No. DE INFORME:	49
FECHA DE INFORME:	18 de Noviembre de 2022
PROCESO Y/O DEPENDENCIA:	Oficina de Planeación e Innovación Institucional
LÍDER DEL PROCESO Y/O DEPENDENCIA:	Administrador de Empresas JAIME RAFAEL MORON BARROS
TEMA DE SEGUIMIENTO:	Verificación del cumplimiento de las políticas y estándares de seguridad – MSPI - 2022

NORMATIVIDAD:

Manual Políticas de Seguridad de la información Código GTI-MA-01, Versión 03
Directiva Permanente No 07 ASDLG-ALOTIC – 130, del 12 de julio de 2021

JUSTIFICACIÓN DEL SEGUIMIENTO:

En seguimiento y evaluación por parte de la Oficina Control Interno, al "Plan de Continuidad al Instrumento de identificación de la línea de base de seguridad para la madurez del MSPI Vigencia 2022", se presenta este informe con una revisión de las novedades relacionadas con el aseguramiento de las políticas, los procedimientos y estándares de seguridad, de acuerdo con las novedades encontradas en las auditorías realizadas a las regionales de la agencia durante la vigencia 2022, y se realizan recomendaciones y observaciones generales acerca del cumplimiento de las políticas y normas de seguridad establecidas, con base en el Manual Políticas de Seguridad de la información Código GTI-MA-01, Versión 03.

GESTIÓN / ACCIONES DEL SEGUIMIENTO:

SEGURIDAD DE LOS RECURSOS

9. SEGURIDAD DE LOS RECURSOS HUMANOS

9.2. DURANTE LA EJECUCIÓN DEL EMPLEO

9.2.3. Proceso Disciplinario

Actuaciones que conllevan a la violación de la seguridad de la información establecida en la ALFM:

L. Recibir o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la institución.

Observaciones:

De acuerdo con la revisión realizada, en la auditoria a la Regional Tolima Grande del 21 al 23 de septiembre de 2022, se evidenció el uso de un correo de Gmail como correo institucional en el comedor BITER 9, ubicado en La Plata Huila, evidenciando incumplimiento de la política de seguridad, en cuanto tener aplicaciones no instaladas y configuradas por la entidad.

9.2. DURANTE LA EJECUCIÓN DEL EMPLEO

9.2.3. Proceso Disciplinario

Actuaciones que conllevan a la violación de la seguridad de la información establecida en la ALFM:

M. Utilizar equipos electrónicos o tecnológicos desatendidos o que, a través de sistemas de interconexión inalámbrica, sirvan para transmitir, recibir y almacenar datos.

Observaciones:

De acuerdo con la revisión realizada en la auditoria a la Regional Tolima Grande, del 21 al 23 de septiembre de 2022, se evidenció el uso de un computador de propiedad de un tercero por parte del señor administrador, del comedor BIPIG, incumpliendo la política seguridad, en cuanto a utilizar equipos electrónicos o tecnológicos desatendidos.

GESTIÓN DE ACTIVOS Y MEDIOS

10. GESTIÓN DE ACTIVOS

10.1. RESPONSABILIDAD POR LOS ACTIVOS

Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.

10.1.1. Inventario de activos

Se deben identificar los activos de información, sus respectivos propietarios, custodios y su ubicación, a fin de elaborar y mantener un inventario actualizado mínimo cada año, de acuerdo a la Guía para la gestión y clasificación de activos de información - GTI-GU-02, mediante formato Registro de Activos de Información alineado con la Ley 1712 de 2014 Ley de Transparencia.

Cada proceso de la ALFM debe ser responsable de mantener actualizado el inventario de activos de información con el acompañamiento de la Oficina TIC, de acuerdo con las directrices establecidas para la gestión de activos.

