Industria y Comercio
SUPERINTENDENCIA

ANEXO

Controles documentados a partir de lección aprendida

1. Datos generales

Área: Grupo de Estudios Económicos (GEE-SIC)

Fecha de documentación: 2022-05-25

Tema: Visualización de archivos del GEE que se tenían almacenados en la carpeta de Google Drive que contienen la extensión **.remk**

Plan, programa proyecto asociado: Plan de Acción del GEE-SIC

2. Describa la situación o experiencia

El pasado 9 de febrero de 2021 se reportó ante la mesa de servicio la existencia de archivos almacenados en la carpeta de Google Drive bajo la extensión **.remk**. Según lo indicado, este tipo de archivo está asociado a un nuevo ataque de tipo *Ransomware* por lo que el área de Seguridad Informática procedió con su respectiva investigación y recolección de evidencias.

3. Impacto frente a los resultados

Activos afectados: Computadores de los funcionarios y contratistas del GEE-SIC.

Áreas de la entidad afectadas: GEE-SIC.

Descripción de las acciones de contención: Se bloquean las cuentas de 10 usuarios para que no puedan acceder a Google Drive. A nivel de la consola de antivirus de McAfee, se realiza el bloqueo de esta firma, pero esta protección solo les aplica a los usuarios que tenga equipos del dominio de la SIC, no personales. Se bloquea también el acceso a VPN para los usuarios identificados.

Resultados de las acciones: Usuarios quedan sin acceso a la información disponible en Google Drive necesaria para el desarrollo de su trabajo, pero entienden la gravedad del incidente. El equipo de Seguridad y de Correo proceden a realizar el ambiente donde se evidencian los archivos maliciosos.

4. Soluciones o acciones de mejora

4.1 Se eliminan los archivos infectados con la extensión **.remk** de todas las cuentas de Google Drive para todos los usuarios de la SIC. Se desinstalan los accesos directos a Google Drive que tienen configurados los equipos. Se realizan escaneos de antivirus con las herramientas McAfee y Malware Bytes sobre todos los equipos de los usuarios implicados, las evidencias se adjuntan en la sección.

4.2 Se solicita a la Mesa de Servicios realizar el *reset* de contraseñas de dominio.

4.3 Se habilita el acceso a VPN y a la cuenta de Google Drive solo a los usuarios que tienen sus equipos libres de malware.

4.4 Se obtuvieron varios resultados de malware en los equipos de la SIC, pero fueron eliminadas por las herramientas mencionadas. Cabe aclarar que esta tarea se realizó solo para equipos que estaban en el dominio de la SIC, no para equipos personales. Para habilitarles el acceso a los usuarios que tengan equipo personal, estos deberán contar con un certificado de que su equipo está libre de malware para que los recursos internos de la entidad estén fuera de riesgo.

5. Lección aprendida

5.1 Que toda la información del grupo siempre debe tener un respaldo, por ejemplo, *Backups* y espacio repositorio con el fin de:

- Prevenir pérdida de información,
- Evitar reprocesos; y,
- Disponer de la información de manera permanente

5.2 Los equipos de cómputo siempre deberán disponer de software y antivirus licenciado y actualizado, esto con el fin de prevenir el ataque de virus en la información.

5.3 La necesidad de articular o coordinar cada una de las áreas involucradas al interior de la entidad.

5.4 La necesidad de definir tiempos de atención y criterios establecidos documentalmente en materia de esta clase de eventos.

6. Recomendaciones para obtener mejores resultados en situaciones similares

6.1 Implementar auditorias de manera permanente a todos los equipos de la entidad con el objeto de garantizar que se están cumpliendo con las directrices dispuestas en materia de seguridad de la información.

6.2 Documentar lineamientos en materia de seguridad de la información, donde se determinen controles y aplicación de políticas de seguridad de la información.

