Informe Seguimiento: Manual Técnico del Sistema de Gestión de Seguridad de la Información

Oficina Control Interno
Bogotá

2021-05-14

Instituto Nacional de Metrología de Colombia - INM
Avenida Carrera 50 No.26- 55 Int. 2 CAN Bogotá D.C.-Colombia
Conmutador: (57- 1) 2542222 - **Website**: www.inm.gov.co
E-mail: contacto@inm.gov.co - Twitter: @inmcolombia
Código Postal 111321

CONTENIDO

1. INTRODUCCIÓN

El informe que se presenta se da de una parte en cumplimiento del Plan de Auditorías de la vigencia 2021 aprobado en Comité Institucional de Coordinación de Control Interno el 1 de marzo de 2021 y de otra parte en cumplimiento a lo establecido en la Ley 87 de 1993, Decreto 1083 de 2015, Decreto 648 de 2017 que definió los roles que actualmente cumplen las Oficinas de Control Interno: i. Liderazgo estratégico; ii. Enfoque hacia la prevención; iii. Relación con entes externos de control; iv. Evaluación de la gestión del riesgo y v. Evaluación y Seguimiento.

2. ALCANCE

El alcance obedece a la vigencia 2020 y lo al 27 de abril de 2021 (fecha de elaboración del informe) y documentalmente al: MANUAL TÉCNICO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN vigente, (E-05-M-002; versión 1, de fecha: 10/Ago/2020) dispuesto para consulta a través de la plataforma de Isolución en: http://192.168.11.216/Isolucion/Administracion/frmFrameSet.aspx?Ruta=Li4vRnJhbWVTZXRBcnRpY3Vsby5hc3A/UGFnaW5hPUJhbmNvQ29ub2NpbWllbnRvTWV0cm9sb2dpYS8yLzJkNjBhMmM3NGQ4NzRlM2I5MDAwNTQwNTM0NTUyNDViLzJkNjBhMmM3NGQ4NzRlM2I5MDAwNTQwNTM0NTUyNDViLmFzcCZJREFSVElDVUxPPTE3MjA=

3. DESCRIPCIÓN METODOLÓGICA

Teniendo presente que se vienen desarrollando las actividades laborales desde casa, se procedió a realizar solicitud de información el 7 de abril de 2021 al Profesional Especializado Omar Enrique Mejía Vargas; sin tener en cuenta información que fuera procesada el día de la solicitud; así:

1. Nombre y cargo del funcionario responsable de liderar proyectos, procesos y actividades relacionadas con seguridad y privacidad e identificación de dicho cargo dentro del Manual de Funciones vigente.
2. Nombre del Profesional de la Secretaría General, denominación o ubicación de dicho cargo en el Manual de Funciones vigente; con autoridad para solicitar cumplimiento legal, de directrices y políticas de seguridad y privacidad en las áreas y responsable de liderar la implementación de Planes de Mejoramiento
3. Nombre del Coordinador del GSIR autorizado para exigir el cumplimiento de normas políticas y actividades asociadas a la seguridad, responsable de velar por la ejecución de actividades propias a sus procesos por medio de las cuales se aplican los controles técnicos establecidos en la norma NTC-ISO-IEC 27001-2013 y la ubicación de dicha función dentro del Manual de Funciones vigente.
4. Detalle (o reseña de las acciones concretas) de la gestión que adelantó el CIGD entre el 1° de septiembre de 2020 y el 31 de marzo de 2021 y cuyo resultado afectó de manera positiva el desempeño del Sistema de Gestión y Seguridad de la Información del INM.
5. Relación y/o detalle de los recursos humanos designados o asignados para la seguridad de la información entre el 1° de septiembre de 2020 y el 31 de marzo de 2021.

6. Relación y/o detalle de los recursos financieros asignados para la seguridad de la información por lo correspondiente a la vigencia 2020 o en su defecto para el periodo entre el 1° de septiembre y el 31 de diciembre de 2020.
7. Relación y/o detalle de los recursos financieros asignados para la seguridad de la información para la vigencia 2021 (del 1° enero al 31 de diciembre de 2021)
8. Esquemas de trabajo que han afectado (de forma positiva y/o adversa) el desempeño u objetivos del Sistema de Gestión de Seguridad de la Información tanto para la vigencia 2020 como para el 2021.
9. Relación y/o detalle de acciones concretas; resultantes de la motivación para el cumplimiento de los objetivos del Sistema de Gestión Seguridad entre el 1° de septiembre de 2020 y el 31 de marzo de 2021.
10. Eventos y/o ciberataques que afectaron el desempeño y los objetivos del Sistema de Gestión de Seguridad de la Información en la vigencia 2020.
11. Eventos y/o ciberataques que afectaron el desempeño y los objetivos del Sistema de Gestión de Seguridad de la Información en lo que va corrido de la vigencia 2021 (del 1° de enero al 31 de marzo de 2021).
12. Documentalmente hablando, concretamente por lo correspondiente al numeral 6.4 del Manual Técnico del Sistema de Gestión de Seguridad de la Información; cuál es el contexto del sistema dentro del numeral en comento (6.4)
13. Detalle (pormenorizado) de las actividades a través de las cuales hubo apalancamiento en la gestión del riesgo de seguridad digital para evitar o en su defecto minimizar la materialización de incidentes como el acaecido en la última semana de enero de 2021, específicamente en la página web institucional.
14. Evidencia y/o registro de las bases establecidas en el 2021 al interior de la entidad, para adopción de cultura de apropiación y aplicación de los conceptos y controles de seguridad.
15. Estado y/o avance del esquema integral de seguridad y privacidad, conforme al desarrollo cronológico (indicando fechas y la fuente de información).
16. Relación (pormenorizado) de los parámetros a través de los cuales se administran los activos de información del INM
17. Prácticas de seguridad implementadas entre el 1° de septiembre de 2020 y el 31 de marzo de 2021, en aras de fortalecer la innovación tecnológica del INM.
18. Relación de los procedimientos, instructivos o guías vigentes en el Sistema Integrado de Gestión (y código); requeridos o necesarios para la adopción de técnicas de seguridad en materia de ciframiento y firma digital.
19. Relación de eventos tratados como incidentes de alta criticidad entre el 1° de septiembre y el 31 de marzo de 2021.
20. Ruta del sitio y/o ubicación donde se pueda consultar el Plan de Recuperación de Desastres vigente.
21. Copia de los registros efectuados entre el 1° de septiembre de 2020 y el 31 de marzo de 2021; a través de los cuales se evidencie la aplicación del procedimiento de Gestión de Activos de Información en donde por ende hubo aplicación de los controles establecidos.

Respecto a la entrega de la información requerida para el 9 de abril de 2021, medió desde el proceso; solicitud de ampliación de plazo para el viernes 16 de abril de 2021, condición esta que se dio ofreciendo

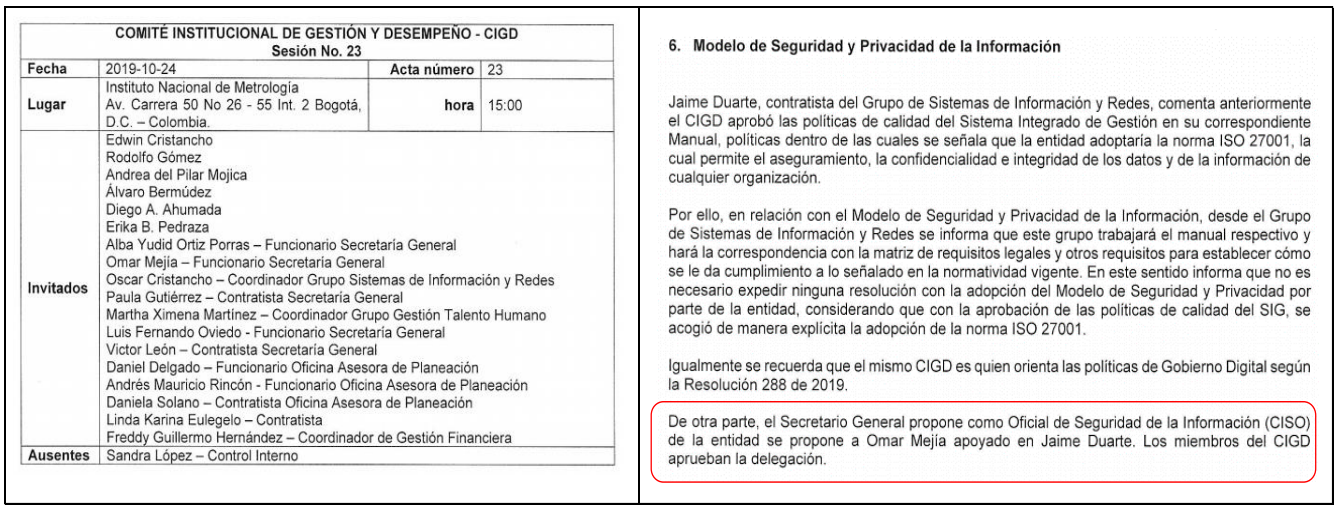
disculpas por las horas de retraso en la entrega y obedeciera particularmente por el hecho presentado con el servicio de correo electrónico.

4. RESULTADOS

Como resultado de la evaluación que se realizara, es preciso señalar:

1. Rol Oficial de Seguridad de la Información

Según da cuenta el numeral 6 del Acta del Comité Institucional de Gestión y Desempeño, suscrita con ocasión a la sesión número 23, de fecha: 24 de abril de 2019, fue "delegado" con el rol de Oficial de seguridad de la información (CISO) el Profesional Especializado (2028-14) Omar Enrique Mejía Vargas; apoyado por Jaime Duarte, tal cual como se aprecia en la ilustración que sigue de este párrafo, obtenida desde la fuente:



COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO - CIGD Sesión No. 23			
Fecha	2019-10-24	**Acta número**	23
Lugar	Instituto Nacional de Metrología Av. Carrera 50 No 26 - 55 Int. 2 Bogotá, D.C. – Colombia.	**hora**	15:00
Invitados	Edwin Cristancho Rodolfo Gómez Andrea del Pilar Mojica Álvaro Bermúdez Diego A. Ahumada Erika B. Pedraza Alba Yudid Ortiz Porras – Funcionario Secretaría General Omar Mejía – Funcionario Secretaría General Oscar Cristancho – Coordinador Grupo Sistemas de Información y Redes Paula Gutiérrez – Contratista Secretaría General Martha Ximena Martínez – Coordinador Grupo Gestión Talento Humano Luis Fernando Oviedo - Funcionario Secretaría General Victor León – Contratista Secretaría General Daniel Delgado – Funcionario Oficina Asesora de Planeación Andrés Mauricio Rincón - Funcionario Oficina Asesora de Planeación Daniela Solano – Contratista Oficina Asesora de Planeación Linda Karina Eulegelo – Contratista Freddy Guillermo Hernández – Coordinador de Gestión Financiera		
Ausentes	Sandra López – Control Interno		

6. Modelo de Seguridad y Privacidad de la Información

Jaime Duarte, contratista del Grupo de Sistemas de Información y Redes, comenta anteriormente el CIGD aprobó las políticas de calidad del Sistema Integrado de Gestión en su correspondiente Manual, políticas dentro de las cuales se señala que la entidad adoptaría la norma ISO 27001, la cual permite el aseguramiento, la confidencialidad e integridad de los datos y de la información de cualquier organización.

Por ello, en relación con el Modelo de Seguridad y Privacidad de la Información, desde el Grupo de Sistemas de Información y Redes se informa que este grupo trabajará el manual respectivo y hará la correspondencia con la matriz de requisitos legales y otros requisitos para establecer cómo se le da cumplimiento a lo señalado en la normatividad vigente. En este sentido informa que no es necesario expedir ninguna resolución con la adopción del Modelo de Seguridad y Privacidad por parte de la entidad, considerando que con la aprobación de las políticas de calidad del SIG, se acogió de manera explícita la adopción de la norma ISO 27001.

Igualmente se recuerda que el mismo CIGD es quien orienta las políticas de Gobierno Digital según la Resolución 288 de 2019.

De otra parte, el Secretario General propone como Oficial de Seguridad de la Información (CISO) de la entidad se propone a Omar Mejía apoyado en Jaime Duarte. Los miembros del CIGD aprueban la delegación.

Al efectuar la consulta de las funciones del Profesional Especializado que viene ejerciendo desde abril de 2019 con el Rol de Oficial de Seguridad, a través del Manual de Funciones vigente (Resolución 040 de 2021); se pudo determinar no fueron formalizadas y/o tenidas en cuenta a través de dicho acto administrativo, pese a que en la tabla 2 del Manual Técnico del Sistema de Gestión de Seguridad de la Información registra el Profesional de la Secretaria General tiene autoridad para solicitar el cumplimiento legal de directrices y políticas de Seguridad y Privacidad en las áreas:

Manual de Funciones INM	Manual Técnico Sistema de Gestión de SI

Código	2028
Grado	14
No. de cargos	Diecinueve (19)
Naturaleza del empleo	Carrera Administrativa
Dependencia	Donde se ubique el cargo
Cargo del jefe inmediato	Quien ejerza la supervisión directa

II. Area Funcional – Oficina de Informática y Desarrollo Tecnológico

III. Propósito Principal

Ejecutar las políticas, planes, programas, proyectos y actividades relacionadas con la gestión de tecnologías de la información e infraestructura tecnológica, de conformidad con la normatividad vigente, objetivo de la entidad y procesos establecidos.

