CIRCULAR Nº01/2021

El Ministerio de Tecnologías de la Información y Comunicación (MITIC) autoridad en materia de ciberseguridad, conforme a las competencias otorgadas mediante el artículo 7, inciso 4 y 23 de la Ley N° 6.207/2018 "Que crea el Ministerio de Tecnologías de la Información y Comunicación, y establece su carta orgánica", así como los artículos 43 a 46 del Decreto N° 2.274/2019 mediante el cual se reglamenta la citada Ley, y en vista a la creciente amenaza de incidentes cibernéticos de ransomware, que involucran el secuestro virtual de activos digitales y la consecuente extorsión con miras a su recuperación, su potencial impacto en el funcionamiento de instituciones gubernamentales y las tendencias en cuanto a las tácticas y técnicas utilizados actualmente por los criminales, se recuerda a todos los Organismo y Entidad del Estado (OEE) tomar los recaudos pertinentes, incluyendo, pero no limitado a, las siguientes directivas:

1. Todo Organismo y Entidad del Estado (OEE) debe contar con un inventario de activos, en el cual tenga identificado claramente aquellos activos de información digitales imprescindibles para el funcionamiento de su organización. Esto incluye, pero no se limita a: documentos ofimáticos, archivos de base de datos, archivos separados por comas, correos electrónicos, códigos fuentes, imágenes de sistemas operativos y virtualizaciones. Para realizar este inventario, se debe tener en cuenta, como mínimo, las siguientes consideraciones:

1.1. Involucre a todas las áreas relacionadas a los procesos críticos de la institución.

1.2. Identifique y documente claramente qué información o datos son imprescindibles para cada proceso.

1.3. Identifique y documente claramente en qué ubicación o medio se almacena dicha información o datos.

1.4. Identifique y documente claramente los usuarios responsables del almacenamiento de dicha información o datos.

2. Todo OEE debe establecer una política o protocolo de gestión de respaldo de seguridad, con procedimientos, mecanismos o herramientas específicas para cada activo de información digital identificado como imprescindible. Se debe cumplir, mínimamente, con las recomendaciones expuestas del "Control 10: Capacidad de recuperación de datos" de la Resolución MITIC Nº 277/2020 - POR LA CUAL SE ACTUALIZA LA GUÍA DE CONTROLES CRÍTICOS DE CIBERSEGURIDAD DEL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN:

2.1. Asegurar los respaldos regulares, preferentemente automatizados, de todos los sistemas o activos de información digitales imprescindibles.

2.2. En el caso de sistemas de información críticos, siempre que sea posible, se debe realizar respaldos como un sistema completo, a través de procesos tales como imágenes, para permitir la recuperación rápida del sistema.
2.3. Probar la integridad de los datos en los medios de copia de respaldo de forma periódica mediante la realización de un proceso de restauración de datos para garantizar que la copia de respaldo funcione correctamente.
2.4. Asegurar la protección adecuada de las copias de respaldo de los activos de información, tanto a nivel de seguridad física como a nivel lógico, preferentemente mediante cifrado. La copia de seguridad debe contar con el mismo nivel de protección que el activo original.
2.5. Asegurar que las copias de respaldo tengan al menos un destino offline (no accesible vía red), tal que un malware que infectara el equipo no pueda aprovechar los mecanismos legítimos de copiado para alterar las copias de seguridad guardadas.