Observaciones:

De acuerdo con la revisión realizada, en la fecha de este informe 10-11-2022, se evidencia en la página Web el registro de activos de información, actualizada al 29-06-2022, cumpliendo con lo establecido en el Numeral 10. Gestión de activos 10.1. RESPONSABILIDAD POR LOS ACTIVOS, 10.1.1. Inventario de activos.

10.3.1. Gestión de medios removibles

Se encuentra restringida la conexión a la infraestructura tecnológica (servidores, computadores, scanner y demás equipos de tecnologías de la información) de la ALFM, de cualquier almacenamiento como dispositivos personales USB, discos duros externos, CD's, DVD's, cámaras fotográficas, cámaras de video, teléfonos celulares, smartphone, tabletas, módems, memorias SD o de almacenamiento, entre otros dispositivos no institucionales. Las excepciones especiales serán autorizadas por la Oficina TIC previo diligenciamiento del Formato Solicitud de Excepciones de Seguridad Informática - GTI-FO-05.

Los medios de almacenamiento removibles como cintas, discos duros, CD's, DVD's, dispositivos USB, entre otros, así como los medios impresos que contengan información institucional, deben ser controlados y físicamente protegidos mediante algún mecanismo (cifrado, resguardo en gavetas de seguridad, cajas fuertes, control de accesos, etc.), que garantice su integridad y confidencialidad.

Observaciones:

En la recepción de información a través de medios magnéticos, como CD´s, no se ha evidenciado la protección de los mismos a través de mecanismos como cifrado, resguardos o controles de acceso.

10.3. MANEJO DE MEDIOS

10.3.2. Disposición de los medios

La información contenida en la generación de Backup debe estar protegida en un lugar seguro y bajo llave, de acuerdo a disposición de la Oficina TIC.
Se debe guardar varias copias de datos valiosos para la ALFM en medios separados, con el fin de evitar la pérdida de información por daño o robo de los medios removibles.
Las copias de Backups se deben guardar en una ubicación alterna a la localización de los datos o aplicaciones, para aumentar la seguridad ante posibles impactos de desastres naturales, accidentes, incendios, entre otros.

Observaciones:

En la oficina de Control Interno no se tiene copia de seguridad realizada por la Oficina de TIC de la información de la Contraloría General de la República, realizada por la oficina de TIC, en cumplimiento del numeral 10.3. MANEJO DE MEDIOS, 10.3.2. Disposición de los medios.

SEGURIDAD FÍSICA Y DEL ENTORNO

13. SEGURIDAD FÍSICA Y DEL ENTORNO

13.1. ÁREAS SEGURAS

13.1.2. Controles físicos de entrada

Se debe exigir a todo el personal, sin excepción, el porte en un lugar visible del mecanismo de identificación adoptado para ello por cada una de las oficinas, mientras permanezcan dentro de las instalaciones de la ALFM.

Observaciones:

No se evidencia la exigencia en el ingreso, y durante la jornada, del porte en lugar visible del carnet de identificación, según lo exigido en el Manual Políticas de Seguridad de la información.

13.2.2. Servicios de suministro

La ALFM cuenta con aire acondicionado, UPS (sistema de alimentación ininterrumpida, en inglés (Uninterruptible Power Supply). que asegura el tiempo necesario de autonomía para que la planta eléctrica entre a soportar la carga o mientras regresa la energía eléctrica, ante una falla en el suministro de energía, un enlace de red redundante y un sistema de monitoreo de las condiciones (temperatura, humedad, voltaje, apertura y cierre de puertas) del DATACENTER.