IV. Descripción de las Funciones Esenciales

1. Participar en la formulación y ejecución de los proyectos de inversión de tecnología de la información del Instituto.
2. Administrar la infraestructura tecnológica y las redes de transmisión de datos del INM, de conformidad con los criterios establecidos.
3. Mantener en condiciones óptimas de operación, la infraestructura de red, comunicaciones y seguridad informática para garantizar la continuidad y disponibilidad de los servicios configurados y sus mantenimientos.
4. Establecer los requerimientos y necesidades de infraestructura tecnológica en cumplimiento de la misionalidad de la entidad
5. Hacer seguimiento a la atención de las solicitudes presentadas por los usuarios internos y externos oportunamente.
6. Coordinar los mantenimientos integrales de los equipos del INM, para que se cumplan las actividades para el correcto funcionamiento de la infraestructura tecnológica.
7. Generar las copias de respaldo garantizando la protección, seguridad y disponibilidad de la información institucional, evitando la pérdida y reduciendo el riesgo de ocurrencia de incidentes.
8. Hacer seguimiento e implementar los componentes de Seguridad de la información, de acuerdo a los lineamientos técnicos establecidos.
9. Aplicar los estándares y lineamientos dictados por las autoridades en la materia en lo referente a infraestructura tecnológica.
10. Realizar las actividades requeridas para la implementación, mantenimiento y mejora del Sistema Integrado de Gestión, así como la atención de auditorías y su correspondiente generación de Planes de Mejoramiento.
11. Desempeñar las demás funciones que le sean asignadas por la autoridad competente, de acuerdo con el área de desempeño, el nivel jerárquico y la naturaleza del empleo.

CARGO / ROL	AUTORIDAD	RESPONSABILIDAD
COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO	— Máxima autoridad del SGSI	— Las establecidas en el Anexo 2 del manual del SIG.
COORDINADORES DE GRUPOS Y LÍDERES DE PROCESO	— Exigir el cumplimiento de normas, políticas y actividades asociadas a la seguridad.	— Velar por la ejecución de las actividades propias a sus procesos por medio de las cuales se aplican los controles establecidos en la norma NTC-ISO-IEC 27001:21 y en particular los siguientes: — Revisión del cumplimiento en su área. Este control establece que: "Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad" (Control A.18.2.2). — Revisión de los derechos de acceso de usuario: Este control establece que: "Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares" Control (A.9.2.5)
PROFESIONAL DE LA SECRETARIA GENERAL	— Solicitar el cumplimiento legal, de directrices y políticas de Seguridad y Privacidad en las áreas.	— Liderar la implementación de Planes de Mejoramiento. — Liderar el proceso de análisis y gestión de riesgos de

[1] Resumen basado en el Anexo 2 del Manual Integrado de Gestión

Paralelamente, la Ley 489 de 1998 indica en los artículos 9 y 10 que podrán delegar la atención y decisión de los asuntos en los empleados públicos de los niveles directivo y asesores vinculados al organismo correspondiente y en el acto de la delegación, que siempre será escrito, se determinará la autoridad delegataria y las funciones o asuntos específicos cuya atención y decisión se transfieren.

De otro lado, el mismo Profesional Especializado, con autoridad para exigir el cumplimiento de normas, políticas y actividades asociadas a la seguridad, según da cuenta el Manual Técnico del Sistema de Gestión de Seguridad de la Información y por expreso señalamiento desde la Oficina, es el Profesional Especializado (2028-14) el Coordinador del GSIR (CIO) y conforme al Manual de Funciones vigente no figura con autoridad de exigir el cumplimiento de normas, políticas y actividades asociadas a la seguridad así como tampoco con responsabilidad de velar por la ejecución de las actividades propias a sus procesos por medio de las cuales se aplican los controles técnicos establecidos en la norma NTC-ISO-IEC 27001: 2013, también conocidos como Seguridad Lógica o Seguridad Informática.

CARGO / ROL	AUTORIDAD	RESPONSABILIDAD
		seguridad digital.
Coordinador del GSIR (CIO)	— Exigir el cumplimiento de normas, políticas y actividades asociadas a la seguridad.	— Velar por la ejecución de las actividades propias a sus procesos por medio de las cuales se aplican los controles técnicos establecidos en la norma NTC-ISO-IEC 27001:2013, también conocidos como Seguridad Lógica o Seguridad Informática. (En particular los siguientes objetivos de control: Seguridad de las Operaciones- A.12, Seguridad de las Comunicaciones A.13, Adquisición, desarrollo y mantenimiento de sistemas - A.14)

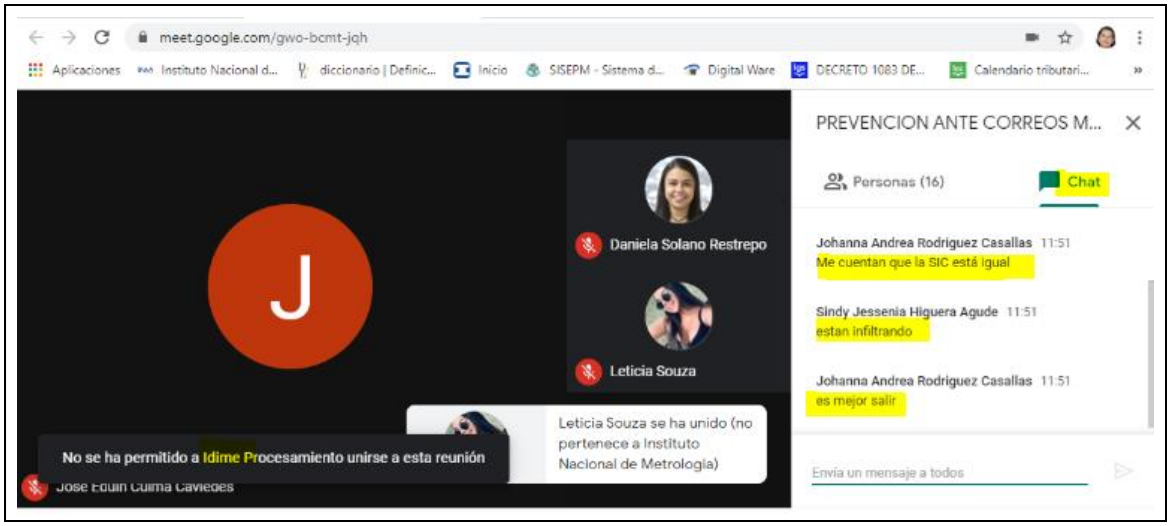
2. Desempeño del Sistema de Seguridad de la Información

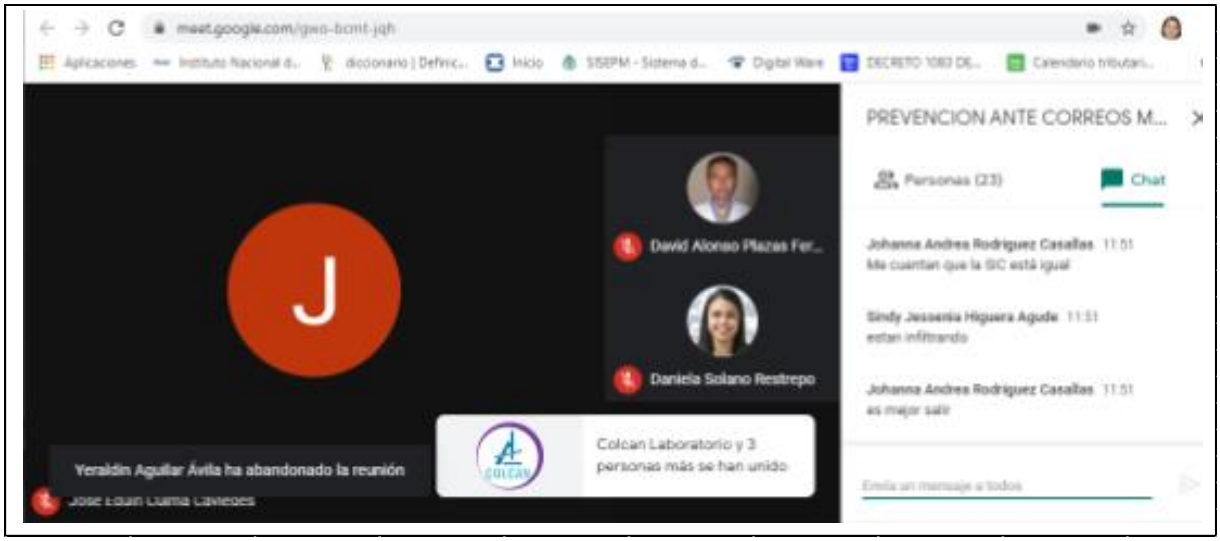
A partir de la consulta acerca del esquema de trabajo que han afectado (de forma positiva y/o adversa) el desempeño u objetivos del Sistema de Gestión de Seguridad de la Información tanto para la vigencia 2020 como para el 2021, hubo indicación expresa sobre el particular: *Los efectos del trabajo en casa, producto de la pandemia por COVID-19, que está incluido en el manual como factor externo,*

"Emergencia Sanitaria", ha afectado el desempeño del Sistema de Gestión de Seguridad de la Información, por cuanto las estadísticas arrojan un incremento en las amenazas. Los efectos de esta situación han sido mitigados por medio de campañas (ej. Campaña prevención uso del correo y antivirus) y lineamientos formalizados por ejemplo mediante las circulares 013 y 014 de 2020, donde a través de validaciones se pudo determinar:

- **Correos mal intencionados (2021-04-16)**

El viernes 16 de abril de 2021, en medio de la reunión que fuera programada para advertir acerca de correos malintencionados; los asistentes a la misma evidenciaron intromisión de usuarios o personas ajenas al dominio del Instituto Nacional de Metrología como por ejemplo: Leticia Souza, Guilherme Mathias dos Santos Idime Procesamiento, Colcan Laboratorio y 3 personas más.





La tipología de los correos mal intencionados que fueran remitidos haciendo mención de la apertura de un proceso judicial, fue entre otros haciendo uso de remitentes como:

- Contacto INM

TRÁMITE DE CONCATENACIÓN POR ATRIBUCIÓN FISCAL Recibidos ×

Contacto INM 9:26 (hace 8 minutos)
para bcc: mí

16 de Abril del 2021
E.S.D.

Asunto: Apertura del Proceso 0016042021

Debido a lo que establece la ley y con el fin de garantizar el debido proceso para todos los ciudadanos, nos permitimos notificarle de forma clara y concreta su vinculación al proceso de responsabilidad fiscal con radicado 0016042021 por el cual usted figura como parte demanda como consecuencia del fraude realizado a los bienes pertenecientes al estado.

Adjunto acuerdo para que se presente al proceso de forma rápida y oportuna.

