CIRCULAR VICETIC Nº 003/2024

El Viceministerio de Tecnologías de la Información y Comunicación "VICETIC" del Ministerio de Tecnologías de la Información y Comunicación "MITIC", solicita a los *Responsables de Seguridad de la Información "RSI"* o Directores Generales o Directores o Jefes o Encargados de áreas de Tecnologías de la Información y Comunicación "TIC", de Organismos y Entidades del Estado "OEE", realizar de forma prioritaria una revisión exhaustiva de la administración de sitios web institucionales oficiales, muy especialmente los concrete/wordpress, de modo a validar que las medidas de protección de las cuentas, y actualización de los sitios estén activas, considerando el creciente número ciberataques a estos.

La revisión debe contemplar mínimamente:

- Verificar que todos los **usuarios estén bien identificados** con nombre y apellido. No usar cuentas genéricas y compartidas.
- Revisar y otorgar **solamente los permisos necesarios**, de acuerdo a las funciones de cada usuario.
- Validar uso de contraseñas robustas y únicas. Mínimamente 16 caracteres, combinando mayúsculas, minúsculas, números y caracteres especiales. No reutilizar otras contraseñas o repetirlas.
- Usar un gestor de contraseñas para almacenarlas de forma segura. No guardar en documentos de texto plano y/o navegadores.
- Asociar las cuentas de usuarios **solamente a cuentas de correo institucionales** nombre@institucion.gov.py. En ningún caso, usar cuentas particulares de gmail, hotmail, o similares.
- Eliminar cuentas de usuarios inactivos y/o que ya no pertenecen al OEE.
- Activar plugins de seguridad. Utilizar wordfence y activar funciones de seguridad:
    - **Activar la obligatoriedad de autenticación de doble factor para todos los usuarios.**
    - Activar las notificaciones al administrador sobre eventos de seguridad en la plataforma.
    - Limitar los intentos fallidos de inicios de sesión, y activar el bloqueo de IP.
- Evitar la conexión a la administración del sitio web desde redes públicas sin las medidas de seguridad necesarias.
- Activar las actualizaciones automáticas de la plataforma y de los plugins que contienen parches para corregir vulnerabilidades. Configurar el horario de actualización y demás detalles.
- Desactivar y eliminar los plugins que sean utilizados.
- Realizar copias de seguridad y probar la restauración de forma periódica. Almacenar las copias offline.
- Validar que el sitio web cuente con certificados SSL y mantenerlo actualizado.
- Verificar los dispositivos desde donde se accede a la plataforma:
    - Instalar y mantener actualizado el software antivirus.
    - Utilizar solamente software descargado desde sitios web oficiales, ya que existe el riesgo de infección por malware y por tanto exfiltración de datos como credenciales de usuarios, cuando se instalan programas no oficiales.
    - Validar la actualización periódica de los navegadores.
    - Activar las actualizaciones automáticas en el sistema operativo.

Obs. *La administración y mantenimientos técnicos de páginas web institucionales deben estar bajo el control de las áreas de TIC y/o Seguridad de la Información del OEE. Se debe evitar delegar estas tareas a áreas de prensa o similares y/o empresas externas tercerizadas. Solamente la gestión del contenido podrá ser delegada a otras áreas.*

El plazo para realizar la revisión vence el 16/08/24

Recordamos que todo Incidente Cibernético en el OEE debe ser reportado al RSI institucional y éste al Centro de Respuestas ante Incidentes Cibernéticos (CERT-PY) detallando el incidente en el correo abuse@cert.gov.py. Para otras consultas se puede escribir un correo electrónico a: ciberseguridad@mitic.gov.py.

JUAN MIGUEL ARDISSONE
Firmado digitalmente por JUAN MIGUEL ARDISSONE
Fecha: 2024.08.06 14:34:43 -04'00'

Viceministerio de Tecnologías de la Información y Comunicación
MITIC