Observaciones:

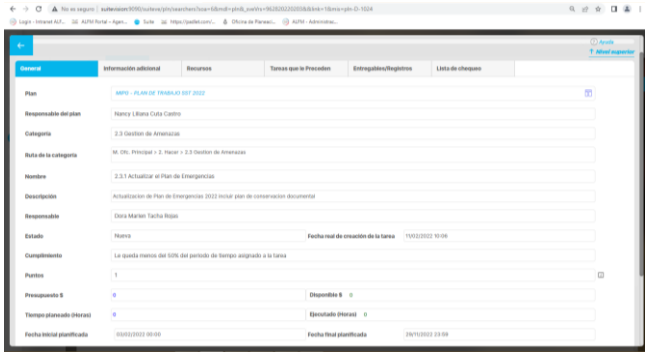
Aunque en la Oficina Principal, se evidencia el sistema de soporte de la carga eléctrica de los equipos, mientras se restablece el fluido de la energía eléctrica, en caso de cortes de la misma; no se evidenció en el comedor BIMEJ de la Regional Amazonia en la auditoria, en sito del 17 de septiembre de 2022, la existencia de una UPS y/o regulador de voltaje, que asegure la protección del equipo.

13.1.5. Trabajo en áreas seguras

La ALFM debe contar con un plan de emergencias definido por la Dirección Administrativa y de Talento Humano., el cual debe estar basado en la Guía para el diseño del plan de emergencias - GTH-GU-11, que debe ser probado anualmente, con el fin de brindar protección contra amenazas externas.

Observaciones:

No se revisó el Plan de Emergencia 2022, ya que el mismo se encuentra en actualización, con fecha final planificada del 29-11-2022.



Fuente: : http://suitevision:9090/suiteve/pln/searchers?soa=6&mdl=pln&_sveVrs=962820220203&&link=1&mis=pln-D-1024

13.2.8. Equipos de usuarios desatendidos

En horas no hábiles, o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deberán dejar los medios que contengan información crítica protegida bajo llave.
Los usuarios deberán bloquear su estación cada vez que se ausenten de su puesto de trabajo y sólo se podrá desbloquear con la contraseña del mismo usuario que la bloqueó.

Observaciones:

No se evidencia, el bloqueo de las estaciones de trabajo por parte de los funcionarios cada vez que se ausenta de su puesto de trabajo, en cumplimiento del Manual de Políticas de Seguridad de la Información, en el *numeral 13.2.8. Equipos de usuarios desatendidos: los usuarios deberán bloquear su estación cada vez que se ausenten de su puesto de trabajo y sólo se podrá desbloquear con la contraseña del mismo usuario que la bloqueó.*

13.2.9. Política de escritorio y pantalla limpios

Al finalizar la jornada laboral el funcionario o tercero debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno, además debe cerrar sesión en los aplicativos que utiliza y debe apagar el equipo de cómputo asignado.

Observaciones:

No se evidencia, mediante observación aleatoria, que al finalizar la jornada de trabajo los documentos que contienen información confidencial o de uso interno, se guarden en lugar seguro.

SEGURIDAD DE LAS OPERACIONES

14. SEGURIDAD DE LAS OPERACIONES

14.7.1. Controles sobre auditorias de sistemas de información

La ALFM apoyada en la Oficina de Control Interno y la Oficina Asesora de Planeación y Gestión Institucional, a través del Procedimiento Gestión de Seguimiento y Evaluación – Auditorías Internas - GSE-PR-02 verificará el cumplimiento de los requisitos de la normatividad legal vigente, los requisitos internos del proceso y procedimientos. Estás deberán ser acordadas y planificadas para reducir al mínimo las interrupciones en los procesos.
Se deben establecer a través de la Oficina de Control Interno y la Oficina Asesora de Planeación y Gestión Institucional, controles que permitan realizar auditorías, supervisión de las actividades por los técnicos responsables de la infraestructura de red y sus sistemas de información.
El alcance de las pruebas técnicas de auditoría se debe acordar y controlar, las pruebas de auditoría que puedan afectar la disponibilidad del sistema se deben realizar fuera de horas laborales.