Adjunto protegido con contraseña: 0016042021

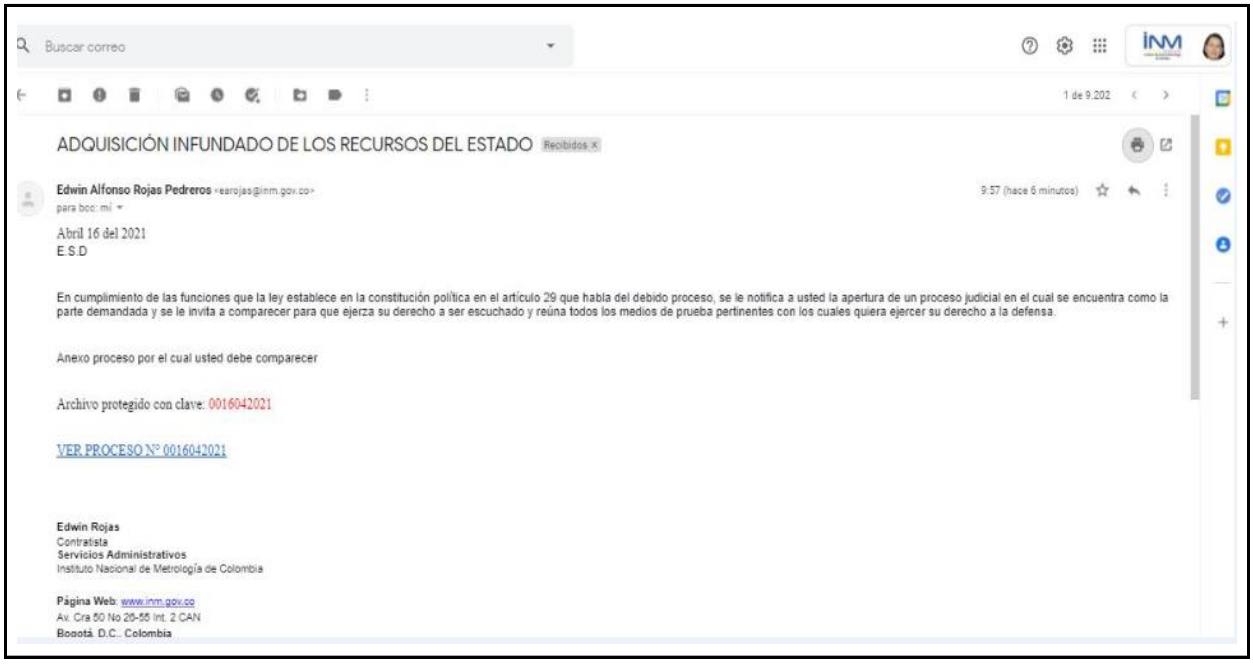
VISUALIZAR ACUERDO DE PROCESO

Cordialmente,

Instituto Nacional de Metrología de Colombia

Página Web: www.inm.gov.co
Av. Cra 50 No 26-55 Int. 2 CAN

- Edwin Alfonso Rojas Pedreros



Buscar correo

1 de 9.202

ADQUISICIÓN INFUNDADO DE LOS RECURSOS DEL ESTADO Recibidos ×

Edwin Alfonso Rojas Pedreros <earojas@inm.gov.co> 9:57 (hace 6 minutos)
para bcc: mí

Abril 16 del 2021
E.S.D

En cumplimiento de las funciones que la ley establece en la constitución política en el artículo 29 que habla del debido proceso, se le notifica a usted la apertura de un proceso judicial en el cual se encuentra como la parte demandada y se le invita a comparecer para que ejerza su derecho a ser escuchado y reúna todos los medios de prueba pertinentes con los cuales quiera ejercer su derecho a la defensa.

Anexo proceso por el cual usted debe comparecer

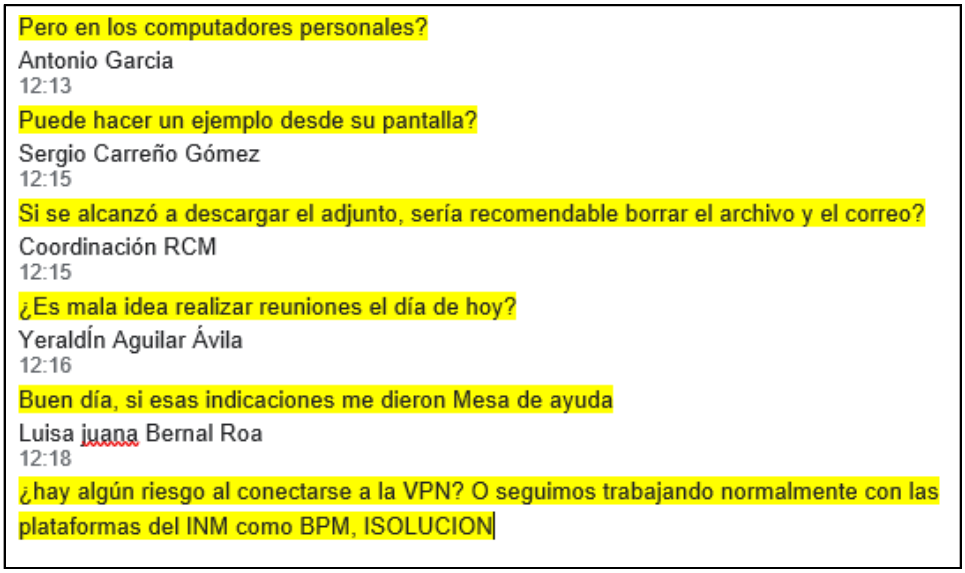
Archivo protegido con clave: 0016042021

VER PROCESO N° 0016042021

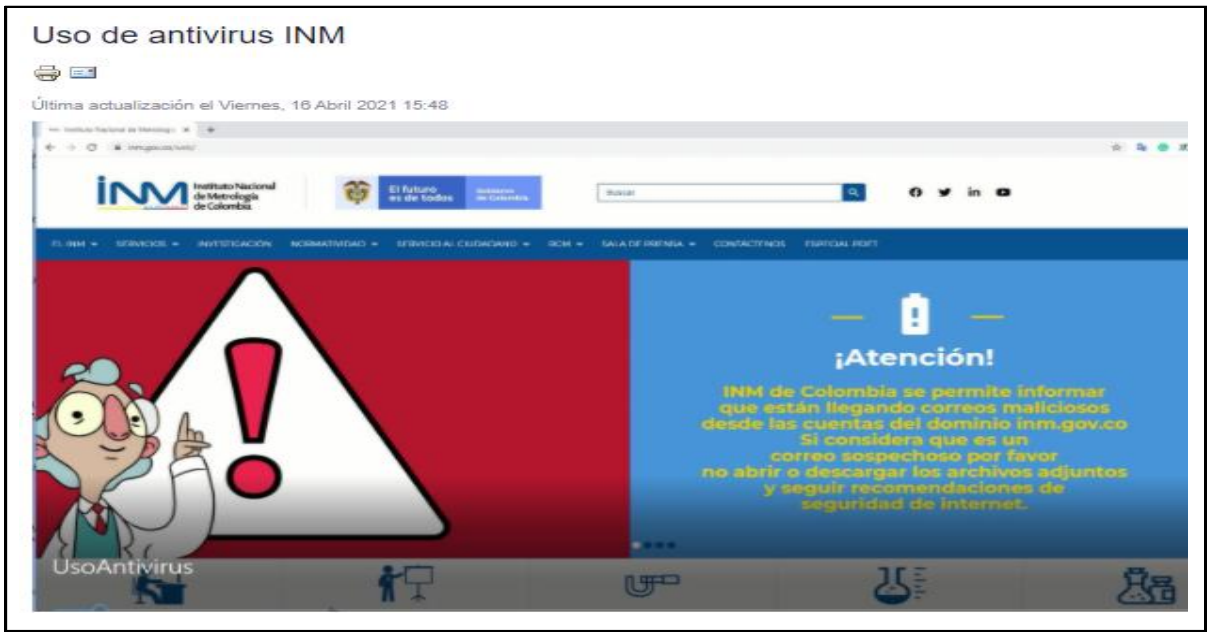
Edwin Rojas
Contratista
Servicios Administrativos
Instituto Nacional de Metrología de Colombia

Página Web: www.inm.gov.co
Av. Cra 50 No 26-55 Int. 2 CAN
Bogotá, D.C., Colombia

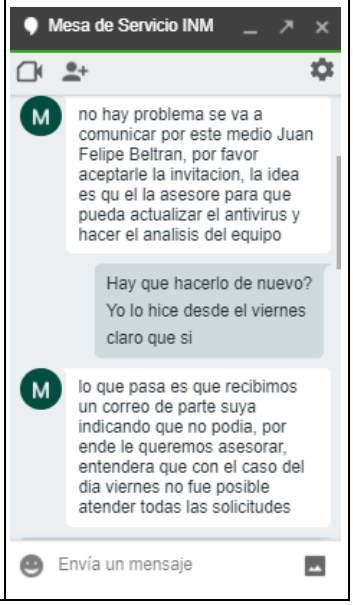
Mientras se llevaba a cabo reunión en que el INM advertía al personal del evento que se estaba presentando a través de correos electrónicos de asunto: adquisición infundado de los recursos del estado, fue evidente a través del chat no hay cultura en la realización de procesos de protección de equipos, casualmente cuando se vienen realizando labores desde casa hace algo más de un año.



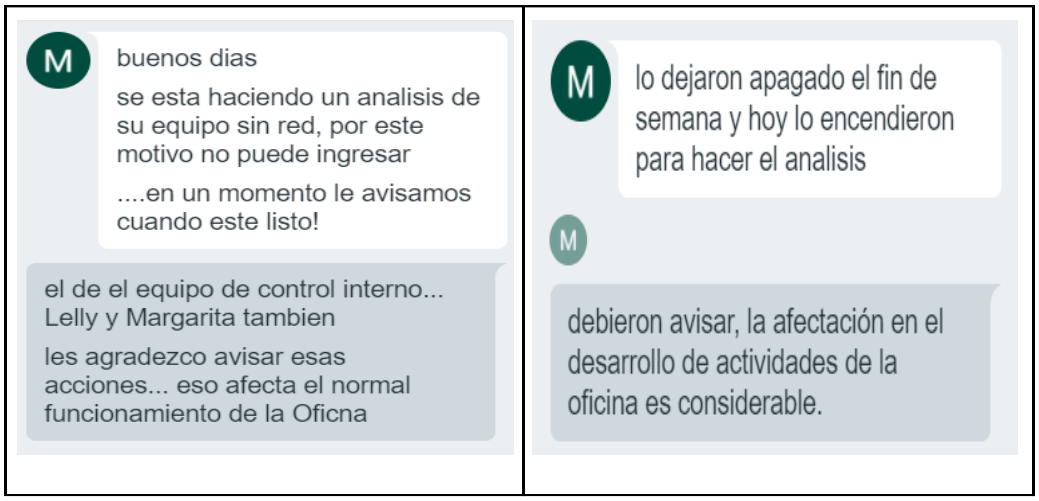
A través de la INMtranet hubo actualización de publicación el mismo 16 de abril de 2020, en la página principal:



De otro lado, en cuanto a las recomendaciones desde el correo institucional de Talento Humano, en casos como el que se trae a modo de ejemplo la mesa de servicio se quedó corta, emitiendo respuesta al cierre de casos sin que hubieran sido atendidos tal cual como ocurriera con el reportado por la funcionaria María Margarita Peña Vargas, desde el viernes 19 de abril de 2021, tras haber recibido correo mal intencionado con remitente Edwin Alfonso Rojas Pedreros, con respuesta formal de ese día (2021-04-16) y fuera contactada a través del chat el lunes 19 de abril de 2021, para efectuar lo que ya había realizado teniendo en cuenta instrucciones impartidas por el funcionario Jose Edwin Culma durante la reunión:

2021-04-16	2021-04-19
	

Aunado a lo anterior, fue posible evidenciar también al inicio de la jornada laboral el lunes 19 de abril de 2021, fallas de comunicación en ausencia de confirmación de acciones a partir de la afectación en algunos equipos por trabajos realizados durante el fin de semana que bien pudieran haber sido la respuesta al mantenimiento y/o continuidad del servicio de plataformas tecnológicas o simplemente rutinas de validación:



- **Ataque a la página web (26 de enero de 2021)**

A través de redes sociales como Twitter, se tuvo conocimiento del acontecimiento del hackeo de páginas de Colombia y Argentina, entre esas la del INM de Colombia (2021-01-26):

A través de internet se consultó la noticia, donde señalaban:


com/hackean-paginas-oficiales-colombia-argentina-promover-scam-criptomonedas/

Negocios **Noticia**

Hackean paginas oficiales de Colombia y Argentina para promover scam de criptomonedas

By Daniel Ramirez-Escudero 26 Enero 2021, 09:24 GMT+0000

compartir artículo

EN RESUMEN

Hackean página del INM de Colombia para publicitar un bot de criptomonedas.

Actualmente la página se encuentra redireccionando a sus usuarios a este scam.

Más de 4000 personas han sido redireccionadas a la pagina scam.

MOST READ

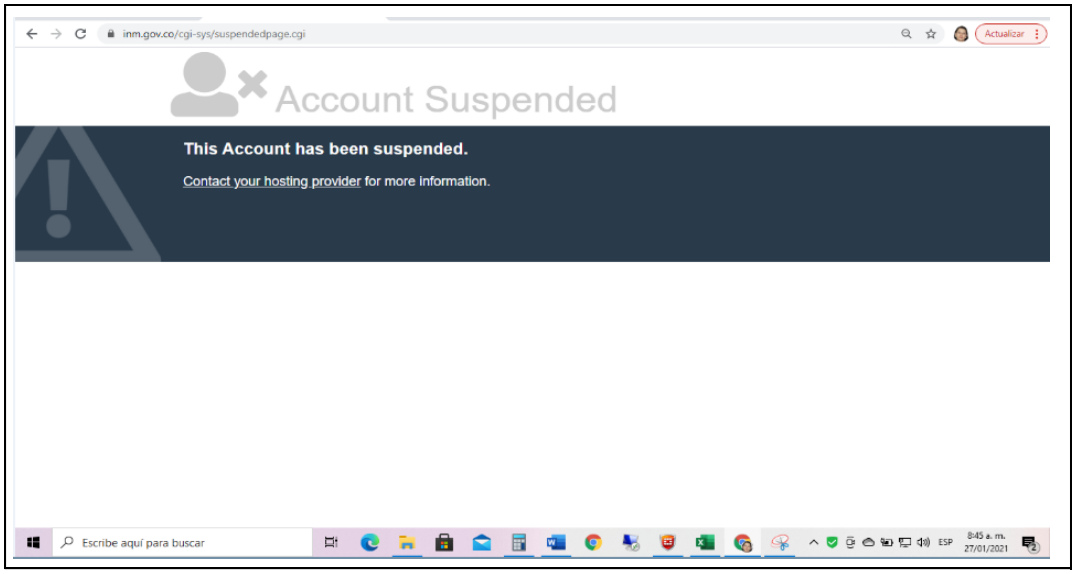
"*Hackean página del INM de Colombia para publicitar un bot de criptomonedas. Actualmente la página se encuentra redireccionando a sus usuarios a este scam. Más de 4000 personas han sido redireccionadas a la página scam.*
La página oficial del Instituto Nacional de Metrología de Colombia (INM) se encuentra en estos momentos comprometida, ya que desde su dominio se pueden encontrar redirecciones directas a una página de estafas con criptomonedas que busca atraer usuarios a bots para ganar dinero por referidos.

