INFORME DE AUDITORÍA											
Proceso:	Gestión de incidentes de seguridad y privacidad de la información y seguridad digital.										
Número de auditoría:	No. 02 de 2024										
Reunión de apertura						**Reunión de cierre**					
Día	09	**Mes**	09	**Año**	2024	**Día**	18	**Mes**	11	**Año**	2024

LÍDER DE PROCESO / JEFE(S) DEPENDENCIA(S):

Dr. Juan David Vélez Bolívar
Subdirector de Información (E)

EQUIPO AUDITOR

AUDITOR LÍDER: Carlos Leonardo Ortegón B, abogado contratista Control Interno de Gestión.

OBJETIVO DE AUDITORÍA: Verificar el cumplimiento del desarrollo de cada una de las actividades establecidas conforme al procedimiento *"Gestión de incidentes de seguridad y privacidad de la información y seguridad digital"*, en aquellos casos en que la Unidad ha sido objeto de estas afectaciones, de acuerdo con el impacto, urgencia y prioridad de los incidentes o eventos presentados.

ALCANCE DE AUDITORÍA: La presente auditoría se centrará en las actividades realizadas por la Subdirección de Información, conforme a los lineamientos definidos por la Unidad para la gestión de incidentes o eventos de seguridad, desde el reporte de estos hasta llegar al informe a entes de control o autoridades competentes y notificación a los afectados, para el periodo comprendido entre el 06 de julio de 2023 hasta el 30 de junio de 2024.

CRITERIOS DE AUDITORÍA:

- Lineamientos, orientaciones, condiciones, actividades y responsables definidos en el procedimiento *"Gestión de incidentes de seguridad y privacidad de la información y seguridad digital"*, código GTI - PR - 02, vigente desde el 06 de julio de 2023.
- Acciones detalladas por los responsables de los procesos.
- Demás normatividad vigente aplicable al caso.

RESUMEN GENERAL

GENERALIDADES

La Unidad Administrativa Especial de Alimentación Escolar *"Alimentos para Aprender"*, cuenta con el procedimiento denominado *"Gestión de incidentes de seguridad y privacidad de la información y seguridad digital"*, código GTI - PR – 02, el cual, fue aprobado por la Subdirección de Información y se encuentra vigente desde el día 06 de julio de 2023, siendo aplicable para todos los procesos de la UApA.

Allí, se establecen las condiciones generales o políticas de operación, así como las diferentes actividades y responsables para gestionar los incidentes y eventos de seguridad y privacidad de la información y seguridad digital, con base en los lineamientos y estándares definidos para una oportuna identificación, atención y respuesta frente a los mismos, con el

objetivo de aminorar el impacto asociado con la pérdida de confidencialidad, integridad, disponibilidad y privacidad de la información de la Unidad.

Así las cosas, para el caso de la UApA se tiene que dichos posibles incidentes o eventos de seguridad y privacidad de la información y seguridad digital, deben ser reportados a la mesa de servicio, o en el caso del ECOSISTEMA a la mesa de servicios externos, para efecto de lo anterior, se tienen dispuestos lo siguientes canales:

- ✓ Mensaje con la solicitud al correo electrónico helpdesk@uapa-pae.gov.co
- ✓ Ingresando al módulo del portal de servicios, iniciando sesión con las correspondientes credenciales, en la opción *"Registrar caso"*, en la dirección https://portaluapa-pae.gov.co/
- ✓ En la herramienta *"Teams"*, *"helpdesk UApA"*.
- ✓ Para el caso del ECOSISTEMA, mediante el correo electrónico sipaecontigo@uapa-pae.gov.co

Es importante anotar que, el colaborador o externo que identifique el posible incidente o evento de seguridad y privacidad de la información y seguridad digital, debe recopilar toda la información y soportes que lo llevó a concluir que estaba frente a este tipo de afectación, tales como capturas de pantalla, correos electrónicos, fotografías, entre otros, con el fin de ser utilizados en la atención y solución del mismo.

Después de recibida la notificación de un posible incidente o evento de seguridad y privacidad de la información y seguridad digital, la mesa de servicios debe realizar una primera categorización en la herramienta para iniciar la atención del mismo, generando un ticket o número de servicio, teniendo en cuenta los siguientes criterios:

- ✓ Daño o pérdida de información física o digital.
- ✓ Fuga y/o robo de información física o digital.
- ✓ Robo de credencias o información, mediante Phishing, Vishing, Smishing o algún ataque de este estilo.
- ✓ Modificación no autorizada de la información.
- ✓ Ocurrencia de un comportamiento anormal del computador y/o sistema de información.
- ✓ Suplantación de identidad.
- ✓ Acceso no autorizado.
- ✓ Pérdida o alteración de registros de base de datos.
- ✓ Pérdida de un activo de información.
- ✓ Presencia de código malicioso "malware, Ransomware".
- ✓ Ocurrencia de una denegación del servicio.
- ✓ Ocurrencia de algún ciberataque.
- ✓ Uso indebido de imagen institucional.
- ✓ Uso inadecuado de los recursos tecnológicos de la Entidad.

Una vez clasificado el incidente o evento de seguridad en la herramienta de gestión, se debe proceder a su categorización de acuerdo con su impacto y urgencia. En la siguiente tabla que se encuentra contemplada dentro del procedimiento[1], se muestra el impacto y su valoración, entendiendo estos últimos factores como las consecuencias que se pueden ocasionar en la UApA en caso de materializarse un evento, como se muestra a continuación:

[1] *"Gestión de incidentes de seguridad y privacidad de la información y seguridad digital"*

Impacto vs Valoración

IMPACTO	DESCRIPCIÓN	VALORACIÓN
CRÍTICO	**Catastrófico:** ➢ De presentarse el hecho, tendría desastrosas consecuencias o efectos sobre la Unidad en los sistemas de información **misionales**. ➢ Impacto operacional: Parálisis en la ejecución de varios procesos con afectaciones en la entrega de los servicios en forma generalizada a las partes interesadas o incumplimiento de los tiempos de respuesta de los trámites. ➢ Impacto en la participación ciudadana: Afectación masiva a ciudadanos en cientos de miles o superior. ➢ Afectación imagen de la UApA a nivel nacional e internacional. ➢ Sanciones a la Unidad por parte de los entes de control.	**CRÍTICO**
ALTO	**Mayor:** ➢ De presentarse el hecho, tendría altas consecuencias o efectos sobre la Unidad en los sistemas de información de **apoyo**. ➢ Impacto operacional: Parálisis en la operación de varios procesos con afectaciones en la entrega de los servicios en forma parcial a las partes interesadas o incumplimiento en los tiempos de respuesta a los trámites. ➢ Impacto en la participación ciudadana: Afectación a los ciudadanos en cantidades mayores a 1000. ➢ Afectación de la imagen de la UApA a nivel nacional. ➢ Sanciones a colaboradores por parte de los entes de control.	**ALTO**
MEDIO	**Moderado:** ➢ De presentarse el hecho, tendría consecuencias medianas o efectos sobre los sistemas de información de gestión.	**MEDIO**