6.3 Fomentar a través de capacitación y divulgación los lineamientos con el objeto de garantizar una cultura organizacional en materia de seguridad de la información.

7. Actividades

El GEE-SIC ha documentado el ejercicio de la implementación de actividades que progresivamente se han venido aplicando con el objeto de mitigar el riesgo materializado y evitar así que se vuelva a presentar un evento que ponga en riesgo la información del GEE-SIC. Lo anterior, se detalla a continuación:

7.1 Crear carpeta GEE-SIC

En el OneDrive, denominada: ARCHIVO, seguida de la vigencia (año)

Una vez creada la CARPETA por vigencia, esta incluirá una serie de SUBCARPETAS las cuales contendrán toda la información de los documentos correspondientes a las series documentales establecidas en la Tabla de Retención Documental (TRD) del GEE-SIC.

7.2 Asignación de Roles y permisos

Para el personal que accede a la información del GEE-SIC en el almacenamiento en la nube OneDrive.

7.3 Rol de Administradora:

El (la) Coordinador(a) del GEE-SIC tendrá el control de la carpeta en el OneDrive y será quien:

- Creará las carpetas
- Autorizará accesos y eliminará accesos
- Verificará mensualmente el estado de permanencia de los integrantes autorizados.

7.4 Rol de Apoyo Documental

Funcionarios y contratistas del GEE-SIC podrán acceder a la información de la carpeta del GEE en el OneDrive, para realizar todas las actividades pertinentes y relacionadas con el almacenamiento y gestión documental de los documentos del GEE.

7.5 Rol de Edición

Todos los funcionarios y contratistas del GEE-SIC podrán acceder a la información y editar lo contenido en ella.

7.6 Rol de observación

A criterio del (la) Coordinador(a), corresponde al personal que por razones de su actividad deban consultar información contenida en la carpeta GEE del OneDrive sin posibilidad de editarla.

7.7 Rol de BackUp

Para el backup realizado por el Grupo de Informática Forense y Seguridad Digital, se designará mediante correo electrónico institucional dirigido al GEE-SIC al funcionario o contratista autorizado para realizar periódicamente el BackUp y actualización de la información contenida en el almacenamiento en la nube OneDrive.

8. Autorizaciones

De acceso a la carpeta del GEE creada en OneDrive.

8.1 La Coordinación autoriza acceso a personal que se encuentre asignado al GEE como funcionario o contratista.

8.2 Funcionario GEE: personal asignado mediante acto administrativo en calidad de funcionario de carrera administrativa o de provisionalidad.

8.3 Contratista GEE: personal que cuente con contrato de prestación de servicios vigente.

8.4 A personal externo al GEE, que, por eventos relacionados con seguridad de la información o actividades de auditoría, deba acceder a la carpeta OneDrive para realizar ejercicios de auditoria o Backups de la información.

9. Eliminación de las Autorizaciones

De acceso a la carpeta GEE en el OneDrive:

9.1 La Coordinación elimina autorización de acceso cuando ya no se encuentre asignado al GEE-SIC el funcionario o contratista o por razones de eventos que se presenten sin ser autorizados o vinculados y que en las revisiones que se realicen llegasen a encontrarse desviaciones.

9.2 Funcionario, que por decisiones administrativas haya sido trasladados a otra dependencia o por desvinculación de la entidad y ya no pertenezcan al GEE-SIC (funcionarios de carrera administrativa o provisionalidad).

9.3 Contratistas GEE, que ya no cuenten con contrato de vinculación asignado al GEE para la vigencia presente se retirará acceso de edición a la carpeta GEE del OneDrive.

9.4 A personal externo al GEE, que por eventos relacionados con seguridad de la información ya no les corresponda realizar actividades relacionadas con ejercicios de auditoria o Backups de la información.