Observaciones:

No hay claridad en los roles de control de la segunda y tercera líneas de defensa que aseguren el cumplimiento de la normatividad legal vigente, los requisitos internos del proceso y procedimientos.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS, Y PROTECCIÓN DE TRANSACCIONES

16. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

16.1.2. Seguridad de servicios de las aplicaciones en redes públicas

La información pública producida por la ALFM, deberá estar resguardada de posibles modificaciones que afecten la imagen institucional, de acuerdo con los parámetros y normatividad vigente.
El portal institucional deberá contener la política de privacidad y uso, de acuerdo a la normatividad vigente.
La ALFM deberá garantizar el derecho de Habeas Data y la Ley de transparencia al público que hace uso de los servicios de sus respectivos portales institucionales y propender por la seguridad de la información ingresada a través de ellos, aclarando que la veracidad de la misma es responsabilidad del ciudadano.
Toda la información, publicada en el portal institucional por parte de los funcionarios autorizados debe contar con la revisión y aprobación de los Directores, Subdirectores o Jefes de Oficina, quienes serán responsables por la información publicada por los editores web de su dependencia.
La información de los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas y modificación no autorizadas.

Observaciones:

Se evidencia la publicación de la Política de Privacidad y uso en la página WEB https://www.agencialogistica.gov.co/transparencia-y-acceso-a-la-informacion-publica/1-informacion-de-la-

entidad/1-2-estructura-organica-organigrama-2/1-5-politicas-de-seguridad-de-la-informacion-y-proteccion-de-datos-personales/

Se evidencia la publicación la política de tratamiento de datos personales, relacionada con el derecho de Habeas Data y Ley de transparencia en la siguientes direcciones de la página WEB https://www.agencialogistica.gov.co/transparencia-y-acceso-a-la-informacion-publica/1-informacion-de-la-entidad/1-2-estructura-organica-organigrama-2/1-5-politicas-de-seguridad-de-la-informacion-y-proteccion-de-datos-personales/ y https://www.agencialogistica.gov.co/transparencia-y-acceso-a-la-informacion-publica/

Se evidencia el control de las publicaciones que se hacen mediante la página WEB, a través de la mediación de la oficina de TIC en las solicitudes de los WEB Master. Se evidencia la optimización de acceso a la información pública con la corrección de enlaces rotos, y el enlace de la información pública que se encuentra a través del menú de Transparencia y Acceso a la Información y el que se muestra en el panel de búsqueda (Buscar en sede electrónica).

16.1.3. Protección de transacciones de los servicios de las aplicaciones

La Oficina TIC, debe incluir las consideraciones de seguridad de la información para las transacciones de los servicios de las aplicaciones, entre otras:
El uso de firmas electrónicas por parte de cada una de las partes involucradas en la transacción.

Observaciones:

Se evidencia el uso de firma electrónica en la mayoría de los documentos generados internamente por la ALFM.

GESTIÓN DE INCIDENTES

18. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

18.1. GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN

18.1.1. Responsabilidades y procedimientos

La priorización del tratamiento de los incidentes se realiza conforme a la criticidad de la información.
Se debe establecer y mantener actualizado un directorio de los encargados de la Gestión de Incidentes de Seguridad de la entidad, el cual será consolidado por la Oficina TIC.
La Oficina TIC deberá difundir el directorio consolidado de los encargados de gestionar los incidentes de seguridad de la ALFM.

Observaciones:

No se evidencia el directorio del personal encargado de la Gestión de los Incidentes de Seguridad, y la difusión de dicho directorio.

SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DEL NEGOCIO

19. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

19.1. CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

19.1.1. Planificación de la continuidad de la seguridad de la información

La seguridad de la información es una prioridad y se incluye como parte de la gestión general de la continuidad y del compromiso de la Alta Dirección.
La ALFM deberá contar con un Plan de Continuidad que asegure la operación de los procesos críticos ante la ocurrencia de eventos no previstos o desastres naturales como sismos, terremotos, tsunami, etc.

Para la ALFM, su activo más importante es el recurso humano y por lo tanto será su prioridad y objetivo principal, establecer las estrategias para mantenerlo.

Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades, estarán incorporados y definidos en el Plan de Continuidad del negocio de la ALFM.

Los responsables de los procesos serán los encargados de mantenerlos documentados y actualizados.

Observaciones:

No se evidencia en SVE, ni en la página WEB el Plan de Continuidad de la ALFM. Por solicitud verbal de la Oficina de Control Interno, a la Oficina de TIC, se recibió el Plan de Continuidad de la Oficina de Tecnología de la Información y Comunicaciones – 2021, más el mismo no está publicado.

OBSERVACIONES Y/O SUGERENCIAS:

SUGERENCIAS

- Se recomienda a los Directores, Subdirectores y Jefes de Oficina asegurar que los funcionarios y contratistas estén sensibilizados en los temas de seguridad de la información, en cumplimiento del numeral 9.2. *DURANTE LA EJECUCIÓN DEL EMPLEO, 9.2.1. Responsabilidades de la Dirección: Los Directores, Subdirectores y Jefes de Oficina, velarán por que los funcionarios y contratistas participen de manera activa en las sensibilizaciones dadas por la Oficina TIC con relación a temas de seguridad de la información.*

- Se recomienda a la Dirección Administrativa y talento Humano, la comunicación a la oficina TIC de los cambios de cargo de personal, para asegurar el cumplimiento del numeral 9.2. *DURANTE LA EJECUCIÓN DEL EMPLEO, 9.2.1. Responsabilidades de la Dirección: La Dirección Administrativa y talento Humano deben comunicar a la Oficina TIC, los cambios de cargo de personal, indicando los cambios en los recursos tecnológicos asignados; especialmente actualizaciones sobre accesos a carpetas compartidas y sistemas de información.* Así como también la comunicación de la desvinculación administrativa, temporal o permanente, laboral o contractual de los funcionarios o contratistas en cumplimiento del numeral 9.3.1. *Terminación o cambio de responsabilidades de empleo: la Dirección Administrativa - talento Humano y la Subdirección General de Contratación o a quienes se deleguen deberán informar a la Oficina TIC, mediante caso generado en la plataforma de mesa de ayuda o vía correo electrónico, la desvinculación administrativa, laboral o contractual del funcionario o contratista…*

- Se recomienda a la Dirección Administrativa y talento Humano incluir en los programas de inducción y reinducción, los temas de seguridad de la información, en cumplimiento del Manual Políticas de Seguridad de la información Código GTI-MA-01, Versión 03, *numeral 9.2.2. Toma de conciencia, educación y formación en la seguridad de la información: Incluir en los programas de Inducción y de reinducción el tema seguridad de la información asegurando que los funcionarios conozcan sus responsabilidades, así como las implicaciones por el uso indebido de activos de información y recursos informáticos, haciendo énfasis en las consecuencias jurídicas que puede acarrear como servidor público.*

- Se recomienda a cada proceso de la entidad, que con acompañamiento de la Oficina de TIC se actualice periódicamente el inventario de activos de información para asegurar el cumplimiento del Manual Políticas de Seguridad de la información en el Numeral 10. Gestión de activos 10.1. RESPONSABILIDAD POR LOS ACTIVOS, 10.1.1. Inventario de activos.

- Se recomienda a la oficina de TIC, impartir capacitación en medios de cifrado o protección de la información para medios de almacenamiento para garantizar su integridad y confidencialidad, en cumplimiento del Manual Políticas de Seguridad de la información Código GTI-MA-01, Versión 03, Numeral *10.3.1. Gestión de medios removibles: Se encuentra restringida la conexión a la infraestructura tecnológica (servidores, computadores, scanner y demás equipos de tecnologías de la información) de la ALFM de cualquier almacenamiento como dispositivos personales USB, discos duros externos, CD's, DVDs, cámaras fotográficas, cámaras de video, teléfonos celulares, smartphone, tabletas, módems, memorias SD o de almacenamiento, entre otros dispositivos no institucionales. Las excepciones especiales serán autorizadas por la Oficina TIC previo diligenciamiento del Formato Solicitud de Excepciones de Seguridad Informática - GTI-FO-05. Los medios de almacenamiento removibles como cintas, discos duros, CDs, DVDs, dispositivos USB, entre otros, así como los medios impresos que contengan información institucional, deben ser controlados y físicamente protegidos mediante algún mecanismo (cifrado, resguardo en gavetas de seguridad, cajas fuertes, control de accesos, etc.), que garantice su integridad y confidencialidad.*

