INFORME DE CIBERSEGURIDAD

Organismo: Ministerio de Turismo de la Provincia de la Provincia de Misiones

Asunto: Evaluación de seguridad tras la publicación de datos en foros de la dark web

Fecha: 06 de marzo de 2025

Responsable: Mauricio Alvez

Área de desempeño: Subsecretaría de Marketing y Promoción de Eventos

---

1. Antecedentes

En los últimos días, se detectó la publicación en un foro de la dark web de datos provenientes de las bases de datos del Ministerio. Aunque la información expuesta es pública, su uso para fines no éticos representa un riesgo reputacional y de seguridad. Ante esta situación, se ha realizado un análisis de seguridad y se han tomado medidas correctivas y preventivas.

2. Análisis de Seguridad Actual

Se han revisado los sistemas web del Ministerio de Turismo para evaluar la posible causa de la filtración y la robustez de las medidas de seguridad implementadas. Los hallazgos encontrados por los especialistas Cristian Aranda y Mauricio Alvez son los siguientes:

1. **Certificados SSL**: El dominio principal y los subdominios cuentan con certificados SSL vigentes, garantizando la encriptación de las comunicaciones.
2. **Seguridad del Hosting**: El servicio de hosting contratado incluye medidas de seguridad como firewalls, detección de intrusiones y protección contra DDoS.
3. **Accesos no autorizados**: No se han detectado ingresos sospechosos a los paneles de administración.
4. **Protección de carpetas y aplicaciones**: Los directorios sensibles están protegidos con contraseñas seguras y sistemas de autenticación.
5. **Configuración de .htaccess**: Los archivos `.htaccess` están configurados para restringir consultas peligrosas a las bases de datos y prevenir ataques de inyección SQL.
6. **Consultas SQL seguras**: Se utilizan consultas preparadas con parámetros en PDO para prevenir inyecciones SQL.
7. **Correos electrónicos corporativos**: Es fundamental identificar y corroborar cuáles son las cuentas activas que están en uso efectivo para evitar accesos no controlados y minimizar riesgos de seguridad.

3. Medidas Implementadas y en Evaluación

Ante esta situación, se han adoptado y se están evaluando las siguientes medidas adicionales:

1. **Monitoreo de la dark web**: Se está evaluando la contratación de un servicio especializado para detectar futuras filtraciones.
2. **Revisión y actualización de sistemas**:
    - Auditoría de accesos y registros de actividad en bases de datos.
    - Refuerzo de políticas de acceso y autenticación de usuarios.
    - Actualización y aplicación de parches de seguridad en software y sistemas operativos.
3. **Refuerzo de protecciones en bases de datos**:
    - Implementación de cifrado de datos sensibles.
    - Monitoreo de consultas inusuales o sospechosas.
4. **Campaña de comunicación**:
    - Se está informando a la ciudadanía que el Ministerio no solicita información por canales no oficiales para evitar posibles intentos de phishing o fraude.

4. Riesgos de Seguridad Adicionales

El uso de software no oficial, la mezcla de cuentas personales con cuentas laborales, el uso de software pirata, hardware obsoleto y dispositivos personales representan riesgos significativos para la seguridad de la información:

- **Falta de aplicaciones oficiales y licencias**: El uso de software no oficial o sin licencia impide recibir actualizaciones de seguridad esenciales, dejando vulnerabilidades abiertas que pueden ser explotadas por atacantes.
- **Mezcla de cuentas personales y laborales**: Utilizar cuentas personales para actividades de trabajo puede exponer información confidencial en plataformas menos seguras y aumentar el riesgo de accesos no autorizados.
- **Software pirata**: El uso de software sin licencia no solo es ilegal, sino que también representa un alto riesgo de infección con malware, spyware o puertas traseras que pueden comprometer sistemas completos.
- **Hardware obsoleto**: Equipos sin soporte técnico o actualizaciones de firmware pueden ser puntos de entrada para ataques, ya que no cuentan con los parches de seguridad necesarios para protegerse contra amenazas modernas.
- **Uso de dispositivos personales**: La utilización de computadores, teléfonos móviles o memorias USB personales en tareas laborales incrementa el riesgo de fuga de información, infección con malware y accesos no controlados. Estos dispositivos suelen carecer de las mismas medidas de seguridad que los equipos corporativos.

Es fundamental garantizar el uso de software y hardware seguros, separar los entornos de trabajo y personales, y actualizar constantemente los sistemas para minimizar riesgos de ciberseguridad.

5. Recomendaciones Adicionales

A la luz del incidente, se recomienda:

- **Implementación de Autenticación Multifactor (MFA)** para accesos administrativos y usuarios clave.
- **Monitoreo continuo de logs** para identificar posibles intentos de acceso no autorizado.
- **Pruebas de penetración periódicas** para evaluar vulnerabilidades.
- **Reforzar la capacitación en ciberseguridad** para empleados, previniendo ataques de phishing y otras amenazas.
- **Backup de bases de datos y configuraciones** con verificación de integridad periódica e implementación de mecanismos de respaldo y recuperación de correos electrónicos críticos, base de datos y sistema de archivos, asegurando la disponibilidad de información en caso de incidentes de seguridad o pérdida de datos.
- **Uso de sistemas de detección de intrusiones (IDS/IPS)** para alertar sobre actividades sospechosas.
- **Políticas de uso de dispositivos personales**, restringiendo su acceso a información sensible y exigiendo medidas de seguridad como antivirus actualizado y cifrado de datos, como también establecer normas claras sobre el uso del correo corporativo, restringiendo su utilización a fines laborales y prohibiendo su uso para actividades personales o en plataformas no autorizadas
- **Concienciación y capacitación**: Es imprescindible instruir a los usuarios con acceso a los sistemas y correos electrónicos oficiales sobre buenas prácticas de seguridad, como la gestión segura de contraseñas, identificación de intentos de phishing y la importancia de no compartir credenciales.

6. Conclusión

Si bien no se han detectado vulnerabilidades críticas en los sistemas, el incidente resalta la necesidad de un monitoreo constante y la implementación de medidas adicionales para proteger la información del Ministerio. Se continuará con la evaluación de las estrategias mencionadas para reforzar la seguridad y mitigar riesgos futuros.

El presente informe se remite para su consideración y toma de decisiones sobre las medidas a adoptar.