	➢ Impacto operacional: Afectación en la ejecución de más de un proceso con implicaciones internas en la operación. ➢ Impacto en la participación ciudadana: Afectación a ciudadanos en cantidades superiores a 100 pero inferiores a 1000. ➢ Afectación a la imagen de un proceso al interior de la entidad. ➢ Hallazgos relacionados con la materialización de riesgos de seguridad y privacidad de la información y seguridad digital por parte de Control Interno de Gestión.	
BAJO	**Menor o insignificante:** De presentarse el hecho, tendría bajo impacto o efecto sobre la Unidad, respecto a lo siguiente: ➢ Sistemas de información común que no afectan la operación de la UApA. ➢ Impacto operacional: Afectación a la ejecución de procesos con repercusiones en la operación interna de un proceso de la Unidad o sin afectación en la ejecución de los procesos. ➢ Impacto en la participación ciudadana: Afectación a un grupo de ciudadanos menor a 100 o sin afectación directa a ningún ciudadano.	**BAJO**

Tabla No. 1 – Elaborada por Control Interno de Gestión con base en el Procedimiento *"Gestión de incidentes de seguridad y privacidad de la información y seguridad digital"*, en el mes de septiembre de 2024.

Urgencia

Urgencia	Descripción
Crítica	El incidente o evento de seguridad y privacidad de la información y seguridad digital debe atenderse inmediatamente, es decir, entre 0 – 1 hora contada a partir del reporte.
Alta	El incidente o evento de seguridad y privacidad de la información y seguridad digital debe atenderse inmediatamente, es decir, entre 0 – 2 horas contadas a partir del reporte.
Media	El incidente o evento de seguridad y privacidad de la información y seguridad digital debe atenderse inmediatamente, es decir, entre 0 – 4 horas contadas a partir del reporte.
Baja	El incidente o evento de seguridad y privacidad de la información y seguridad digital debe atenderse inmediatamente, es decir, entre 0 – 8 horas contadas a partir del reporte.

Tabla No. 2 – Elaborada por Control Interno de Gestión con base en el Procedimiento *"Gestión de incidentes de seguridad y privacidad de la información y seguridad digital"*, en el mes de septiembre de 2024.

Es importante anotar que, los anteriores tiempos corresponden al máximo en que debe ser atendido el incidente o evento de seguridad y privacidad de la información, pero no al tiempo en que deben ser solucionados, pues esto dependerá de cada caso. Igualmente, la prioridad de la atención de dichos incidentes está asociada a la valoración del impacto y la urgencia como se muestra en la siguiente tabla:

URGENCIA	IMPACTO	PRIORIDAD
Crítica	Crítico	1 - Crítica
Alta	Alto	2 - Alta
Media	Medio	3 - Media
Baja	Bajo	4 - Baja

Tabla No. 3 – Elaborada por Control Interno de Gestión con base en el Procedimiento *"Gestión de incidentes de seguridad y privacidad de la información y seguridad digital"*, en el mes de septiembre de 2024.

Como mínimo los equipos de respuesta que atiendan los incidentes o eventos de seguridad y privacidad de la información y seguridad digital están conformados por las siguientes personas:

- ✓ El propietario y/o custodio del activo.
- ✓ El profesional de la Subdirección de Información que apoya la gestión de incidentes o eventos.
- ✓ Demás profesionales de las oficinas que tengan a cargo activos o servicios que se vean afectados.
- ✓ Oficial de seguridad de la información o quien haga sus veces.

De la misma manera, este equipo puede solicitar información o participación de otros colaboradores, procesos, especialistas y operadores estratégicos para la atención del incidente o evento.

En aquellos incidentes o eventos de seguridad que sean considerados **CRÍTICOS o ALTOS**, se debe informar al oficial de seguridad o quien haga sus veces, para que informe a la alta gerencia (Comité Institucional de Gestión y Desempeño) sobre la ocurrencia del mismo y active el Plan de Recuperación ante Desastres – DRP, de la misma manera, se debe instalar la mesa de crisis con el fin de analizar los recursos financieros, humanos y tecnológicos, así como evaluar alternativas para contener, erradicar y solucionar el incidente o evento.

Aunado a lo anterior, se debe reportar ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) del Gobierno para el apoyo y coordinación en la gestión de los incidentes o eventos, a través del formato de reporte establecido por dicho Equipo, el cual, estará disponible en los canales de comunicación autorizados.

Igualmente, es importante conservar las evidencias recolectadas para evitar que las mismas sufran modificaciones y no sean admisibles posteriormente en un proceso judicial, por tanto, dependiendo de la evidencia que se genere en la gestión del incidente o evento de seguridad y privacidad de la información y seguridad digital, se determinará el lugar donde debe conservarse la misma, es decir, las evidencias producto de un ataque informático (Logs de auditoría) se almacenarán en un repositorio que cumpla con los requisitos mínimos de seguridad de acuerdo con la clasificación de la información, con el fin de garantizar la integridad, disponibilidad y confidencialidad de la misma. En todo caso, para la recolección de evidencias de elementos informáticos deben seguirse los lineamientos establecidos en el manual de custodia de la Fiscalía General de la Nación.

Aquellos incidentes o eventos de seguridad que el equipo de respuesta considere pertinente, serán postulados a la base de datos de conocimiento, en el módulo de artículos de conocimiento que se encuentra disponible en la herramienta de gestión, siguiendo lo establecido en el modelo de gestión de conocimiento de la Unidad. Por otro lado, es importante tener

en cuenta que, algunos incidentes o eventos de seguridad pueden ser solucionados desde su contención, pero otros requieren la recuperación o restauración del sistema a su estado normal de operación.