- Se recomienda, asegurar por parte de la Oficina de TIC las copias de seguridad de la información en cumplimiento del Manual Políticas de Seguridad de la información en el numeral 10.3. MANEJO DE MEDIOS, 10.3.2. Disposición de los medios.

- Se recomienda a la Oficina de TIC el aseguramiento de los filtros y restricciones de acceso a páginas y contenidos, teniendo en cuenta los perfiles definidos en el Manual Políticas de Seguridad de la información, numeral 11. CONTROL DE ACCESO. 11.1. REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO, 11.1.2. Acceso a redes y a servicios en red perfiles de navegación: Perfiles de Navegación: A. Perfil de navegación Bajo, B. Perfil de navegación Medio, C. Perfil de navegación Alto y D. Perfil de navegación Tecnología.

- Se recomienda a la Dirección Administrativa socializar al equipo de seguridad de la Agencia, y a los funcionarios de la misma, la exigencia del porte del carnet de identificación en cumplimiento del Manual Políticas de Seguridad de la información, numeral *13. SEGURIDAD FÍSICA Y DEL ENTORNO, 13.1. ÁREAS SEGURAS, 13.1.2. Controles físicos de entrada: Se debe exigir a todo el personal, sin excepción, el porte en un lugar visible del mecanismo de identificación adoptado para ello por cada una de las oficinas, mientras permanezcan dentro de las instalaciones de la ALFM.*

- Se recomienda socializar, nuevamente, a los funcionarios la exigencia de guardar de forma segura los documentos que contiene información confidencial o de uso interno, en cumplimiento del Manual Políticas de Seguridad de la Información, *numeral 13.2.9. Política de escritorio y pantalla limpios: Al finalizar la jornada laboral el funcionario o tercero debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno, además debe cerrar sesión en los aplicativos que utiliza y debe apagar el equipo de cómputo asignado.*

- Se recomienda aclarar y definir los roles de control de la segunda y tercera línea de defensa que aseguren el cumplimiento de la normatividad legal vigente, los requisitos internos del proceso y procedimientos, en cumplimiento del Manual Políticas de Seguridad de la Información, *numeral 14. SEGURIDAD DE LAS OPERACIONES, 14.7.1. Controles sobre auditorias de sistemas de información.*

- Se recomienda ampliar la documentación que requiere el uso, exclusivo de firma electrónica, en cumplimiento del Manual de Políticas de Seguridad, *numerales 15.2. TRANSFERENCIA DE INFORMACIÓN, 15.2.1. Políticas y procedimientos de transferencia de información:*
  Para el trámite de las comunicaciones internas, se debe tener en cuenta lo siguiente:
  A. Se utilizará la firma electrónica en PDF, evitando imprimir innecesariamente estos documentos al ser viables el trámite de forma digital y dando cumplimiento a la Directiva Permanente de Cero Papel; y el numeral16.1.3. Protección de transacciones de los servicios de las aplicaciones: La Oficina TIC, debe incluir las consideraciones de seguridad de la información para las transacciones de los servicios de las aplicaciones, entre otras:
  El uso de firmas electrónicas por parte de cada una de las partes involucradas en la transacción.