3. Los procedimientos de respaldo de cada activo de información digital identificado como imprescindible deben contener, como mínimo, la siguiente información:
3.1. La persona o área responsable de realizar la copia de seguridad de cada activo de información.
3.2. La ubicación o medio en la que se almacenará la copia de seguridad de cada activo (medios extraíbles, discos externos, dispositivo de almacenamiento, servicio en la nube, u otros). En ningún caso se debe almacenar la copia de seguridad en el mismo dispositivo que el activo original. Para la elección de la ubicación o medio de destino, se deberá tomar en cuenta, como mínimo, las siguientes consideraciones:
   i. Disponibilidad de medios.
   ii. Espacio requerido.
   iii. Frecuencia requerida.
   iv. Necesidad de retención de copias.
3.3. En el caso de procedimientos automatizados, la herramienta mediante la cual se realizará la copia de cada activo de información, así como el tipo de copia (completo, incremental, diferencial, etc.).
3.4. La periodicidad de las copias de seguridad. Ésta debe estar acorde a la periodicidad con la que se modifica cada activo de información y la tolerancia de pérdida de datos de éste (continuo, diario, semanal, mensual, etc.).
3.5. Anualmente deben realizarse como mínimo pruebas de recuperación de los respaldos, así como también la persona o área responsable de ejecutar esas pruebas. La periodicidad de estas pruebas debe determinarse de acuerdo a la criticidad de los datos, la necesidad de recuperación, entre otros factores. En ningún caso, la frecuencia de las pruebas podrá ser inferior a anual.
3.6. La ubicación o medio del destino offline en el que se almacenará la copia y la periodicidad con la que se almacenará en dicho destino.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

4. Todo OEE deberá implementar medidas de seguridad básicas tendientes a minimizar el riesgo de infección de ransomware, las cuales incluyen, pero no se limitan a:

4.1. Identificar los equipos de su red con servicios expuestos a Internet, especialmente Escritorio Remoto (Remote Desktop Protocol - RDP) y adoptar medidas de protección específicas, tales como:

i. Limitar la exposición del servicio a Internet, ya sea a través del uso de VPN y/o mediante filtrado de IPs.
ii. Asegurar que los usuarios locales del equipo, así como usuarios del dominio que inician sesión en el equipo, cuenten con contraseñas robustas. Preferentemente, utilice autenticación de doble factor.
iii. Verificar las credenciales almacenadas en el equipo, incluida aquellas del dominio que hubieran iniciado sesión en el pasado. Puede realizarlo desde el Administrador de Credenciales de Windows[1].
iv. Asegurar que los componentes del servicio se encuentren actualizados.
v. Implementar políticas de bloqueos ante un número determinado de intentos de acceso.

4.2. Instruir y concienciar periódicamente a los usuarios de la institución, a tomar los recaudos necesarios al momento de recibir correos electrónicos, incluido, pero no limitado a:

i. Evitar abrir correos sospechosos no solicitados.
ii. Evitar ingresar en enlaces o abrir archivos adjuntos en los correos sospechosos o de dudosa procedencia.
iii. Verificar siempre la dirección de correo electrónico del remitente.

4.3. Asegurar que todos los equipos de la institución cuenten con antivirus activado, actualizado y configurado de tal manera que no pueda ser desactivado localmente.

4.4. Mantener actualizados los sistemas operativos, navegadores, aplicaciones, clientes de correo, ofimática y demás programas de usuario.

4.5. Identificar los servicios expuestos a Internet, tales como servidores web, correo, aplicaciones de gestión de equipos de red, entre otros y asegurar que los mismos se encuentren actualizados y con credenciales robustas.

5. En caso de que el OEE no disponga de los medios físicos o lógicos adecuados o suficientes para almacenar los respaldos de sus activos de información digitales imprescindibles, deberá notificar al MITIC, a través de una nota oficial solicitando una asistencia. El MITIC, en la medida de sus posibilidades, buscará facilitar los medios necesarios.

6. El Responsable de Seguridad de la Información o en su defecto el Director de TIC del OEE o equivalente, serán los responsables de realizar las acciones y

[1] https://support.microsoft.com/es-es/windows/obtener-acceso-al-administrador-de-credenciales-1b5c916a-6a16-889f-8581-fc16e8165ac0

gestiones necesarias tendientes a la implementación de las directivas de la presente Circular en su organización.

7. Se recuerda además que, en caso de sufrir un incidente cibernético relacionado a ransomware o cualquier otro incidente de seguridad, el mismo debe ser reportado obligatoriamente al MITIC, conforme lo establecido en la Resolución MITIC N° 346/2020.

Asunción, 30 de marzo de 2021

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
REPÚBLICA DEL PARAGUAY
MITIC

Fernando Saguier Caballero Bernardes
Ministro Interino - MITIC