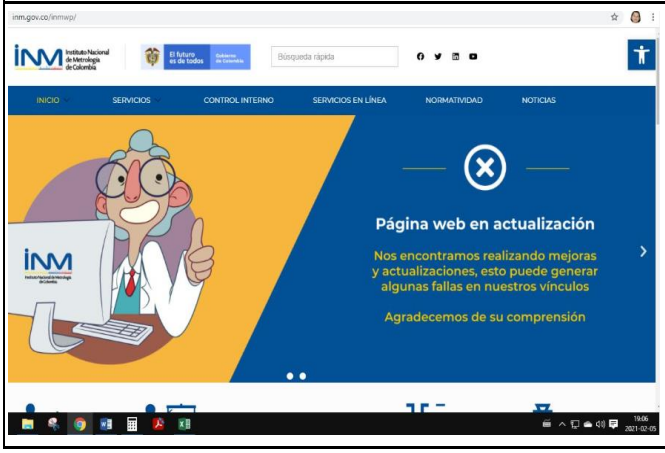
Aún no se tiene constancia de los autores del scam, pero se especula que podrían ser trabajadores del Estado, algún subcontratista que tiene acceso al dominio o servidor del INM o quizás pueda ser algún empleado del INM debido al modus operandi. Asimismo, la tesis de un hack exterior tampoco ha quedado descartada. La acción buscaba valerse de la confianza de una página del Gobierno para redireccionar a los usuarios al sitio de estafa financeindex.co.

Sin embargo, el incremento de tráfico que ha tenido en Google ha dejado en evidencia que se trata de una estafa bien organizada que busca captar a personas ingenuas que deseen sumarse al rally del Bitcoin en un momento donde las criptomonedas cada día están más de moda.


Aún no se tiene constancia de los autores del scam, pero se especula que podrían ser trabajadores del Estado, algún subcontratista que tiene acceso al dominio o servidor del INM o quizás pueda ser algún empleado del INM debido al modus operandi. Asimismo, la tesis de un hack exterior tampoco ha quedado descartada. La acción buscaba valerse de la confianza de una página del Gobierno para redireccionar a los usuarios al sitio de estafa financeindex.co.

Tras haber sido aprovechada la vulnerabilidad(es) que se presentaran al momento en que hubiera sido modificado el contenido del sitio web institucional para redireccionar el tráfico hacia un sitio de promoción, desde entonces (finales de enero de 2021) tras haber estado suspendida la cuenta y hasta la fecha de verificación en este informe (21 de abril de 2021) se han presentado avisos a través de la página web de la entidad indicando que la página web se encuentra en actualización o no han sido realizados los arreglos necesarios para poner de nuevo en condiciones óptimas la operación de la página; haciendo caso omiso a la recomendación que se viene efectuando para dar cumplimiento legal a través de diversos recordatorios en medio de correos institucionales y la INMtranet.



Fecha del anuncio: 2021-02-05	Fecha del anuncio: 2021-04-21
	

A partir de la tabla No 1 del Informe-Plan de recuperación y Gestión de Incidente (Página Web), expedido por la Secretaría General con fecha 2021-02-09; el Plan de Restablecimiento página Web,

estaba hasta el 15 de febrero de 2021 y no precisamente hasta finales de abril tal cual como se aprecia en las imágenes precedentes y la que sigue:

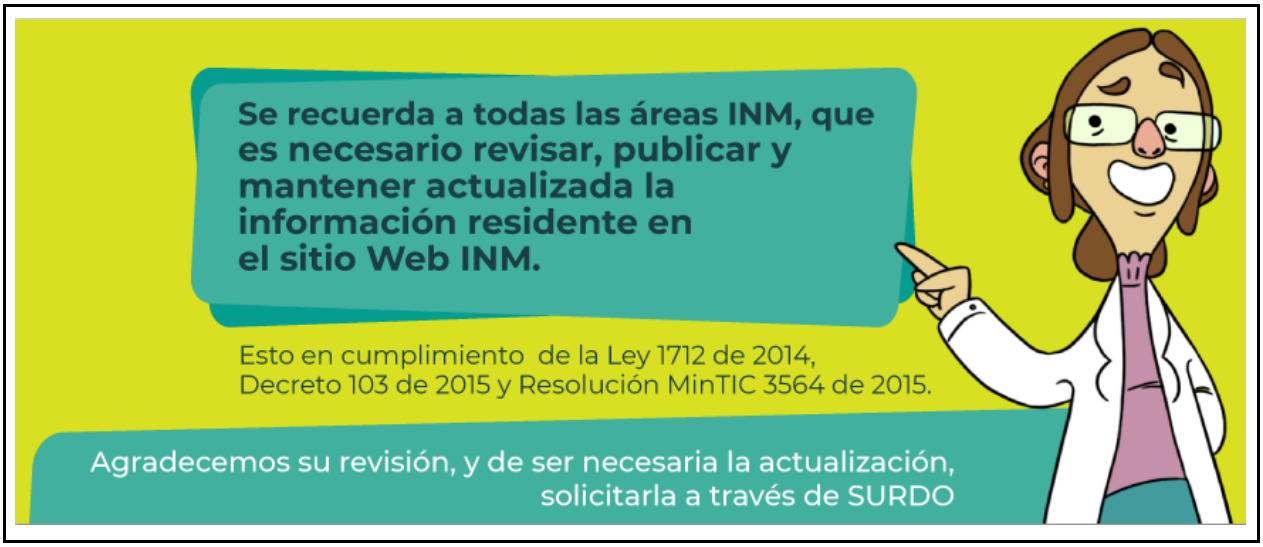
Tabla No. 1.
Plan de Actividades Finales – Restablecimiento Pagina WEB

Acciones	Resultado esperado	Responsable	Línea de tiempo			
			Feb 9 a 12	Feb 13	Feb 15	Feb 16 a 19
Restablecer contenidos	Contenidos restablecidos	Camilo R./Laureano U.				
Habilitar Página en Internet	Página habilitada	Camilo R./Laureano U				
Comunicar a usuarios	Divulgación	Luis F. Oviedo				
Validación de contenidos por parte de áreas	Contenidos validados	Usuarios				
Seguimiento	Seguimiento	Omar M.				
Realización Ethical hacking y plan de acción.	Acciones desarrolladas	Omar M. / Oscar R.				

Según da cuenta el documento de respuesta una de las actividades contempladas para mitigar el compromiso de servidores es la actualización permanente de los parches (patch) o actualizaciones al sistema operativo, en el Anexo 1 se adjuntan ejemplos de la actualización de servidores del INM, actividad que se realiza en forma constante.

Por otra parte, en la matriz de riesgos de la OIDT, se encuentra establecido que ante el riesgo de exposición de nuevas amenazas informáticas y como protección ante nuevos ataques informáticos, se definieron como medidas de mitigación: el control de acceso a la información (en 2020 se realizaron mejoras al formato de solicitud de acceso y se realizó depuración de permisos a carpetas compartidas) y la aplicación de acuerdos de confidencialidad.

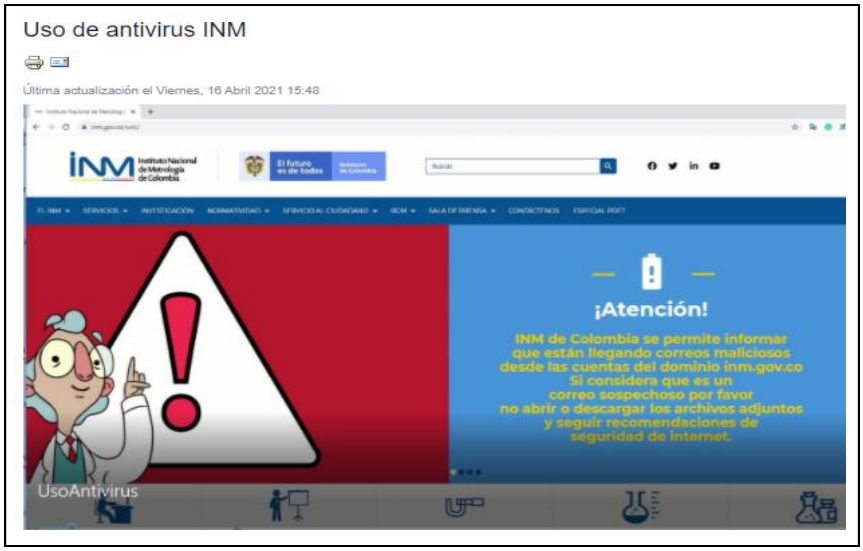
A partir de la observación que se registra con ocasión al evento del 26 de enero de 2021, la Oficina de Control Interno hace extensivo el recordatorio que se viene realizando a través de mensajes de correo electrónico y tener la información residente en el sitio web de la entidad verdaderamente actualizada, toda vez que hay indicación de la implementación de medidas de protección.



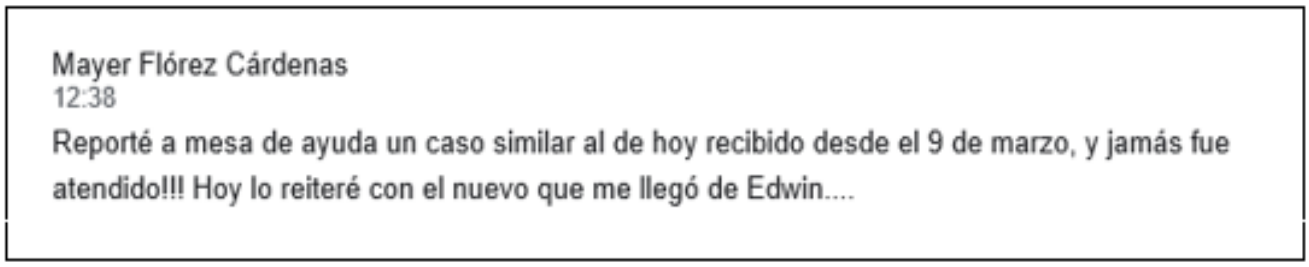
- **Campaña prevención (uso del correo y antivirus)**

A partir del evento acaecido el viernes 16 de abril de 2021, se pudo determinar presencia de vulnerabilidades y no precisamente consolidación de la campaña bajo el espectro de la interiorización y/o concientización por el personal del INM, dado que fue evidente entre otros la afectación precisamente del usuario contacto@inm.gov.co y del contratista de la Secretaria General Edwin Alfonso Rojas Pedreros.

Como medida, se evidenció orientación a través de la intranet para hacer uso del antivirus, con actualización del mismo día de haberse presentado el evento.