- Se recomienda la publicación y la difusión de los encargados de la Gestión de los Incidentes de Seguridad en la entidad, en cumplimiento del Manual de Políticas de Seguridad, *numeral 18.1. GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN, 18.1.1. Responsabilidades y procedimientos: La priorización del tratamiento de los incidentes se realiza conforme a la criticidad de la información.*
  Se debe establecer y mantener actualizado un directorio de los encargados de la Gestión de Incidentes de Seguridad de la entidad, el cual será consolidado por la Oficina TIC.
  La Oficina TIC deberá difundir el directorio consolidado de los encargados de gestionar los incidentes de seguridad de la ALFM.

OBSERVACIONES:

- En relación con el Plan de Emergencias 2022, definido por la Dirección Administrativa y de Talento Humano, este tiene como fecha final planificada en la Suite Visión Empresarial el 29-11-2022. Teniendo en cuenta lo anterior, se realiza la observación de generar el Plan de Emergencias, al principio del año, para su aplicación durante el mismo, o generarlo al final del año con fecha del siguiente año y aplicación durante el mismo.

- No se observa el cumplimiento del Manual Políticas de Seguridad de la Información, *numeral 13.2.8. Equipos de usuarios desatendidos: los usuarios deberán bloquear su estación cada vez que se ausenten de su puesto de trabajo y sólo se podrá desbloquear con la contraseña del mismo usuario que la bloqueó.*

HALLAZGO:

No.	Descripción	Requisito Incumplido	Proceso
1.	**Plan de Continuidad de Negocio de la ALFM** No se evidencia la publicación del Plan de Continuidad de Negocio de la ALFM, según lo establecido en el Manual Políticas Seguridad de la Información.	***Manual Políticas Seguridad de la Información.*** *19. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO* *19.1. CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN* *Objetivo: La continuidad de seguridad de la información se deberá incluir en los sistemas de gestión de continuidad del negocio de la ALFM.* *19.1.1. Planificación de la continuidad de la seguridad de la información* *La seguridad de la información es una prioridad y se incluye como parte de la gestión general de la continuidad y del compromiso de la Alta Dirección.* *La ALFM deberá contar con un Plan de Continuidad que asegure la operación de los procesos críticos ante la ocurrencia de eventos no previstos o desastres naturales como sismos, terremotos, tsunami, etc.* *Para la ALFM su activo más importante es el recurso humano y por lo tanto será su prioridad y objetivo principal, establecer las estrategias para mantenerlo.* *Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades, estarán incorporados y definidos en el Plan de Continuidad del* *Negocio de la ALFM.*	**Oficina Asesora de Planeación e Innovación Institucional -** **Oficina TIC** **Oficina Principal**

		Los responsables de los procesos serán los encargados de mantenerlos documentados y actualizados.	

SOPORTES DE LA REVISIÓN:

Herramienta Suite Visión Empresarial
Correos Electrónicos con reportes de novedades TICS
Auditorías Internas OCI

Alejandro Murillo Devia

Firmado digitalmente por Alejandro Murillo Devia
Fecha: 2022.11.18 11:01:25 -05'00'

Aprobó: Contador Público Alejandro Murillo Devia
Cargo: Jefe Oficina de Control Interno

Neil Aldrin Devia Acosta

Firmado digitalmente por Neil Aldrin Devia Acosta
Nombre de reconocimiento (DN): cn=Neil Aldrin Devia Acosta, o=Agencia Logistica de las Fuerzas Militares, ou=Control Interno, email=neil.devia@agencialogistica.gov.co, c=CO
Fecha: 2022.11.18 08:32:55 -05'00'

Elaboró: Adm. Emp. Neil Aldrin Devia Acosta
Cargo: Profesional de Defensa – Oficina de Control Interno

Oscar Alfredo Martínez Rodríguez

Firmado digitalmente por Oscar Alfredo Martínez Rodríguez
Fecha: 2022.11.18 10:54:29 -05'00'

Revisó: Ing. Mec. Oscar Alfredo Martinez Rodriguez
Cargo: Profesional de Defensa – Oficina de Control Interno