Los incidentes o eventos de seguridad y privacidad de la información y seguridad digital deben ser documentados en la herramienta de gestión de servicios, no obstante, para los incidentes con impacto **ALTO** o **CRÍTICO** también se debe elaborar un informe que evidencie las actividades realizadas para su contención y solución para el respectivo cierre.

Cuando el incidente o evento de seguridad y privacidad de la información y seguridad digital comprometa datos personales, debe reportarse la novedad por parte del oficial de protección de datos personales a la Superintendencia de Industria y Comercio a través del formato dispuesto para tal fin, apoyándose del manual de usuario RNBD de la Superintendencia.

La Dirección de la Unidad a través del oficial de seguridad y privacidad de la información, son los únicos autorizados para reportar los incidentes o eventos a entes externos, solo en aquellos casos en que la solución y contención se encuentre fuera del alcance del personal encargado de la Unidad.

Los canales dispuestos para el reporte a los entes previamente mencionados son los siguientes:

- ✓ CSIRT Gobierno, reportar al correo csirtgob@mintic.gov.co, y la línea 01 8000 910742 Opción 2, seguridad digital.
- ✓ Centro cibernético Policial reportar en la siguiente ruta: https://caivirtual.policia.gov.co/
- ✓ ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), reportar al correo electrónico: contacto@colcert.gov.co o al Teléfono: (+571) 2959897.

Asimismo, los incidentes o eventos de seguridad y privacidad de la información y seguridad digital que sean considerados por los responsables como **MEDIOS** y **BAJOS** deben ser comunicados al CSIRT Gobierno para efecto de llevar una estadística de los incidentes y conocer las tipologías de los mismos. El oficial de seguridad de acuerdo con las lecciones aprendidas interiorizará y generará conciencia en los demás colaboradores mediante estrategias sobre la gestión del reporte de incidentes.

Finalmente, se debe notificar a los afectados sobre los incidentes o eventos de seguridad que afecten la confidencialidad, disponibilidad, integridad o privacidad de la información, así como de las medidas adoptadas para solucionarlo.

No	Actividad	Descripción	Responsable
1	Reportar el posible incidente o evento de seguridad y privacidad de la información y seguridad digital.	Reportar el posible incidente o evento de seguridad a la mesa de servicios a través de los canales definidos por la Unidad en el procedimiento.	Servidores públicos y contratistas de la UApA.
2	Registro del incidente o evento.	Categorizar y registrar el incidente o evento de seguridad en la herramienta de gestión, generando el ticket o número de servicio.	Profesionales de la Subdirección de Información.
3	Gestionar el incidente o evento de seguridad.	Analizar y clasificar el incidente o evento de seguridad reportado y categorizarlo en la herramienta de gestión de acuerdo con su impacto y urgencia.	Oficial de seguridad y privacidad de la información o quien haga sus veces.

			Profesionales de la Subdirección de Información.
4	Seleccionar los equipos de respuesta a los incidentes o eventos de seguridad.	Comunicar a los implicados en la solución y conformar los equipos de respuesta como mínimo por los siguientes integrantes: el propietario y/o custodio del activo, el profesional de la Subdirección de Información, los profesionales de las oficinas que tengan a cargo activos o servicios que se vean afectados y el oficial de seguridad de la información o quien haga sus veces.	Oficial de seguridad y privacidad de la información o quien haga sus veces. Profesionales de la Subdirección de Información.
5	Analizar el incidente o evento de seguridad y privacidad de la información y seguridad digital.	Hacer el análisis correspondiente para determinar la causa o causas que dieron origen al incidente o evento de seguridad.	Oficial de seguridad y privacidad de la información o quien haga sus veces. Profesionales de la Subdirección de Información.
6	Contención del incidente o evento de seguridad.	El grupo de respuesta a incidentes o eventos de seguridad y privacidad de la información y seguridad digital debe desarrollar todas las acciones necesarias para contener el incidente y minimizar su impacto.	Oficial de seguridad y privacidad de la información o quien haga sus veces. Profesionales de la Subdirección de Información.
7	Erradicación de la causa raíz del incidente o evento de seguridad.	Realizar todas las acciones necesarias por parte del equipo de respuesta, con el objetivo de erradicar la causa raíz que origina el incidente o evento de seguridad y privacidad de la información y seguridad digital.	Oficial de seguridad y privacidad de la información o quien haga sus veces. Profesionales de la Subdirección de Información.
8	Solución del incidente o evento de seguridad y privacidad de la información y seguridad digital.	Realizar todas las acciones necesarias por parte del equipo de respuesta, con el objetivo de solucionar el incidente o evento de seguridad.	Oficial de seguridad y privacidad de la información o quien haga sus veces. Profesionales de la Subdirección de Información.
9	Documentar las evidencias del incidente o evento de seguridad.	Se deben organizar y conservar las evidencias recopiladas en la investigación	Oficial de seguridad y privacidad de la

		del incidente o evento de seguridad, con el fin de evitar que las mismas sufran modificaciones y no sean admisibles ante un ente judicial.	información o quien haga sus veces. Profesionales de la Subdirección de información.
10	Protección de las evidencias.	De acuerdo con la evidencie que se genere en el tratamiento del incidente o evento de seguridad, se determina el lugar en que debe conservarse, por ejemplo, cuando se trate de un ataque informático se debe almacenar la evidencia en un repositorio, para garantizar la integridad, disponibilidad y confidencialidad de la misma. No obstante, deben seguirse los lineamientos definidos por la Fiscalía General de la Nación en el manual de cadena de custodia.	Oficial de seguridad y privacidad de la información o quien haga sus veces. Profesionales de la Subdirección de información.
11	Documentar el incidente o evento de seguridad y privacidad de la información y seguridad digital.	Se debe documentar el incidente o evento de seguridad en la herramienta de gestión de servicios y para aquellos casos que sean considerados con ALTO o CRÍTICO impacto, se debe generar adicional un informe sobre las actividades de contención y solución adelantadas. Cuando el incidente o evento de seguridad esté relacionado con datos personales, se debe reportar a la Superintendencia de Industria y Comercio.	Profesionales de la Subdirección de información. Oficial de Protección de Datos Personales o quien haga sus veces.
12	Informar a los entes de control o autoridades competentes sobre el incidente o evento de seguridad.	Con base en la evidencia recopilada, se evalúa si se debe poner en conocimiento de los entes de control o autoridades competentes	Oficial de Seguridad de la Información o a quien la Dirección delegue las funciones.
13	Revisar las respuestas a los incidentes o eventos de seguridad y privacidad de la información y seguridad digital.	Revisar la respuesta y solución dada al incidente o evento de seguridad, precisando que, aquellos que sean considerados por el equipo de respuesta serán postulados a la base de datos de conocimiento, específicamente en el módulo de artículos de conocimiento disponible en la herramienta de gestión.	Oficial de seguridad y privacidad de la información o quien haga sus veces. Profesionales de la Subdirección de información.