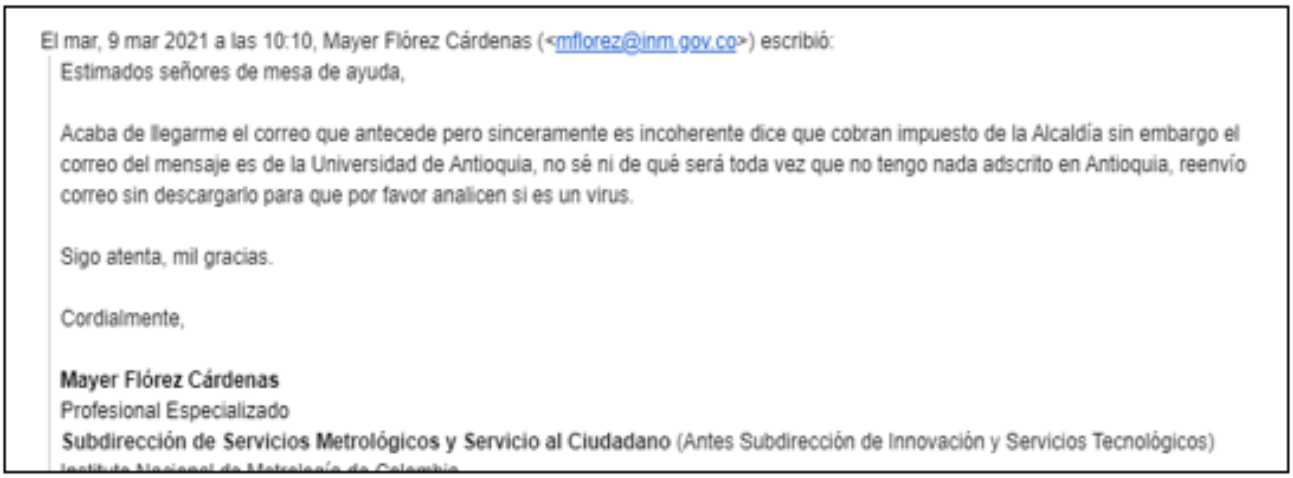


Aunado a lo anterior, en medio de la reunión del mismo 16 de abril de 2021, la funcionaria Mayer Flórez realizó comentario sobre un caso similar de un correo que a la recepción del mismo le generó sospecha, sin que hasta entonces (2021-04-16), pasado algo más de un mes, tuviera respuesta o hubiera sido informada sobre el impacto generado, el alcance dado por el INM sobre el tema en particular, cuando en efecto la tipología del correo es similar a la que se diera con el evento que se conoció.



Mayer Flórez Cárdenas
12:38

Reporté a mesa de ayuda un caso similar al de hoy recibido desde el 9 de marzo, y jamás fue atendido!!! Hoy lo reiteré con el nuevo que me llegó de Edwin....



El mar, 9 mar 2021 a las 10:10, Mayer Flórez Cárdenas (<mflorez@inm.gov.co>) escribió:

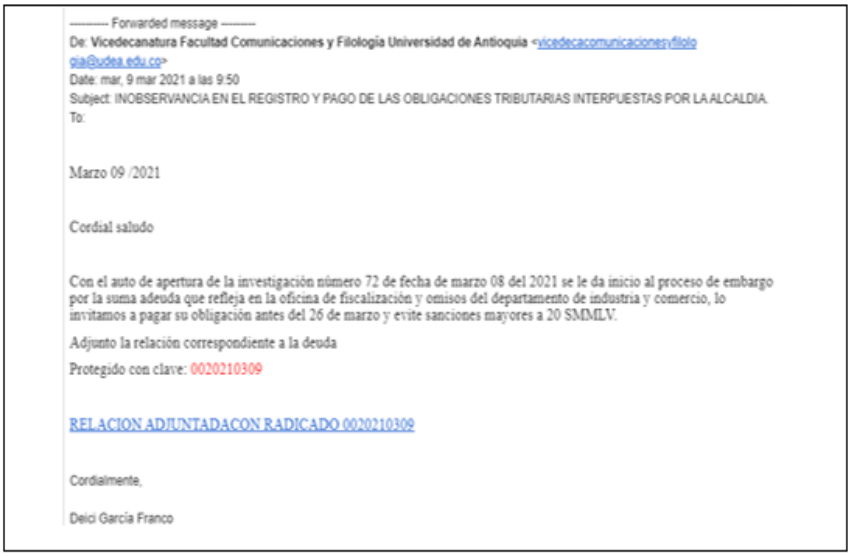
Estimados señores de mesa de ayuda,

Acaba de llegarme el correo que antecede pero sinceramente es incoherente dice que cobran impuesto de la Alcaldía sin embargo el correo del mensaje es de la Universidad de Antioquia, no sé ni de qué será toda vez que no tengo nada adscrito en Antioquia, reenvío correo sin descargarlo para que por favor analicen si es un virus.

Sigo atenta, mil gracias.

Cordialmente,

Mayer Flórez Cárdenas
Profesional Especializado
Subdirección de Servicios Metrológicos y Servicio al Ciudadano (Antes Subdirección de Innovación y Servicios Tecnológicos)
Instituto Nacional de Metrología de Colombia



---------- Forwarded message ---------
De: **Vicedecanatura Facultad Comunicaciones y Filología Universidad de Antioquia** <vicedecacomunicacionesyfilologia@udea.edu.co>
Date: mar, 9 mar 2021 a las 9:50
Subject: INOBSERVANCIA EN EL REGISTRO Y PAGO DE LAS OBLIGACIONES TRIBUTARIAS INTERPUESTAS POR LA ALCALDIA.
To:

Marzo 09 /2021

Cordial saludo

Con el auto de apertura de la investigación número 72 de fecha de marzo 08 del 2021 se le da inicio al proceso de embargo por la suma adeuda que refleja en la oficina de fiscalización y omisos del departamento de industria y comercio, lo invitamos a pagar su obligación antes del 26 de marzo y evite sanciones mayores a 20 SMMLV.

Adjunto la relación correspondiente a la deuda

Protegido con clave: 0020210309

RELACION ADJUNTADACON RADICADO 0020210309

Cordialmente,

Deici García Franco

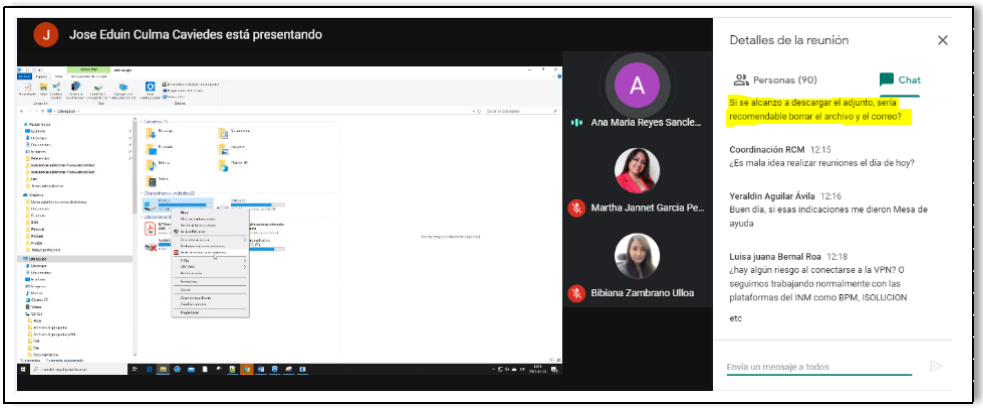
Al efectuar validación a través del reporte de eventos que fuera vinculado al documento de respuesta, vale la pena mencionar no se observa a partir del solicitante el caso en comento:

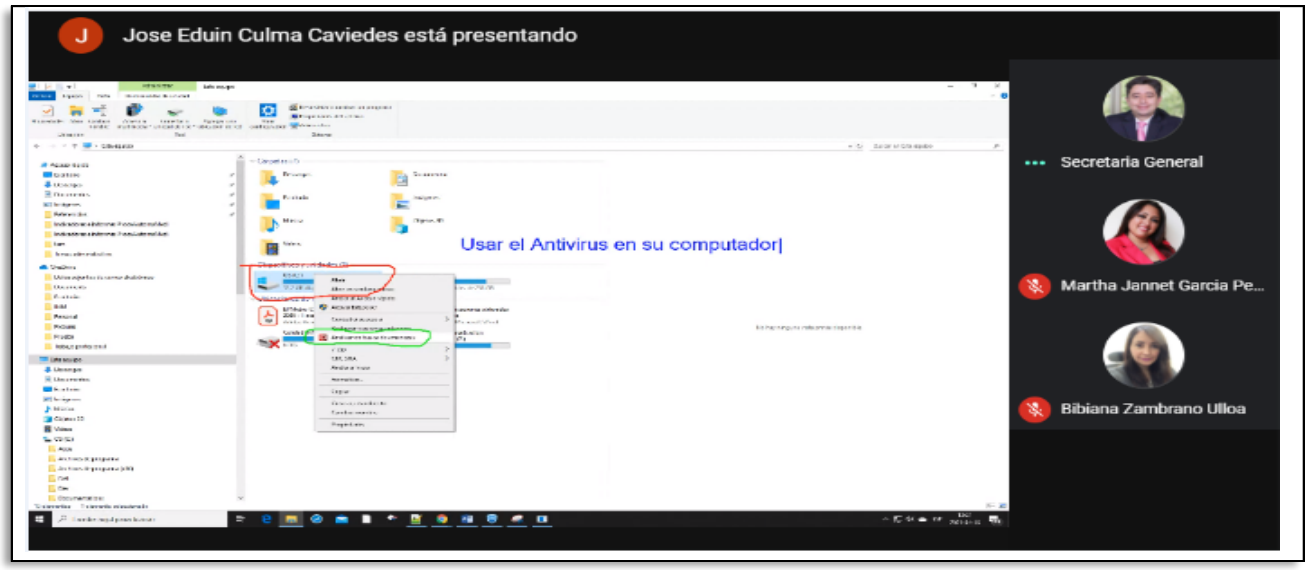
	ID de la	Modo de solicitud	Grupo	Solicitante	Departamento
Ciberseguridad					
	11214	Correo Electrónico	Gestión de TI	Gloria Isabel Motta Carvajal	SECRETARIA GENERAL
	11241	Chat	Gestión de TI	Lida Marcela Pedraza Vega	GESTION FINANCIERA
	11246	Correo Electrónico	Gestión de TI	Jose Laureano Urrego	SUBDIRECCION DE INNOVACION Y SERVICIOS TECNOLOGICOS
	11411	Correo Electrónico	Gestión de TI	Sergio Garcia Martinez	SERVICIO ADMINISTRATIVO
	11488	Chat	Gestión de TI	Lida Marcela Pedraza Vega	GESTION FINANCIERA
	11492	Correo Electrónico	Gestión de TI	Freddy Guillermo Hernández Sandoval	GESTION FINANCIERA
	11523	Chat	Gestión de TI	Monica Diaz Guzman	General
	11529	Correo Electrónico	Gestión de TI	Oscar Ramirez Cardenas	General
Rec	8				

- **Circular 013 y 014 de 2020**

La circular 013 de 2020, de asunto: Recomendaciones para la seguridad de la información durante el trabajo en casa fue expedida casi a los 80 días de haberse dado inicio de manera improvisada e intempestiva al desarrollo de funciones laborales desde casa en nuestro país una vez declarada la emergencia sanitaria con ocasión de la pandemia por Covid-19.

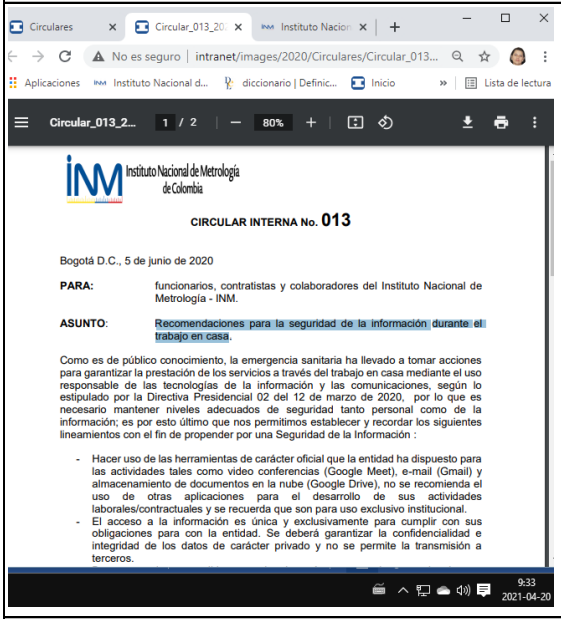
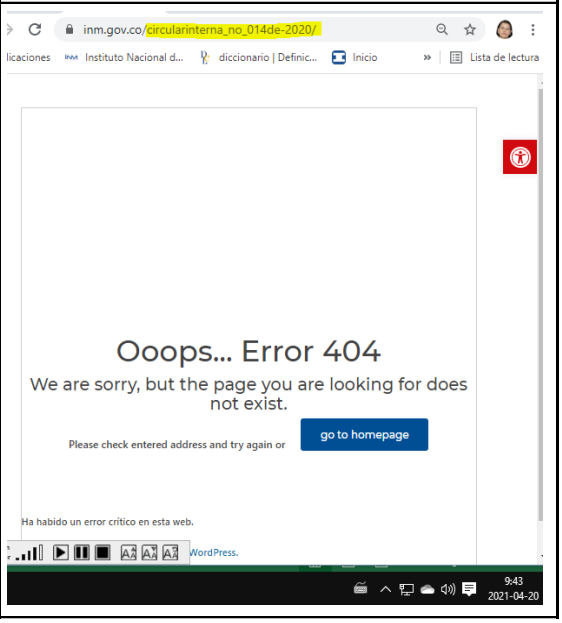
A partir de comentarios realizados por personal del INM durante reunión del 16 de abril de 2021, fue evidente no había cultura en lo que atañe al uso de antivirus tanto para los equipos del INM como para los equipos personales, la documentación remitida a través de correos electrónicos no había cumplido su cometido a todo nivel, tal cual como se puede deducir e inferir a través de la duda implícita sobre comentarios realizados: *"Si se alcanzó a descargar el adjunto, sería recomendable borrar el archivo y el correo?*



