curse al Ministerio del Interior y por su intermedio a la Dirección Nacional de Identificación Civil (DNIC) , el siguiente pedido de informes:

Habiendo tomado conocimiento del incidente informático que tuvo lugar en los servidores de la DNIC, detectado el día 8 de diciembre de 2020, solicito al Sr. Ministro informe:

1. **¿Cómo calificó el CERTuy dicho incidente informático ? ¿Qué tipo de incidente tuvo lugar y con qué severidad?**

2. **¿Qué tipo de vulnerabilidad fue explotada por parte de los atacantes?, ¿había sido detectada con anterioridad por CERTuy o personal propio?. De ser así, ¿existían acciones de mitigación pendientes de ejecución?, ¿cuáles?, ¿por qué estaban pendientes?**

3. ¿Cuáles fueron las medidas técnicas, operativas y administrativas desplegadas para contrarrestar el evento?

4. De las recomendaciones planteadas por CERTuy como parte de su informe, ¿qué plan de acción han definido el Ministerio del Interior y la DNIC para su implementación?

5. Si bien se concluyó que "no se detectaron pérdidas de información", puede asegurarse que los atacantes no lograron obtener información desde la DNIC? De no ser así, ¿cuáles son los activos e información contenidos en la infraestructura comprometida a la que accedieron los atacantes?

6. **¿Qué activos de información fueron comprometidos por el incidente informático?, ¿Qué datos o tipo de contenido alojan esos activos?**

7. ¿Cuál es el volumen de información potencialmente afectada por el incidente? (cantidad de registros, cantidad de archivos, cantidad de ciudadanos de los que sus datos pueden estar comprometidos)

8. Listar la información sensible, reservada, confidencial y/o personal que puede haber sido accedida o afectada durante el incidente.

9. Listar la información sensible, reservada, confidencial y/o personal que con certeza se puede asegurar que no fue accedida o afectada durante el incidente.

10. En caso de haberse vulnerado (o se haya detectado probabilidad de vulneración) de datos personales, ¿se informó a la Unidad Reguladora y de Control de Datos Personales (URCDP) por parte del responsable o encargado de la base de datos?

    A partir de la nueva legislación, cuando el responsable o encargado de una base de datos tome conocimiento de que se ha vulnerado la seguridad de dicha base, deberá informarlo de inmediato, conjuntamente con las medidas adoptadas, tanto al titular de los datos como a la URCDP, quien coordinará con el Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay (CERTuy) los pasos a seguir.
    From <https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/cambios-recientes-legislacion-sobre-proteccion-de-datos-personales-en>

11. ¿Qué indicios, errores u omisiones detectados motivaron llevar adelante una "investigación administrativa"?. ¿Qué alcance tiene dicha investigación ?

12. Luego de las pericias realizadas, ¿desde qué momento se estima que los atacantes contaban con acceso al o los servidores/sistemas/datos?

13. ¿Qué acciones de remediación se ejecutaron por parte de la DNIC previo a informar a CERTuy?

14. ¿Se tienen indicios de que exista sabotaje interno?

15. ¿Qué contiene la denuncia realizada a la justicia, en la que está trabajando la fiscal Silvia Perez?

16. Se reportó que "en función de la alta demanda en la solicitud de audiencias para renovar el documento de identidad u obtenerlo por primera vez" se dio de baja la expedición de turnos en línea.. ¿Cuál fue el nivel de demanda recibido durante este año?, ¿se identificó un perfil de consultas distintas a la habitual, en relación a país de procedencia, días/horas u otras características?, ¿cómo se compara con igual período de 2020?. Se solicita se brinde detalle de la utilización del sitio, como ser cantidad de consultas por hora y lugar de origen de cada consulta.

17. ¿Qué acciones se han tomado para lograr retomar el servicio de reserva on line para obtener el documento de identidad?

18. ¿Qué riesgos remanentes se entiende que aún existen en la realidad actual de estos servidores/sistemas?, ¿Qué plan se ha elaborado para su gestión?

19. ¿Cómo ha implementado la DNIC el "Marco de Ciberseguridad" definido por Agesic?. ¿Qué acciones concretas se han ejecutado?
https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-de-ciberseguridad

20. ¿Qué establece la Política de Seguridad de la Información del Ministerio del Interior y de la DNIC para la mitigación de ataques informáticos y fugas de información?. ¿Se identificaron omisiones o errores en este caso con respecto a la política establecida?