14	Notificación a los afectados con el incidente o evento de seguridad y privacidad de la información y seguridad digital.	Se debe informar a los afectados sobre el incidente o evento de seguridad que afecte la confidencialidad, integridad o privacidad de su información, igualmente, se debe poner en conocimiento las medidas adoptadas para la superación del mismo.	Oficial de seguridad y privacidad de la información o quien haga sus veces.
15	Reportar el posible incidente o evento de seguridad	Reportar el incidente o evento de seguridad de acuerdo con lo señalado en los párrafos precedentes.	Servidores públicos y contratistas de la Unidad.

Cuadro No. 01 – Elaborado por Control Interno de Gestión con base en el procedimiento *"Gestión de incidentes de seguridad y privacidad de la información y seguridad digital"*, en el mes de septiembre de 2024.

ACCIONES DE SEGUIMIENTO

Control Interno de Gestión presentó el día 09 de septiembre de 2024 el requerimiento de información sobre los incidentes o eventos de seguridad y privacidad de la información y seguridad digital, ocurridos en la Unidad durante el periodo comprendido entre el 06 de julio de 2023 al 30 de junio de 2024, el cual, fue resuelto por parte de la Subdirección de Información el día 27 de septiembre de 2024, informando lo siguiente:

- ✓ Durante el periodo previamente referido no se presentaron incidentes o eventos de seguridad y privacidad de la información y seguridad digital, por lo anterior, no se reportó ninguno a través de los canales de comunicación dispuestos para tal fin.

- ✓ Teniendo en cuenta que no se presentó ningún incidente o evento de seguridad y privacidad de la información y seguridad digital durante el periodo mencionado, no se cuenta con soportes de registro, categorización y clasificación de alguno.

- ✓ En razón a lo expuesto, tampoco se cuenta con soportes sobre la identificación, contención y solución de incidentes o eventos de seguridad, así como tampoco hubo lugar al diligenciamiento del formato GTI-FR-10 *Registro de incidentes de seguridad y privacidad de la información y seguridad digital*, ni del formato GTI-FR-09 *Acta de recolección de evidencias digitales.*

No obstante, la Subdirección de Información con su respuesta remitió los soportes relacionados con el ataque cibernético sufrido por IFX Networks, el cual, afectó de manera indirecta a la Unidad con la interrupción del aplicativo KACTUS HCM en el mes de septiembre de 2023, por tanto, en el presente informe se detallarán las causas, solución, tiempos de respuesta y forma en que fue abordada dicha situación.

- ✓ **Ataque de ciberseguridad sufrido por IFX Networks**

Generalidades del ataque

Con relación al ataque de ciberseguridad sufrido por IFX Networks el día 12 de septiembre de 2023, es importante anotar que, de acuerdo con lo señalado por la Subdirección de Información, la Unidad Administrativa Especial de Alimentación

Escolar *"Alimentos para Aprender"* no tiene su infraestructura tecnológica alojada en los servidores de IFX, por tanto, no se vieron afectados con el ataque cibernético aplicaciones como el Ecosistema SiPAE, Aranda, página web en construcción y el servicio de Office 365 (paquete de ofimática que contiene Word, Excel, PowerPoint, OneDrive, SharePoint, entre otros), los cuales, se encuentran en la nube pública de Microsoft Azure.

Sin embargo, para el caso del aplicativo KACTUS HCM contratado para los servicios tipo SaaS[2] de los módulos Nómina y Gestión del Talento Humano, la Unidad suscribió el contrato No. UAPA-OPS-029-2023 con el proveedor DIGITALWARE S.A.S., el cual, si tiene su infraestructura tecnológica alojada en IFX, por tanto, se vio afectada por el ataque (Ransomware) de manera indirecta la Unidad para efecto de la liquidación de la nómina del mes de septiembre de 2023.

Al respecto, se encuentra que DIGITALWARE notificó a la Unidad a través de oficio de fecha 12 de septiembre de 2023, manifestando que se había presentado un inconveniente que impactaba el servicio SaaS y que se encontraban trabajando para superar el mismo en el menor tiempo posible, de la misma manera, allegó la certificación correspondiente para presentar ante la Dirección de Impuestos y Aduanas Nacionales – DIAN, en atención a lo estipulado en el artículo 14 de la Resolución No. 000013 del 11 de febrero de 2021.

Posteriormente, DIGITALWARE remitió a la Unidad el día 15 de septiembre de 2023 el seguimiento al inconveniente tecnológico, donde señaló que, IFX Networks como su proveedor de Data Center precisó que no se evidenciaron vulnerabilidades en la información, privacidad y seguridad de los datos alojados en la nube, debido a los protocolos de seguridad de la información.

Después se recibió en la UApA un nuevo seguimiento al inconveniente tecnológico, con fecha 26 de septiembre de 2023, donde DIGITALWARE informó que, de acuerdo con la información reportada por IFX, ya se habían reestablecido 5707 servicios equivalentes al 94,7%, por tanto, el CSIRT había procedido a cerrar el Puesto de Mando Unificado habilitado para la gestión del incidente tecnológico.

Medidas adoptadas por la UApA frente al ciberataque

La Unidad Administrativa Especial de Alimentación Escolar *"Alimentos para Aprender"*, adelantó la gestión correspondiente con el proveedor para adoptar las medidas iniciales de contingencia, con el objetivo de liquidar la nómina del mes de septiembre de 2023, estas medidas contemplaron, entre otras, las siguientes:

- ✓ El uso de un sistema parametrizado, es decir, un KACTUS temporal para el mes de septiembre 2023.
- ✓ El uso de las copias de seguridad de la base de datos solicitada mensualmente al proveedor en el marco de la ejecución contractual.
- ✓ La disposición de la información que se tenía para configurar el sistema temporal y poder liquidar la nómina del mes de septiembre 2023.