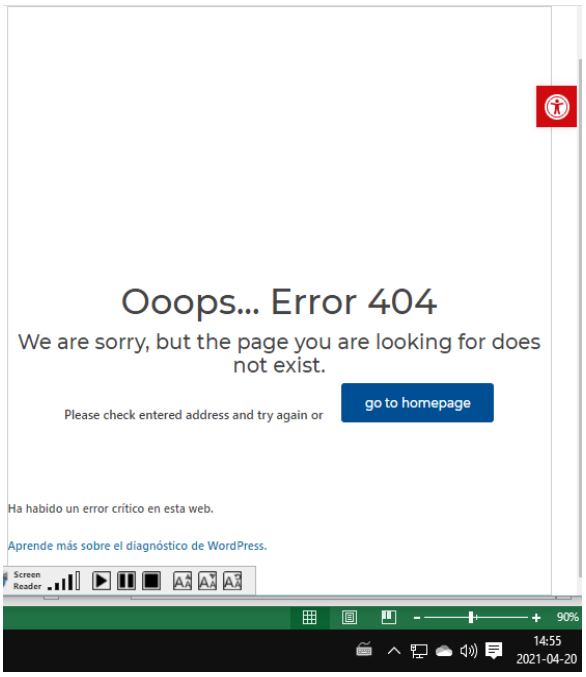


De otro lado y en aras de validar el contenido de la Circular 014 de 2020, a través de la INMtranet no fue posible dada la ausencia del enlace, mientras que en la página web ni siquiera figuran estas dos circulares y las relacionadas tienen enlaces rotos, tal cual como se aprecia a continuación en las imágenes captadas desde la fuente:

INMtranet: http://intranet/index.php/normatividad/circulares#circulares-2020

Circular 013 de 2020	Circular 014 de 2020
	

Página web: https://inm.gov.co/web/normatividad/circulares/

https://inm.gov.co/web/normatividad/circulares/	https://inm.gov.co/circular-interna-no-017/
	

3. Reporte de eventos

A partir de la información allegada pudo determinarse tanto en 2020 como en 2021, hubo reportes de parte de los funcionarios informando situaciones que consideraron atípicas en desarrollo de sus funciones o que pudieran afectar el desempeño y los objetivos del Sistema de Gestión de la seguridad de la información.

A modo de resume se pudo determinar para el 2021, fueron catalogados como eventos de seguridad, 6 casos, relacionados a continuación:

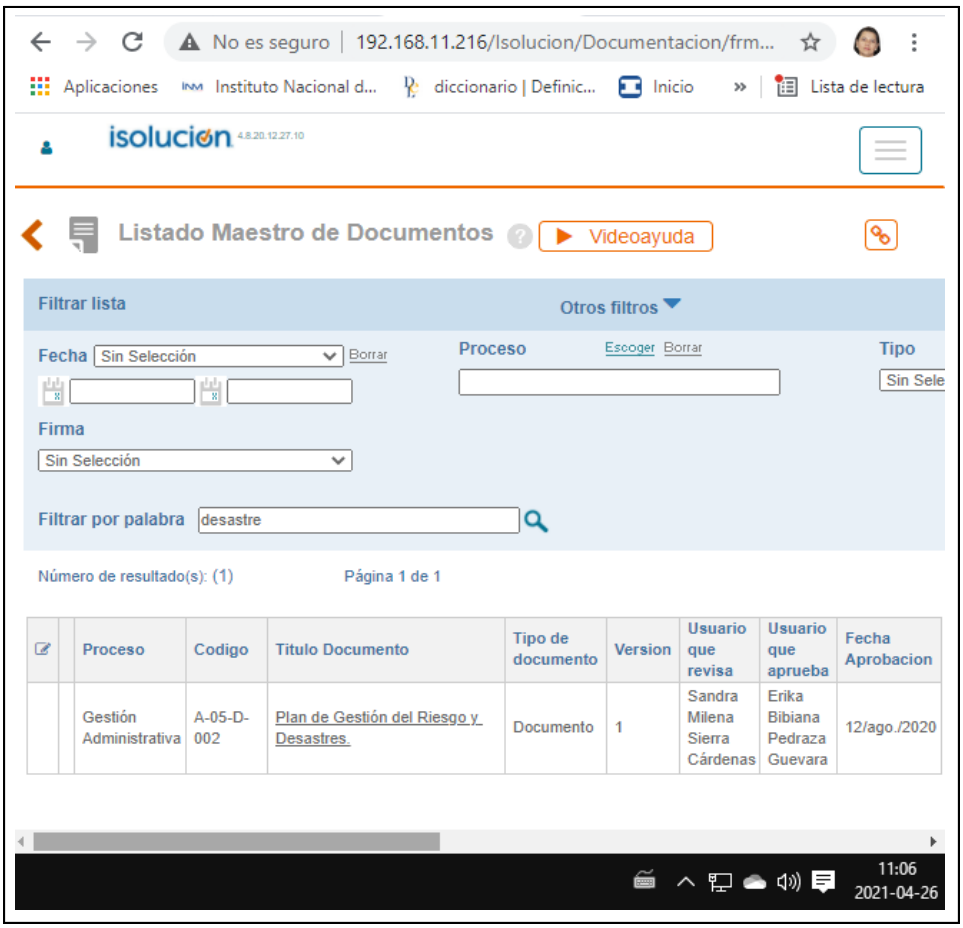
Modo de solicitud	Departamento	Subcategoría	Asunto
Correo Electrónico	Secretaria General	Bloqueo y políticas firewall	Habilitación VPN
Chat	Gestión Financiera	Instalación firma digital y/o token	Alerta al usar token
Correo Electrónico	Subdirección De Innovación Y Servicios Tecnológicos	Amenazas informáticas	Correo sospechoso
Correo Electrónico	Servicio Administrativo	Bloqueo y políticas firewall	Habilitar VPN fin de semana
Chat	Gestión Financiera	Alertas - Errores	Error en el token
Correo Electrónico	Gestión Financiera	Amenazas informáticas	Reporte de embargo

4. Plan de Recuperación de Desastres

Desde la óptica documental, a propósito del plan o esquema para la recuperación de desastres, hubo indicación expresa a través del documento de respuestas remitido, que el documento previsto, dispuesto para consulta a través de la plataforma de Isolución es objeto de actualización por reestructuración institucional y que dicho plan se complementa con el procedimiento de backups y restauración de información en equipos de cómputo y servidores.

A partir de la consulta efectuada el 26 de abril de 2021, en la plataforma de Isolución no se encontró tal cual como indicaran en el documento de respuesta: "*En el sistema Isolución se encuentra cargado el documento RECUPERACIÓN ANTE DESASTRES_v1 el cual se encuentra en estos momentos en actualización por reestructuración institucional Ver Anexo 3.*"

El único resultado que arroja la búsqueda a partir de la palabra desastre corresponde al Plan de Gestión del Riesgo y Desastres del proceso de Gestión Administrativa, tal cual como se aprecia en la imagen que sigue capturada desde la fuente: Isolución



5. Recursos

La asignación de recursos humanos y financieros para la seguridad de la información entre 2020 y 2021 fue según el informe denominado documento de respuesta requerimiento de información Manual Técnico del SGSI:

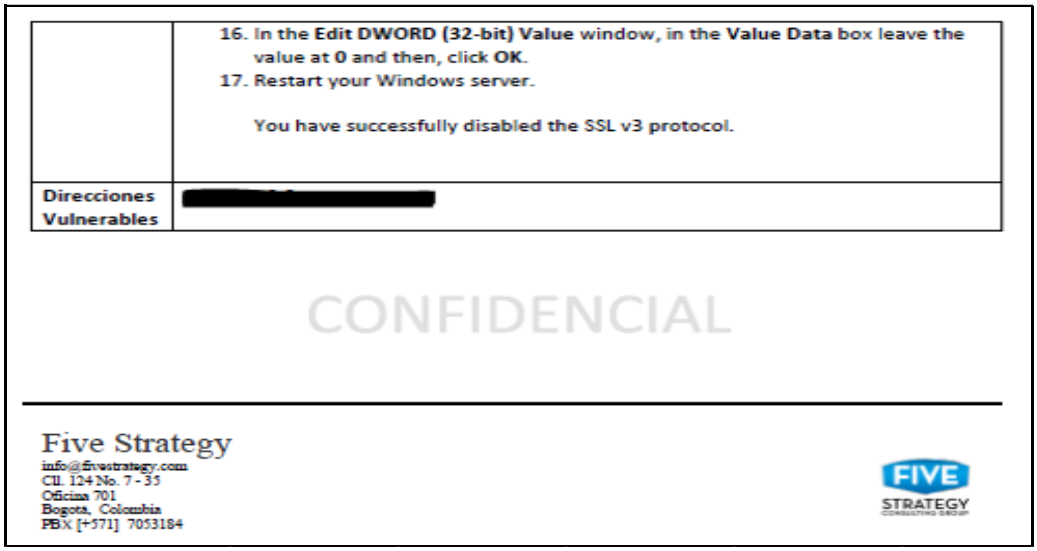
Nombre del colaborador	Actividades o rol	Característica de la dedicación
Rodolfo Gómez Rodríguez	Seguimiento y establecimiento de necesidades y directrices para seguridad de la información	Dedicación parcial. (estimado 2%)
Omar Enrique Mejía	Rol de oficial de Seguridad de la Información (Delegación realizada en CIGD – 23 del 2019-10-24 ver acta aquí)	Dedicación parcial (estimado 10%)
Nelson Francisco Rodríguez	Gestión de herramientas antivirus. Aplicación del procedimiento de back ups en servidores.	Dedicación parcial (estimado 15%)
Jhon Diaz M	Gestión de herramientas de monitoreo de servidores. Administración de Servidores (actualización)	Dedicación parcial (estimado 20%)
Viviana Mendoza Diego Diaz Luis A Diaz	Apoyo en la atención y escalamiento de incidentes. Atención de toma de back ups en PCs.	Orden de prestación de servicios. (estimado 30%)
Oscar Ramírez C	Apoyo en la implementación, monitoreo y gestión del sistema. Apoyo en la investigación y atención de incidentes.	Orden de prestación de servicios. (100%)

Concepto	Valor para la vigencia 2020 (en millones)
Honorarios por prestación de servicios.	$54,6
Costo licencias y soporte de herramientas de seguridad (Antivirus, Firewall, Fortinet).	$171,5

Concepto	Valor para la vigencia 2021 (en millones)
Honorarios por prestación de servicios.	$61.4
Costo licencias y soporte de herramientas de seguridad (Antivirus, Firewall, Fortinet).	$269,2 sujeto a los resultados del proceso de contratación.

Al efectuar consulta a través de SECOP II, se evidenció contratación de referencia: MC 029 de 2020, descrita como prestación de servicios Ethical Hacking, donde se pudo conocer además de información relacionada con generalidades, condiciones, servicios, documentos del proveedor, información presupuestal, ejecución del contrato; información relevante que resulta de interés casi que con exclusividad para el INM y de riesgo alto por su contenido y exposición para quienes buscan atentar desde el ciberespacio, donde por ejemplo **hay precisión acerca de las direcciones que son vulnerables**.

De otro lado en el mismo informe también se ve paradójicamente a través de la marca de agua, anuncio de confidencialidad, que precisamente no se dio, verbigracia:



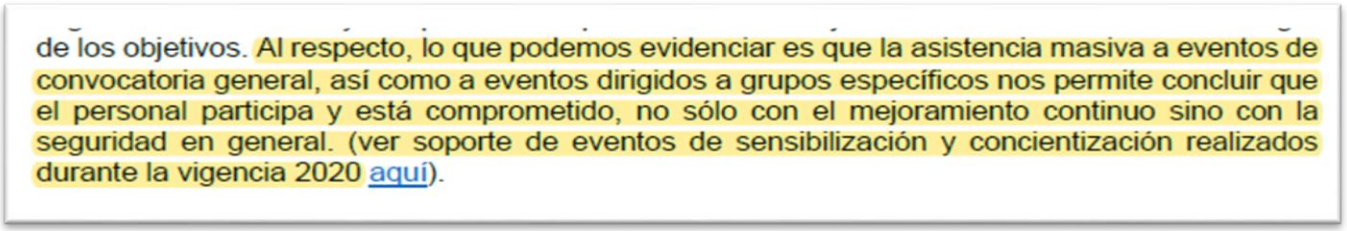
	16. In the **Edit DWORD (32-bit) Value** window, in the **Value Data** box leave the value at **0** and then, click **OK**. 17. Restart your Windows server. You have successfully disabled the SSL v3 protocol.
Direcciones Vulnerables	[redacted]

En el informe de supervisión de la Carta de Aceptación de Oferta 030 de 2020, hubo señalamiento acerca del cumplimiento de compromisos acordados, indicación de la entrega del informe para archivo en el expediente contractual; concluyendo a la fecha se ha realizado la ejecución del contrato acorde a lo estipulado en el mismo.