Decreto 452-009 - Las Unidades Ejecutoras de los Incisos 02 al 15 del Presupuesto Nacional, deberán adoptar en forma obligatoria una Política de Seguridad de la Información, tomando como base la "Política de Seguridad de la Información para Organismos de la Administración Pública"
From <https://www.impo.com.uy/bases/decretos/452-2009>

21. ¿Se han realizado recomendaciones/observaciones por parte del CERTuy al Ministerio del Interior o a la DNIC en función de su cometido de "proteger los sistemas informáticos que soporten activos de información críticos del Estado"?. ¿Qué acciones han definido y ejecutado el Ministerio del Interior y la DNIC al respecto?, ¿Qué acciones quedan pendientes? ¿Cuál es el plan de acción y sus prioridades?

22. ¿Se ha alertado por parte del CERTuy al Ministerio del Interior o a la DNIC sobre amenazas y vulnerabilidades de seguridad en sistemas informáticos del organismo? ¿Qué acciones se tomaron al respecto?

Cometido CertUY: "Alertar ante amenazas y vulnerabilidades de seguridad en sistemasinformáticos de los organismos"
From <https://www.impo.com.uy/bases/decretos/451-2009>

23. ¿Qué medidas específicas ha tomado la DNIC para la protección de sus activos de seguridad críticos ?

Articulo 8: Obligaciones de los organismos. Los organismos establecidos en el art. 2 del presente Decreto tendrán las siguientes obligaciones:
a) Informar de forma completa e inmediata la existencia de un potencial incidente de seguridad informática.
b) Adoptar medidas de seguridad eficientes para proteger sus activos de información críticos.
c) Responder por la integridad de la información generada o en su poder.

From <https://www.impo.com.uy/bases/decretos/451-2009>

24. ¿Cuenta el Ministerio del Interior con un Centro de Operaciones de Ciberseguridad?. ¿Quiénes son sus responsables?, ¿Cómo opera?, ¿Qué acciones ha tomado últimamente?

A modo de ejemplo, el M. Turismo esta formando uno:
<https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/noticias/centro-operaciones-ciberseguridad-ministerio-turismo>

25. ¿Cuáles son las actividades que lleva adelante el Ministerio del Interior y la DNIC para analizar periódicamente los riesgos asociados a sus activos de información críticos?. ¿Qué resultados han tenido últimamente? ¿Qué acciones se han llevado adelante?

26. ¿Qué capacitación y entrenamiento ha recibido el personal de Tecnología de la Información del Ministerio del Interior y de la DNIC en el último año ?
27. La Ley 19.670 estableció la obligatoriedad de incorporar la figura del "delegado de protección de datos". ¿A quién designó la DNIC en este rol?, ¿Cuándo se realizó la designación?, ¿Qué acciones ha llevado adelante desde su designación?

    La normativa hoy vigente establece que las entidades públicas y las privadas que traten grandes volúmenes de datos o datos sensibles como negocio principal deben incorporar obligatoriamente la figura del "delegado de protección de datos". Este tendrá entre sus funciones asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales; supervisar el cumplimiento y proponer las medidas pertinentes para adecuarse a la normativa y a los estándares internacionales en la materia y actuar como nexo entre su entidad y la URCDP.

    From <https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/cambios-recientes-legislacion-sobre-proteccion-de-datos-personales-en>

28. Considerando la condición de infraestructura crítica de los activos de la DNIC, ¿cuáles son las decisiones técnicas, de diseño e implementación que se llevan adelante para garantizar la continuidad operativa?
    ¿Existe infraestructura de contingencia en modalidad activo-activo?,¿cuál es la geodistribución de la infraestructura?, ¿Cuál es el plan de recuperación ante desastres o incidentes críticos que afecten disponibilidad?,
    ¿Cuáles son las acciones llevadas adelante para maximizar la seguridad de la información?

En el entendido que parte de esta información puede ser de carácter confidencial y reservado, quizás sea más apropiado que parte de la información solicitada se nos brinde en una reunión con quienes serán los responsables de las respuestas. Dejamos a vuestra consideración la forma atentos a que nuestro interés es comprender a cabalidad la situación.

Silvia Nane
Senadora