No obstante, la Unidad decidió realizar el proceso de liquidación de la nómina manualmente y evitar que la misma se hiciera en forma extemporánea, con el compromiso de que el proveedor posteriormente realizara la migración de la información del mes de septiembre 2023 al KACTUS, sin que ello generara costos adicionales para la UApA. Dicha decisión se tomó teniendo en cuenta que para el uso del KACTUS temporal era necesario tener toda información de la liquidación de la

[2] El software como servicio (SaaS) es un modelo de entrega de software basado en la nube, es decir, permite a los usuarios conectarse a aplicaciones que están en la nube a través de internet, con un sistema de pago por uso.

nómina del mes de agosto 2023, con el fin de que este sistema pudiera calcular la de septiembre sin inconvenientes, situación que requería de un tiempo de verificación adicional.

De la misma manera, se realizó un seguimiento diario a los boletines del COLCERT – CSIRT Presidencia y se envió el día 14 de septiembre de 2023, a través del correo electrónico de la Oficina Asesora de Comunicaciones, recomendaciones a todos los colaboradores de la Unidad frente a ataques cibernéticos. Igualmente, la Subdirección de Información presentó diferentes recomendaciones para que este tipo de incidentes no afecten la continuidad de la operación de los servicios que presta la Unidad, dentro de las que se encuentran las siguientes:

- ✓ El fortalecimiento de las obligaciones en contratos, convenios o acuerdos, con los proveedores frente a la continuidad de los servicios.
- ✓ Identificar escenarios de riesgos de interrupción de los servicios en los contratos, convenios o acuerdos que se generen.
- ✓ Asistir a las capacitaciones de seguridad y privacidad de la información convocadas por la Subdirección de Información.
- ✓ Generar conciencia en los colaboradores de la Unidad frente a las afectaciones de los ataques de ingeniería social (Phishing, Vishing, Smishing, Spear Phishing, entre otros).
- ✓ Acatar las recomendaciones de seguridad y privacidad de la información impartidas por los expertos y demás entidades del estado rectoras en la materia.

De igual modo, el día 25 de septiembre de 2023 la supervisora del contrato por parte de la UApA presentó solicitud de información a DIGITALWARE, con el objetivo de conocer de manera detallada las acciones de mitigación, prevención, corrección y mejora frente al ataque cibernético sufrido, incluyendo los componentes tecnológicos y contractuales. Por otro lado, manifestó la necesidad de implementar un plan de acción conjunto para garantizar la integridad, confidencialidad y disponibilidad de la información y de los sistemas de la Unidad, conforme lo establece la Ley 527 de 1999[3] y la Ley 1581 de 2012[4].

En ese orden de ideas, DIGITALWARE dio respuesta a los interrogantes mediante oficio fechado del 17 de octubre de 2023, en el que manifestó lo siguiente:

Componente tecnológico

- ✓ *Sobre los centros alternos de la infraestructura tecnológica que soporta KACTUS y los espejos con los que cuenta DigitalWare para evitar interrupción del servicio.*

  Con relación a este punto manifestó que el Data Center de IFX Networks contratado por ellos, establece en su política de servicio que, adicional al respaldo dinámico, también se genera un backup con toda la información de DIGITALWARE y la de sus clientes, igualmente, señaló que dentro de los protocolos y políticas de seguridad de la información de IFX, se encuentra la denominada *"SEG-PL01 Políticas Generales de Seguridad de la Información"*, la cual, contempla el respaldo de la información crítica de la compañía de manera periódica, almacenando la misma en custodia externa o enviados a Datacenters alternos que cuentan con mecanismos de protección ambiental como detección de humo, incendio, humedad y mecanismos de control de acceso físico.

[3] *"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"*

[4] *"Por la cual se dictan disposiciones generales para la protección de datos personales"*

✓ *Sobre la planeación para la migración de la información de la nómina de septiembre al KACTUS en producción, dado que esta fue gestionada manualmente por la Unidad*

Frente a este punto, DIGITALWARE indicó que la Unidad decidió realizar el cargue de las novedades en el aplicativo KACTUS HCM y liquidar la nómina en el ambiente productivo, por tanto, no fue necesaria la migración de la información.

✓ *Sobre la afectación y vulneración de la data de la Unidad tras el ataque.*

DIGITALWARE manifestó que, de acuerdo con las investigaciones realizadas por los especialistas externos en ciberseguridad de IFX, no se encontraron indicaciones de que la información se haya visto comprometida con el ataque, también informaron que no se tiene evidencia de una fuga de datos personales ni que los mismos hayan sido publicados en la web oscura.

✓ *Sobre el árbol de comunicación interna y externa ante incidentes que impliquen la interrupción del servicio contratado.*

Frente al particular, DIGITALWARE señaló que cuenta con diferentes niveles de escalonamiento que detallan las actividades y participantes involucrados en cada etapa, dichos niveles se activan una vez se ha registrado la solicitud en su herramienta de gestión de solicitudes, como se muestra en la siguiente imagen:

Imagen No. 01 – Capturada por Control Interno de Gestión del documento *"Solicitud de informe y plan sobre acciones frente a ciberataque a IFX Networks"*, en el mes de septiembre de 2024.

✓ *Sobre las buenas prácticas de desarrollo seguro del sistema de información de KACTUS.*

Respecto a este punto, DIGITALWARE aclaró que contrató con IFX Networks un Data Center que tiene implementada una Política de Desarrollo Seguro (DES-PL03), la cual, define lineamientos para el desarrollo de aplicaciones a través del uso de buenas prácticas internacionales de seguridad basadas en OWASP[5], que

[5] *"Proyecto de código abierto dedicado a establecer y eliminar los errores que provocan que un software no sea seguro"*

aseguran la información confidencial y fomentan la cultura de Seguridad de la Información en el desarrollo de las diferentes aplicaciones, teniendo en cuenta los siguientes criterios:

- Autenticación.
- Autorización.
- Gestión de cookies.
- Validación de entrada de datos.
- Gestión de errores y fuga de información.
- Log de Auditoria.
- Cifrado de datos.
- Entorno de código seguro.
- Gestión de sesiones (login/logout).

✓ *Sobre los planes de contingencia ante eventos que impliquen la interrupción de los servicios, donde se contemplen los tiempos de recuperación que requiere la entidad en los procesos que se realicen en KACTUS.*

Al respecto, DIGITALWARE indicó que cuenta con un plan de continuidad del servicio, que presenta posibles escenarios que podrían enfrentarse y la forma en que se recuperaría la operación ante algún tipo de contingencia, es decir, allí se definen estrategias que permiten reanudar la operación de DIGITALWARE, enfocándose en procesos críticos y/o sensibles de tecnologías, así como también, en la implementación de actividades que involucran procesos críticos de tecnología de DIGITALWARE con los servicios del tercero.