Aunado a lo anterior y en virtud de la observación que se registra relacionada con la actualización del Plan de Desastres, vale la pena comentar que a través de consulta realizada en la plataforma de SECOP II se pudo determinar a la fecha de elaboración de este informe (2021-04-16) se encuentra publicado el contrato 059 de 2021, suscrito con el objeto de: "Contratar el servicio profesional para el apoyo en la elaboración y actualización de documentos del proceso de gestión de tecnologías de la información, que sirvan de base en la gestión del proceso y en la implementación de planes de gestión de servicios tecnológicos; con recomendación en términos de: *Es necesario contar con personal calificado para elaborar, controlar y mantener la documentación que se requiere concerniente al grupo de sistemas de información y redes, como son manuales, procedimientos, instructivos y formatos entre otros, que deben generarse, actualizarse, y cargarse en el aplicativo ISOLUCION como parte del sistema de gestión de la entidad. De igual manera su implementación es indispensable para la gestión que desarrolla el INM, basados en las diferentes normas ISO que debe aplicar en consideración a su misionalidad. así mismo el Modelo de Planeación y Gestión, define las actividades que requieren de apoyo en temas relacionadas con la atención del proceso de gestión de tecnologías de la información, como lo son el control y reporte de indicadores, riesgos asociados al proceso, planes de mejoramiento, análisis de causas, atención de auditorías, entre otras*

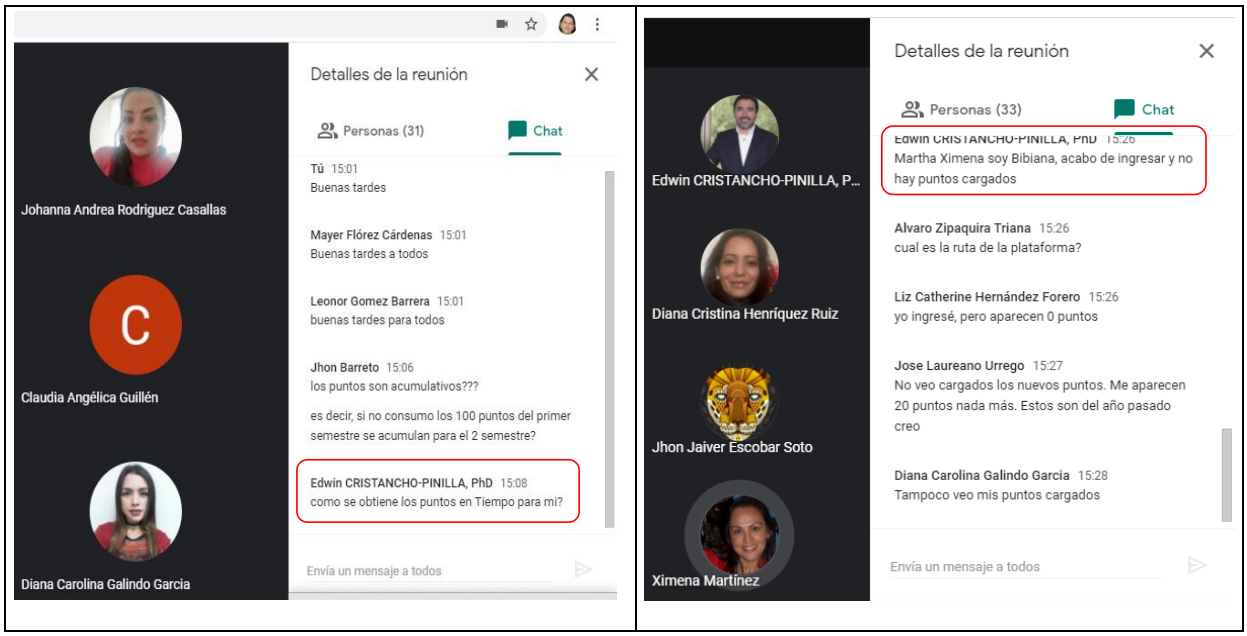
6. Acciones de motivación

Dentro del contexto organizacional previsto a la luz del Manual Técnico del Sistema de Gestión de Seguridad de la Información (Código: E-05-M-002, versión 1), fueron identificados factores que pueden afectar el desempeño u objetivos del SGSI, contemplando de manera puntual la motivación y compromiso con esquemas de mejoramiento continuo. Por expreso señalamiento a través del documento de respuesta, está previsto como acciones de motivación para el cumplimiento de los objetivos del Sistema de Gestión Seguridad entre el 1° de septiembre de 2020 y el 31 de marzo de 2021; es decir una vez liberada la última versión del Manual que nos ocupa a efectos de este seguimiento:


de los objetivos. Al respecto, lo que podemos evidenciar es que la asistencia masiva a eventos de convocatoria general, así como a eventos dirigidos a grupos específicos nos permite concluir que el personal participa y está comprometido, no sólo con el mejoramiento continuo sino con la seguridad en general. (ver soporte de eventos de sensibilización y concientización realizados durante la vigencia 2020 aquí).

A propósito de lo manifestado por el proceso a través del documento de respuesta relacionado con el compromiso en materia de seguridad, a modo de ejemplo pudo evidenciarse falta de concientización de usuarios de los sistemas por el mantenimiento de controles, cuando el 26 de marzo de 2021, durante el re lanzamiento de la plataforma Bienestar a la medida a través del link meet.google.com/kju-qhwm-

ict, se evidenció la utilización del usuario del Director General por parte de la asistente de Dirección: Bibiana Zambrano.



7. Pruebas de Seguridad de Sistemas

Conforme lo indica el Manual Técnico del Sistema de Gestión de Seguridad de la Información vigente (E-05-M-002, versión 1) las pruebas de Seguridad de Sistemas de las que trata el numeral 10.4.2 tiene por objetivo evaluar la efectividad de los controles de seguridad de la información en sistemas de información desarrollados o adquiridos y su realización permite el cumplimiento del control que hace parte del dominio de adquisición, desarrollo y mantenimiento de sistemas (identificado como A.14.2.8 de la ISO 27001:2013), por lo anterior es importante que éstas pruebas se realicen durante el desarrollo o preparación y antes de la puesta en producción de un nuevo sistema de información o la mejora a uno existente, como lo refiere el control citado.

A propósito de controles y pruebas antes de la puesta en producción de un nuevo sistema; es evidente que casos como BPMetro siguen siendo objeto de oportunidades de mejora. A modo de ejemplo se trae el caso más reciente que fuera dado a conocer y a toda luz es considerado grave, precisamente por una de las partes que en el modelo de las tres líneas de defensa es responsable de llevar a cabo actividades de control; en este caso precisamente a partir del uso del sistema en comento: BPMetro. A continuación aparte del reporte efectuado desde el proceso:

El presente es para poner en conocimiento de todos ustedes un problema del aplicativo que desde mi punto de vista es muy grave.

En el radicado 21000355 de la empresa Pinzuar Ltda, se realizó la cotización de siete servicios, sin embargo el cliente realizó el pago de sólo cuatro por un valor total de $14.711.300 como se evidencia en el correo del cliente (imagen 4.1); al momento de realizar la programación de los servicios en el aplicativo BPMetro, se evidencia que aparecen 5 instrumentos (imagen 1.1) por un valor total de $18.889.100 (imagen 2.1 y 1.1).

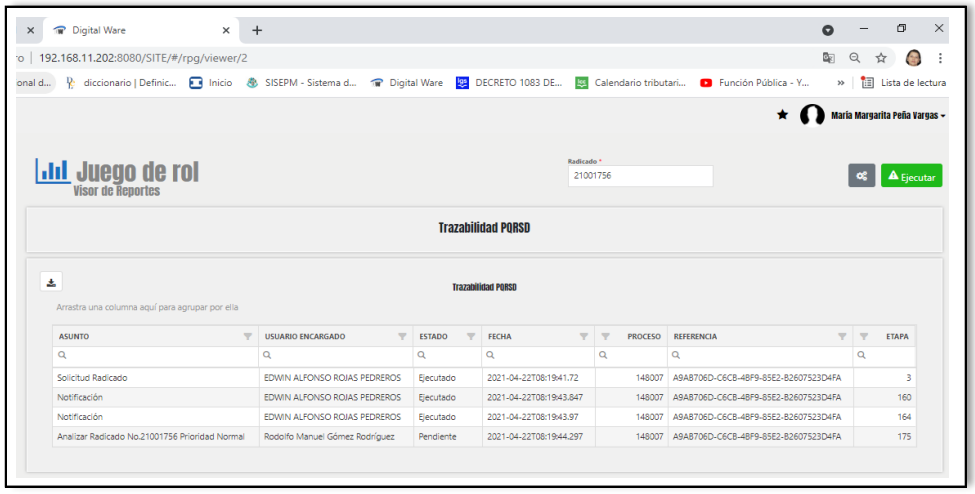
De acuerdo con lo anterior considero que es algo sumamente delicado, porque para los laboratorios el sistema es transparente y se asume que lo que aparece en el aplicativo es lo que el cliente paga y se debe programar, sin embargo, como se muestra en las imágenes, se logra evidenciar que ***el sistema habilita para programación servicios NO pagos.***

Espero que puedan tomar acciones al respecto pues se supone que el aplicativo estaba adaptado para que nada de esto sucediera.

Muchas gracias y quedo pendiente de cualquier novedad.

Atentamente

A propósito de las fallas y debilidades detectadas al sistema en otras evaluaciones realizadas por esta oficina y con antelación a este seguimiento, es preciso traer también como ejemplo las debilidades en las pruebas realizadas antes de la puesta en producción de BPMetro, cuando no es posible efectuar una validación a partir de la conversión de un reporte generado en el sistema al pasarlo a Excel para visualizar un radicado donde por ejemplo el caso traído corresponde a una víctima del ataque a las cuentas de correo del INM, fue destinatario de un mensaje mal intencionado que le ocasionara sospecha y desconfianza por no dejarlo ver en su totalidad el contenido y a partir del rol de consulta de la funcionaria María Margarita Peña Vargas tampoco es posible visualizar la totalidad del cuestionamiento realizado: "… *Deseo saber si es cierto que existe en dicha entidad la apertura de un proceso judicial en el cual me encuentro como la parte demandada"…*

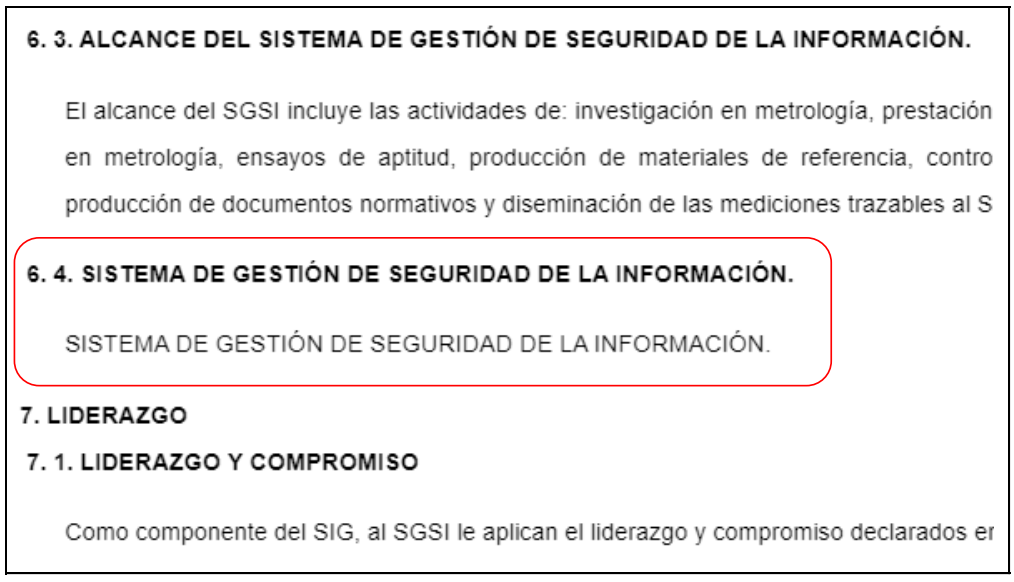


8. Seguimiento Planes de Mejoramiento

Tras la revisión del estado y avance de cumplimiento frente a acciones previstas en Planes de Mejoramiento como por ejemplo No 36 y 39 asociado al proceso de Gestión de la Información, se pudo observar a la fecha de emisión de este informe el 26 de abril de 2021, no fue gestionado ni siquiera al 50% de las acciones, tal cual como se registra en el SISEPM. Se recomienda efectuar seguimiento a la totalidad de acciones dispuestas a modo de acción a implementar y no corresponden precisamente a la vigencia en curso.