10. Control

10.1 Autorizaciones:

Con periodicidad mensual, la administradora de la carpeta hará una revisión y verificará si el personal autorizado para acceder a la carpeta GEE-SIC en el OneDrive, se mantienen vigente y sin novedades, para ello tomará como evidencia un pantallazo, el cual será dispuesto en una carpeta del OneDrive, el cual se denominará Autorización OneDrive.

En caso de presentarse alguna inconsistencia se procederá a:

- Tomar evidencia (pantallazo)
- Eliminación el acceso al personal no autorizado
- Informar a la mesa de servicio el evento presentado para lo que corresponda en la materia
- El resultado de esta revisión se consignará en el acta de comité de gestión correspondiente.

10.2 Copia de seguridad:

El servidor público o contratista del Grupo del Grupo de Trabajo de Informática Forense y Seguridad Digital encargado de realizar las copias de seguridad, quincenalmente realiza copia de seguridad de los documentos contenidos en la carpeta del GEE-SIC en el OneDrive, ubicándola en el repositorio asignado al GEE-SIC.

Asimismo, se remitirá reporte a través del correo institucional, indicando el estado de conservación de esta copia de seguridad. En caso de que no se aporte el reporte, el GEE-SIC solicitará a la OTI/Mesa de Servicios, el cumplimiento de la actividad. Se evidencia a través del reporte emitido quincenalmente por la OTI/Mesa de Servicio. Se encuentra relacionado en la documentación de la Mesa de Servicios Tecnológicos.

10.3 Software antivirus licenciado:

El servidor público o contratista del Grupo de Servicios Tecnológicos encargado de realizar las actualizaciones del software antivirus, actualiza y ejecuta periódicamente o cuando se requiera el software antivirus asignado por la entidad a los equipos de usuario final de los funcionarios, de acuerdo con las notificaciones emitidas por el fabricante. En caso de identificarse que el antivirus no ha sido asignado o actualizado, se procede a realizar la actualización del software antivirus del equipo correspondiente. Como evidencia se cuenta con los reportes generados relacionados en la documentación de la Mesa de Servicios Tecnológicos.

10.4 Controles de seguridad:

Establecidos por Office 365 para la herramienta OneDrive: El (la) Coordinador(a) del GEE-SIC anualmente solicitará a la mesa de servicio se informe cuáles son los controles de seguridad establecidos para mantener la integridad de la información en la herramienta OneDrive de Office 365.

Por su parte, la mesa de servicios realiza consulta ante el proveedor del servicio Office 365 y una vez reciba respuesta la escala ante el grupo de Informática Forense y Seguridad Digital, para que elabore el concepto técnico y finalmente lo remita al GEE-SIC, dando cuenta de las soluciones de seguridad que se implementan por parte del proveedor Office 365 para proteger la integridad de la información que se almacena en la herramienta OneDrive.

En caso de que no se aporte el concepto técnico, el GEE-SIC solicitará al Grupo de Informática Forense y Seguridad Digital el cumplimiento de la actividad. La evidencia de la ejecución del control es el concepto técnico. Actualmente, no se tiene identificado en cuál procedimiento lo tiene establecido el proveedor del servicio Office 365, una vez se reciba respuesta a la consulta, se definirá donde se encuentra documentado.

11. Lineamientos

11.1 Estos serán socializados a los integrantes del GEE-SIC en el Comité de Gestión y se remitirán a sus cuentas de correo institucional.

11.2 Estos serán objeto de actualización cada vez que se requiera de acuerdo con la dinámica del proceso y los lineamientos de esta Superintendencia.

11.3 Estos serán de estricto cumplimiento y aplicación por todos los integrantes del GEE-SIC, de acuerdo con las actividades que se realicen y que se encuentran descritas en los documentos del SIGI, proceso DE03-P01 Elaboración de Estudios económicos sectoriales y DE03-P03 Elaboración de análisis económicos[1].

[1] El área autoriza que la información contenida en este documento pueda ser compartida con otras áreas y/o entidades para efectos de gestionar el conocimiento y los aprendizajes.