✓ *Plan de continuidad de la operación del servicio contratado.*

De acuerdo con lo manifestado por DIGITALWARE en su respuesta, IFX Networks cuenta con un plan de continuidad del negocio (SEG-PN03), el cual, asegura que la compañía se encuentra preparada para responder ante posibles eventos de desastre, recuperarse de los mismos y mitigar los impactos ocasionados sobre los servicios de internet, cloud y datacenter que se puedan materializar sobre la Infraestructura Tecnológica que hace parte del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) y del Sistema de Gestión de Servicios (SGS), permitiendo la continuidad de los servicios críticos para la operación.

Dicho en otras palabras, el objetivo de este plan es la protección de los procesos críticos del negocio contra desastres o fallas mayores, junto con las posibles consecuencias que se puedan tener, ya sean de tipo financiero, legales, de imagen, etc., por la no disponibilidad de los recursos de IFX para la prestación de sus servicios.

Componente contractual

Para los efectos del presente informe solamente se observarán aquellas obligaciones generales y específicas que están relacionadas con el ciberataque sufrido por IFX Networks, que afectó de manera indirecta a la Unidad con la indisponibilidad del aplicativo KACTUS en el mes de septiembre de 2023, así como la respuesta dada por DIGITALWARE frente al cumplimiento de las disposiciones contractuales, con ocasión del requerimiento presentado por la Subdirección de Información el 25 de octubre de 2023.

Obligaciones Generales

1. *Informar al supervisor, en el momento que ocurran incidentes de seguridad o se materialice un riesgo de seguridad y privacidad de la información que afecten la disponibilidad, integridad, confidencialidad o privacidad de la información de la entidad, en el marco de la ejecución del contrato.*

   Respecto a esta obligación, DIGITALWARE manifestó que informó a la Unidad sobre el inconveniente tecnológico que se estaba presentando en el servicio SaaS el mismo día en que tuvo conocimiento del ataque cibernético, esto es, el 12 de septiembre de 2023. De la misma manera, indicó que posteriormente los días 13, 15, 19 y 26 de septiembre de 2023 remitieron al correo electrónico de la supervisora del contrato, los comunicados del avance y actualización del inconveniente tecnológico referido.

2. *Salvaguardar los activos de información de la Unidad Administrativa Especial de Alimentación Escolar.*

   Con relación a esta obligación y como se señaló en los párrafos precedentes, el proveedor informó que IFX Networks cuenta con un backup adicional al respaldo dinámico, con toda la información de DIGITALWARE y la de sus clientes activos, así como con los protocolos y políticas de protección de la información

3. *Prever el plan de recuperación y contingencia del servicio contratado ante los eventos que puedan afectar el cumplimiento de la ejecución de éste.*

   DIGITALWARE S.A.S cuenta con un plan de continuidad del servicio denominado *"DOC-039-Plan-de-Continuidad-del-Servicio-V3"*, de la misma manera, el proveedor IFX Networks cuenta con su plan de continuidad denominado *"SEG-PN03 Plan de continuidad de negocio"*, respecto de los cuales se hizo referencia y la explicación correspondiente en los párrafos precedentes del componente tecnológico.

4. *Disponer de los medios necesarios para el mantenimiento, cuidado y custodia de la información objeto del presente contrato.*

   DIGITALWARE manifestó en su respuesta que, IFX Networks tiene implementado el documento denominado *"GOR-PN02 Plan de Mantenimiento de Data Center"*, el cual, define aspectos relacionados con las actividades de mantenimiento preventivo en el Data Center que soporta los servicios de cloud, conectividad y seguridad. Es decir, este mantenimiento preventivo incluye el reemplazo de componentes al interior del Data Center, el ajuste de los mismos, limpieza de filtros de aire, lubricación y se revisan las condiciones generales de la infraestructura física. Igualmente, dentro de las actividades de mantenimiento realizadas también se destacan las siguientes:

   - Mantenimiento del sistema electrógeno.
   - Mantenimiento del sistema de respaldo (UPS).
   - Mantenimiento del sistema mecánico (Aire acondicionado).
   - Mantenimiento del sistema contra incendios.
   - Mantenimientos no invasivos.

Obligaciones específicas

1. *Cumplir con las horas contratadas acorde con las necesidades de la Entidad*
   Con relación a esta obligación, DIGITALWARE señaló que las horas contratadas se ejecutaron de acuerdo con la necesidad de la Unidad, pero aclaró que esta responsabilidad contractual es ajena a la situación que se presentó con el Data Center de IFX Networks.

2. *Garantizar que las actividades desarrolladas durante la ejecución del contrato no interfieran en la continuidad, disponibilidad, integridad e interoperabilidad de los servicios informáticos de la UAPA*

   Frente a esta disposición contractual, el proveedor manifestó que las actividades de mantenimiento y soporte que se programaron no interfirieron en la continuidad, disponibilidad, integridad e interoperabilidad de los servicios informáticos de la Unidad de Alimentos para Aprender, sin embargo, reiteraron que la situación presentada con el Data Center de IFX es ajena a la responsabilidad contractual.

3. *Garantizar la integridad y confidencialidad de la información institucional a la cual llegue a tener acceso directamente o por intermedio de terceros. Adoptar todas las medidas necesarias para impedir su duplicación, sustracción, divulgación, alteración, ocultamiento o utilización indebida. En ninguna circunstancia, dicha información y/o documentación podrá ser utilizada por el contratista para fines distintos al desarrollo del contrato. Al finalizar la ejecución del contrato, toda la información y documentos entregados deben ser retornados a la Entidad*

   Al respecto, DIGITALWARE manifestó que de acuerdo con las investigaciones realizadas por los especialistas externos en ciberseguridad de IFX, no se encontraron indicios de que la información se haya visto comprometida con el ataque. De la misma manera, indicaron que no existe evidencia sobre una fuga de datos personales ni que los mismos haya sido publicados en la web oscura.