9. Actualización y ajustes del documento (E-05-M-002)

Como cualquier documento del Sistema Integrado de Gestión, al momento de ser tenido en cuenta para revisión y/o actualización el Manual objeto de este seguimiento, vale la pena adentrarse a mejorar en términos de redacción todo aquello que no es concordante con lo que en realidad se da a nivel de proceso máxime cuando es de aquellos catalogados como transversales o por incidencia a todo nivel en la entidad. Aunado a lo anterior y en cuando a redacción es de tener en cuenta por ejemplo en el numeral 6.4, señalar todo aquello de lo que diera cuenta el documento de respuesta a través del numeral 12, dejando que cualquier lector obtenga total y entera comprensión al momento de ser consultado: *da cumplimiento al requisito 4.4. de la ISO 27001:2013, el cual se refiere al establecimiento del SGSI en la organización. Los 3 elementos descritos en el manual a saber: Requisitos y Controles, Políticas y Proceso de Análisis y Gestión de Riesgos, hacen parte de la estructura del sistema y del contexto del sistema en el INM*.



6. 3. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

El alcance del SGSI incluye las actividades de: investigación en metrología, prestación en metrología, ensayos de aptitud, producción de materiales de referencia, contro producción de documentos normativos y diseminación de las mediciones trazables al S

6. 4. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

7. LIDERAZGO

7. 1. LIDERAZGO Y COMPROMISO

Como componente del SIG, al SGSI le aplican el liderazgo y compromiso declarados er

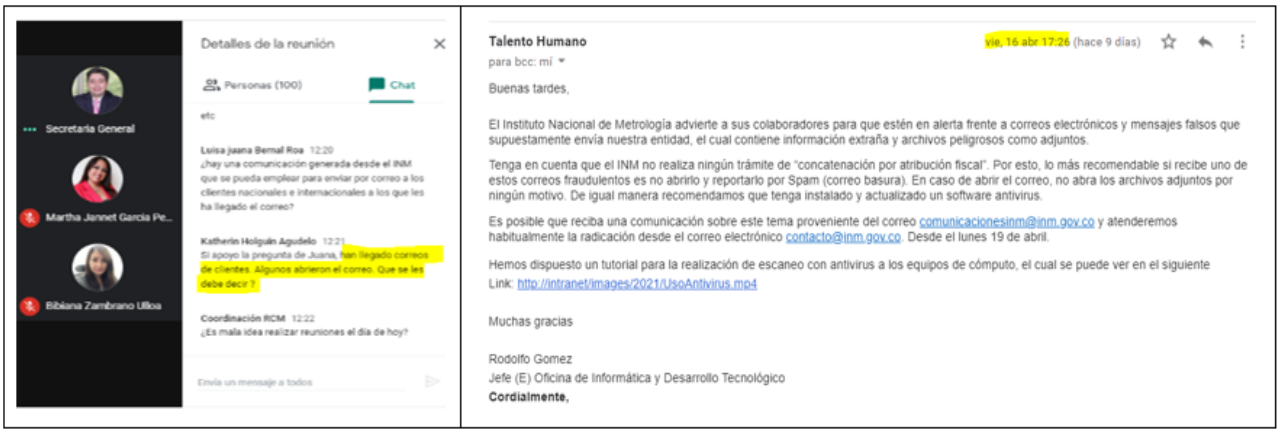
5. CONCLUSIONES

a) A partir de la publicación del Manual Técnico, constituyeron acciones concretas con efecto dentro de la entidad y su contexto: de la gestión por parte del CIGD, documentalmente

hablando: Aprobación de la actualización del Inventario de Activos de Información. CIGD – 27 (2020-12-21); Aprobación de la actualización del Manual técnico del SGSI (versión 2). CIGD – 28 (2020-12-30); Aprobación del Plan Operativo de Seguridad de la Información y Plan de Tratamiento de Riesgos de Seguridad de la Información – vigencia 2021. CIGD – 1 – 2021 (2021-01-29) y Revisión por la Dirección Requisito 9.3 de la ISO27001:2013, correspondiente al segundo semestre de 2020. Revisión SIG 2021-03-08.

b) El Profesional Especializado con Rol de Oficial de Seguridad y de Coordinador del GISIR, no tiene formalizadas las funciones que asocian los roles con las que registra el Manual de Funciones vigente (Resolución 040 de 2021).

c) Con la intrusión del 2021-04-16, hubo la posibilidad de afectación a los equipos de algunos de los usuarios (ciudadanos) que abrieron el correo y descargaron los adjuntos, tal cual como lo planteara la funcionaria Katherin Holguín a través del chat de la reunión (y Ana María Reyes) con su intervención donde solicitó colaboración formal mediante comunicado escrito, el cual fue emitido una vez finalizara la jornada ordinaria de ese día.



d) La presencia de vulnerabilidades a nivel de la página web se han visto traducidas en malogro y pérdida de información pública de uso interno y externo.

e) Con la recepción de correos mal intencionados, por parte de usuarios externos del INM se lograron generaron alarmas con expectativas de todo tipo, que en algunos casos pudieron haber sido objeto de reparación.

f) Con antelación al 16 de abril de 2021 y tras la ocurrencia de eventos adversos en sistemas de información del INM, no se llevaron a cabo o no fueron propiciados espacios de interacción (y retroalimentación) para tratamiento de lecciones aprendidas de tal manera que se pudiera generar conciencia, en materia de prevención a propósito de las recomendaciones que se hubieran dado a través de los mensajes de correos electrónicos, cuando existen por esta época casos o ejemplos tipificados.

g) Con la emisión de Circulares Internas como 013 y 014 de 2021, documentalmente quedaron formalizados lineamientos direccionados hacia la prevención frente a factores externos y/o ajenos al INM.

h) Entre la última semana de enero y finales de abril de 2021, no se ha mantenido actualizada en su totalidad la información residente en el sitio web del INM, tal cual como se ha recordado en múltiples oportunidades a través de mensajes institucionales con expreso señalamiento a todas las áreas INM que es necesario revisar, publicar y mantener actualizada la información residente en el sitio web INM, esto en cumplimiento de la ley 1712 de 2014, Decreto 103 de 2015 y Resolución MinTIC 3564 de 2015.

Adicional a lo anterior puede ser tenido como ejemplo en materia de actualización y/o restauración de información; a través de la página web no es posible visualizar la totalidad de contratos que figuran en la plataforma de SECOP II para lo correspondiente a la vigencia 2020 y ausencia de información de la vigencia 2021, tal cual como se aprecia en la ilustración que sigue, capturada desde la fuente correspondiente a solo una de las modalidades de contratación:


Contratación Directa

2020 | 2019 | 2018 | 2017

NUMERO DE CONTRATO	Nombre completo del contratista o RL	OBJETO	CONTRATO SECOP 2
1	SAMUEL	PRESTA LOS SERVICIOS DE APOYO ADMINISTRATIVO Y DE GESTION DOCUMENTAL AL GURPO DE GESTION JURIDICA DEL INM.	Ver link
2	Paula Andrea Gutierrez Gutierrez	PRESTAR SERVICIOS PROFESIONALES DE APOYO JURÍDICO PARA LA EJECUCIÓN, SOLUCIÓN Y SEGUIMIENTO DE ACTIVIDADES, ASÍ COMO LA ELABORACIÓN DE CONCEPTOS JURÍDICOS QUE SEAN REQUERIDOS POR LA SECRETARÍA GENERAL.	Ver link

i) Tanto la documentación como la socialización de documentos es importante tener en cuenta entre uno de los procesos que reviste importancia de manera transversal para la entidad. Una vez liberada la actualización del Plan de Recuperación de desastres se recomienda realizar socialización del mismo de forma práctica, preferiblemente de manera interactiva y didáctica.

j) Con la eliminación de notificaciones de aviso para validar los documentos que fueron cargados en el Sistema de Seguimiento de Planes de Mejoramiento por parte de los responsables de planes, se desató involución a nivel de seguimiento y por ende afectación de forma adversa del rol de evaluación y seguimiento que le corresponde por Ley ejercer a la Oficina de Control Interno, por ende, también con afectación a lo que constituye la tercera línea de defensa.

k) A partir del reporte efectuado de Ethical Hacking, pudo inferirse a partir de su contenido que de un lado existe nivel de exposición y posibilidades de aprovechamiento de parte de quienes se dedican a aprovecharse de las debilidades de los sistemas de formación y de otro lado la divulgación y/o tratamiento no adecuado de información que fuera catalogada por parte del proveedor como confidencial.

l) El mantenimiento de controles de acceso eficaces en lo que atañe a contraseñas de seguridad; merece fortalecimiento a todo nivel dentro de la entidad, de tal manera que guarde total consistencia y por ende cumplimiento con la PSPI 4 de la que trata el Manual Técnico del Sistema de Seguridad de la Información:

"Seguridad del Talento Humano. El grupo de gestión del talento humano liderado por su coordinador(a) realiza esfuerzos y aplica controles durante el ciclo laboral de los servidores públicos, esto es; selección, vinculación, permanencia y desvinculación, con el fin de asegurar que los servidores sean sensibilizados y educados en la puesta en práctica de las políticas de seguridad y privacidad y que los activos de información no se vean afectados por el cambio de etapa en el ciclo citado".

6. RECOMENDACIONES DE LA OCI

Mantenimiento y/o restablecimiento de funcionalidades para el SISEPM: El Sistema de Seguimiento de Planes de Mejoramiento como herramienta complementaria y de apoyo al desarrollo de labores de la Oficina de Control Interno en lo que atañe al rol de evaluación y seguimiento; ha sido intervenida desde hace algunos días sin que mediara autorización de parte de la Oficina de Control Interno para eliminar las notificaciones cuya función reviste suma importancia de doble vía tanto para el responsable del plan de mejoramiento como para la Oficina de Control Interno al momento de efectuar validación del cargue de documentos y evaluación de su efectividad.

A la fecha 26 de abril de 2021, han cursado requerimientos al área sin que haya solución y se haga necesario pasar a otra herramienta[1], acudiendo a alternativas de tipo manual que pueden

[1] Isolución

resultar siendo discrecionales y debilitando de forma importante el Sistema de Control Interno de la entidad.

A nivel institucional es evidente que existe la necesidad de estructurar un verdadero plan de comunicación, sensibilidad y capacitación en temas relacionados tanto con la seguridad como con la privacidad de la información.

Los ciberataques (información, activos, financieros, etc.) son casos que pueden servir de lección aprendida, ser tratados de manera participativa, con intercambio de experiencias y de paso interiorizar en cultura de prevención, justo cuando por esta época hay ataques a la orden del día en todos los escenarios posibles.

Contemplar la posibilidad de dar a conocer consejos que justo por esta época no sobran dados los casos de fraude y ciberataques que se presentan advirtiendo con ejemplos sencillos y prácticos como:

- Una URL que tiene https, indica una conexión segura, no un sitio web seguro. En un sitio con https, un hacker externo no puede husmear en su actividad de navegación (algo que es bueno recordar cuando esté en un sitio bancario de un proveedor). Sin embargo, el https no garantiza que el sitio no sea malicioso.

- La mejor manera de compartir información confidencial es por medio de un servidor corporativo. El correo electrónico y los medios de almacenamiento portátiles son mucho menos seguros, y las aplicaciones de uso público como Dropbox son una mala opción, pues el control de estos sistemas siempre está en manos de otra organización.

- Si usted trabaja de manera remota o accede a los sistemas de la empresa (al correo electrónico, por ejemplo) desde la red de su casa, es muy importante que utilice una conexión segura. Si no lo hace, los estafadores podrían obtener acceso a la red de su empresa y a sus datos.

- Algunos tipos de malware pueden revolver (también conocido como encriptar) su computadora y cualquier otra que esté en la misma red. A este tipo de malware se le llama ransomware. El ransomware mantiene a los datos como rehenes, a cambio de dinero.

- Aunque los archivos adjuntos maliciosos son un método común de esparcir el malware, no son la única forma. Otros métodos pueden incluir software pirata, juegos o aplicaciones gratuitas, ventanas emergentes y sitios web comprometidos. El ransomware también explota las vulnerabilidades de navegadores y otros softwares desactualizados.

- Los estafadores pueden integrar software malicioso en los archivos adjuntos. Si descarga un archivo peligroso, se puede infectar la computadora y comprometer la red de la organización.

- Los teléfonos móviles se pierden con una frecuencia alarmante, y guardan muchos datos (contactos, historial de navegación en internet, acceso a correo electrónico y más). Debe procurar por usar un NIP, contraseña u otro bloqueo de seguridad siempre que sea posible.

Sandra Lucía López Pedreros

Firmado digitalmente por Sandra Lucía López Pedreros
Fecha: 2021.05.14 20:54:16 -05'00'

Sandra Lucia López Pedreros
Jefe de Control Interno
Fecha: 2021-05-14

Revisó: Sandra Lucía López Pedreros
Elaboró: María Margarita Peña Vargas