4. *El contratista se obliga a atender cualquier solicitud de soporte de la aplicación teniendo en cuenta el nivel de complejidad en horas laborales*

5. *Atender, gestionar y solucionar, en los tiempos establecidos en los acuerdos de niveles de servicio, los incidentes reportados sobre todos los módulos implementados durante la ejecución del contrato*

   Sobre las anteriores obligaciones (4 y 5), DIGITALWARE señaló que una vez se presentó el incidente con el Data Center de IFX Networks, se activaron todos los niveles de servicio para dar respuesta, soporte e información a la Unidad, así como también se elaboró y coordinó un plan de contingencia para el aplicativo KACTUS, el cual, se explicó en los párrafos precedentes.

6. *Informar de inmediato y por escrito, a la supervisión del contrato, la ocurrencia de cualquier novedad o anomalía, situaciones de fuerza mayor o caso fortuito que puedan afectar la ejecución del contrato, incluyendo las recomendaciones que procedan según el caso*

   Con relación a esta obligación, el proveedor DIGITALWARE manifestó en su respuesta que el mismo día en que tuvo conocimiento del ciberataque, esto es, el 12 de septiembre de 2023, comunicó a la Unidad Administrativa Especial *"Alimentos para Aprender"* sobre el inconveniente tecnológico presentado en su servicio SaaS.

Igualmente, que los días 13, 15, 19 y 26 de septiembre de 2023, envió vía correo electrónico a la supervisora del contrato por parte de la UApA, los comunicados sobre el avance y actualización del inconveniente tecnológico.

Informe de IFX Networks a DIGITALWARE S.A.S.

En el informe presentado por IFX Networks de fecha 06 de octubre de 2023, manifiestaron que desde que detectaron el incidente el día 12 de septiembre de 2023, su Centro de Operaciones de Seguridad (SOC) en colaboración con sus asesores externos pusieron en marcha de forma inmediata todos los protocolos y políticas para asegurar los sistemas, implementando a su vez, la política de recuperación partiendo de los procesos de la norma ISO 27001, con las siguientes acciones:

- Conformación de mesa de crisis para la atención de la situación.
- Investigación de las acciones ejecutadas por el atacante, impacto generado, detección y neutralización de amenazas adicionales, análisis forense de la situación y causa raíz.
- Investigación forense para contener el ataque y restablecer las actividades de operación.
- Trabajo directo con los fabricantes de los componentes base de la arquitectura de la nube para la construcción, implementación y aseguramiento de las plataformas.
- Cierre de privilegios, cambios de credenciales, aislamiento de conexiones a servicios funcionales y a redes comprometidas.

En ese orden de ideas, detectaron que el malware de cifrado no tuvo la capacidad de autorreplicación ni de replicarse lateralmente, por tal motivo, no existió riesgo de que se propagara a las redes de los clientes, igualmente, se encontró que solamente afectó una parte limitada de sus sistemas ESXi, por ende, los demás sistemas que no se ejecutan con dichos sistemas funcionaron con normalidad.

En cuanto a las afectaciones generadas, IFX informó que, de acuerdo con las investigaciones de sus especialistas, no existe indicación alguna de que la información se haya visto comprometida, ni de violación de los códigos de seguridad, ni de pérdida, robo y/o acceso no autorizado de información alguna de las bases de datos. No obstante, en el marco de la Resolución No. 6890 del 19 de julio de 2022[6], IFX reportó el incidente de ciberseguridad el mismo 12 de septiembre de 2023 a los correos malware@colcert.gov.co y contacto@colcert.gov.co, es decir, dentro de las 24 horas hábiles subsecuentes a la detección del incidente, cumpliendo con el deber de reportar al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT). De la misma manera, se notificó a la Fiscalía General de la Nación, Superintendencia de Industria y Comercio y Colombia Compra Eficiente.

Finalmente, IFX Networks señaló en su informe de fecha 06 de octubre de 2023, que se había comunicado públicamente a sus clientes que se encontraban restaurados los servicios y que los sistemas y clientes no reportaban novedades en su funcionalidad, así mismo señalaron que todos los sistemas habían sido sometidos a un proceso de validación, pruebas y garantía antes de ser puestos en funcionamiento.

[6] *"Por la cual se modifican algunas disposiciones del régimen de calidad para los servicios de telecomunicaciones contenidas en los capítulos 1 y 2 del Título V de la Resolución CRC 5050 de 2016 y se dictan otras disposiciones"*

FORTALEZAS

- La Unidad Administrativa Especial *"Alimentos para Aprender"*, cuenta con el procedimiento *"Gestión de incidentes de seguridad y privacidad de la información y seguridad digital"*, código GTI - PR – 02, el cual, permite una oportuna identificación, atención y respuesta frente a los eventuales incidentes o eventos que se presenten, con el objetivo de aminorar el impacto asociado con la pérdida de confidencialidad, integridad, disponibilidad y privacidad de la información de la Unidad.

- La Unidad tiene dispuestos para reportar posibles incidentes o eventos de seguridad y privacidad de la información y seguridad digital, los siguientes canales:

  - ✓ Mensaje con la solicitud al correo electrónico helpdesk@uapa-pae.gov.co
  - ✓ Ingresando al módulo del portal de servicios, iniciando sesión con las correspondientes credenciales, en la opción *"Registrar caso"*, en la dirección https://portaluapa-pae.gov.co/
  - ✓ En la herramienta *"Teams"*, *"helpdesk UApA"*.
  - ✓ Para el caso del ECOSISTEMA, mediante el correo electrónico sipaecontigo@uapa-pae.gov.co

- Durante el periodo objeto de auditoría no se presentaron incidentes o eventos de seguridad y privacidad de la información y seguridad digital, por lo anterior, no se reportó ninguno a través de los canales de comunicación dispuestos para tal fin, así como tampoco se realizaron clasificaciones en la herramienta de gestión de la mesa de ayuda.

- La Unidad tiene su infraestructura tecnológica alojada en la nube pública de Microsoft Azure, por tanto, no se vieron afectados con el ciberataque del 12 de septiembre de 2023 aplicaciones como el Ecosistema SiPAE, Aranda, página web en construcción y el servicio de Office 365 (paquete de ofimática que contiene Word, Excel, PowerPoint, OneDrive, SharePoint, entre otros).

RIESGOS Y EVALUACIÓN DE CONTROLES:

En la Matriz de Riesgos Institucionales se identificó para el proceso *"GTI Gestión de la tecnología e información"*, el siguiente riesgo relacionado con las actividades objeto de auditoría:

"Posibilidad de desvío de recursos físicos o económicos por identificación errónea de las necesidades que dan cumplimiento al objetivo del PROMISE para el favorecimiento propio o de un tercero".

El cual se encuentra clasificado como *"Posibilidad de recibir o solicitar cualquier dádiva o beneficio"*, que puede generar como consecuencia *"Problemas de calidad y seguridad en la información"*, por tanto, se establece como control de tipo detectivo el siguiente:

"El asesor de planeación consolida la información de ejecución presupuestal y de gestión para la operación del PROMISE, de forma semestral, a través de un informe que se presenta a la unidad coordinadora del programa del MEN."

PROCESO	NOMBRE DEL RIESGO	ENFOQUE	CLASIFICACIÓN DEL RIESGO	CAUSAS		CONSECUENCIAS	ANALISIS DEL RIESGO INHERENTE (ANTES DE CONTROLES)			ACTIVIDA	
				INTERNAS	EXTERNAS		PROBABILIDAD	IMPACTO	VALORACIÓN	Descripción del control	Tipo
GTI Gestión de la tecnologia e información	Posibilidad de desvio de recursos fisicos o económicos por identificación errónea de las necesidades que dan cumplimiento al objetivo del PROMISE para el favorecimiento propio o de un tercero	Riesgo de corrupción	Posibilidad de recibir o solicitar cualquier dádiva o beneficio	Desconocimiento de Intereses personales Uso malintencionado Falta de documentac	Cambios en políticas No aplica No aplica No aplica	Pérdida de confianza y cre Toma de decisiones basa Omisión de información rel Problemas de calidad y se	Baja 40%	Catastrófico 100%	Extremo	El subdirector de informa El subdirector de gestión El asesor de planeación El asesor de planeación El asesor de planeación	Preventivo Preventivo Detectivo Detectivo Detectivo

PLANES, PROGRAMAS, PROYECTOS E INDICADORES

De acuerdo con la gestión estratégica de la dependencia auditada, se recomienda verificar la pertinencia de definir y formular dentro del mapa de riesgos institucionales, controles y actividades encaminadas a la identificación, evaluación y gestión de incidentes y eventos de seguridad y privacidad de la información y seguridad digital, para aquellos casos en los que se vea afectada la infraestructura tecnológica de la Unidad Administrativa Especial *"Alimentos para Aprender"* o la de algunos de sus proveedores.

MECANISMOS DE SEGUIMIENTO Y AUTOEVALUACIÓN

En atención a las actividades establecidas dentro del procedimiento de *"Gestión de incidentes de seguridad y privacidad de la información y seguridad digital",* es necesario definir acciones de seguimiento y monitoreo sobre el avance de la solución formulada, que permitan dar conocer en términos de calidad y oportunidad a la alta dirección de la Unidad la información correspondiente.

PARTICIPACIÓN CIUDADANA

El alcance definido en las actividades auditadas por el equipo auditor fue de carácter interno, el presente informe podrá ser publicado en la Página WEB de la UApA, con el fin de garantizar la transparencia y acceso a la información pública de las partes interesadas.

CONCLUSIONES

- Durante el periodo objeto de auditoría no se presentaron incidentes o eventos de seguridad y privacidad de la información y seguridad digital que afectaran la infraestructura tecnológica de la Unidad.

- La Unidad tiene contratado el aplicativo KACTUS HCM para el módulo de nómina a través de los servicios tipo SaaS con el proveedor DIGITALWARE, el cual, tiene alojada su infraestructura tecnológica en IFX Networks.

- IFX Networks sufrió un ataque cibernético de tipo Malware (Ransomware) el día 12 de septiembre de 2023, que afectó de manera indirecta a la Unidad por la indisponibilidad del aplicativo KACTUS HCM para la liquidación de la nómina del mes de septiembre de 2023.

- La Unidad recibió a través de correo electrónico los días 13, 15, 19 y 26 de septiembre de 2023, comunicados de DIGITALWARE sobre el avance y actualización del inconveniente tecnológico y su solución.

- Como plan de contingencia ante la imposibilidad de utilizar el aplicativo KACTUS HCM, la Unidad resolvió liquidar la nómina del mes de septiembre de 2023 de manera manual, con el fin de evitar que la misma se hiciera en forma extemporánea.

- IFX Networks señaló en su informe de fecha 06 de octubre de 2023, que se había comunicado públicamente a sus clientes la restauración de los servicios, así como también, que los sistemas no reportaban novedades en su funcionalidad.

- En el marco de la Resolución No. 6890 del 19 de julio de 2022, IFX reportó el incidente de ciberseguridad el mismo 12 de septiembre de 2023 a los correos malware@colcert.gov.co y contacto@colcert.gov.co, es decir, dentro de las 24 horas hábiles subsecuentes a la detección del incidente, cumpliendo con el deber de reportar al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT). De la misma manera, se notificó a la Fiscalía General de la Nación, Superintendencia de Industria y Comercio y Colombia Compra Eficiente.

- El ataque cibernético tipo malware de cifrado, no tuvo la capacidad de autorreplicación ni de replicarse lateralmente, por tal motivo, no existió riesgo de que se propagara a las redes de los clientes de IFX Networks.

- De acuerdo con las investigaciones de los especialistas de IFX y a lo manifestado por DIGITALWARE, no existió indicación alguna de que la información se hubiera visto comprometida, ni de violación de los códigos de seguridad, ni de pérdida, robo y/o acceso no autorizado de información de las bases de datos.

RECOMENDACIONES:

- Establecer un plan de contingencia para aquellos eventos en que no sea posible la liquidación de la nómina a través de KACTUS HCM, toda vez que, al hacerlo manualmente se aumenta el riesgo de imprecisiones en la información y por ende errores en la liquidación. Por otro lado, al hacerlo a través del KACTUS temporal, implica la posterior migración de la información e incurrir en un mayor tiempo para la validación de los datos, lo cual, puede derivar en la liquidación extemporánea de la nómina.

INFORME DETALLADO			
Resultado		**Descripción**	**Recomendación**
HZ	**OM**		
N/A	**N/A**	N/A	N/A

AUDITORÍA DE CALIDAD / AMBIENTAL Y OTROS MODELOS REFERENCIALES			
Resultado		**Requisito o numeral**	**Descripción**
NC	**OB**		
N/A	**N/A**	N/A	N/A

LÍDER DEL EQUIPO AUDITOR: CARLOS LEONARDO ORTEGÓN BARINAS.
CONTROL INTERNO DE GESTIÓN