INFORME TÉCNICO DE LA MADUREZ DEL SGSI

Área de Gestión de Seguridad Informática – GESU

Unidad Informática – UNIN

Subdirección Administrativa

HOSPITAL MILITAR CENTRAL - HOMIL

PRESENTACIÓN

El presente informe busca mostrar la evaluación del sistema de gestión de seguridad de la información - SGSI para los procesos del Hospital Militar Central - HOMIL, de manera que se tenga claridad acerca de la protección y mantenimiento que se tiene y debería tener sobre los activos de información.

TABLA DE CONTENIDO

OBJETIVO

Este informe tiene como objetivo principal diagnosticar el nivel de madurez del SGSI, presentando las evidencias necesarias en cuanto a los procesos y sus procedimientos en la ejecución de las diferentes actividades misionales, y el cumplimiento de estas labores respecto a la ***Norma ISO/IEC 27001:2013***.

ALCANCE

El alcance del informe es brindar las recomendaciones para que la Unidad de Informática - UNIN pueda generar las respectivas políticas, directrices y/o procedimientos que puedan mitigar las vulnerabilidades tanto administrativas como Técnicas que se presentan en los activos del Hospital Militar.

INFORME

Después de realizar las 2 primeras fases del plan de trabajo que le fue presentado las cuales consistían en:

FASE 1 - Levantamiento de información

Fase en la cual se obtuvieron los siguientes datos:

a. Organigrama del HOMIL
b. Mapas de Procesos
c. Política de Seguridad de la información
d. Roles y Responsabilidades (Incluido en la Política de Seguridad de la información – ítem 7. MISIONES PARTICULARES)
e. Procedimientos de algunos Procesos (Unidad de Informática, Talento Humano, Activos)

FASE 2 - Diagnóstico

Fase en la cual se determinó el estado actual de la gestión de seguridad y privacidad de la información al interior del HOMIL, dicha verificación se realizó con el instrumento de evaluación MSPI emitido por el MINTIC.

Esta verificación permitió identificar el nivel de madurez del SGSI.

Además, se pudo identificar las vulnerabilidades técnicas y administrativas que sirven como insumo para realizar la fase siguiente que es de planificación.

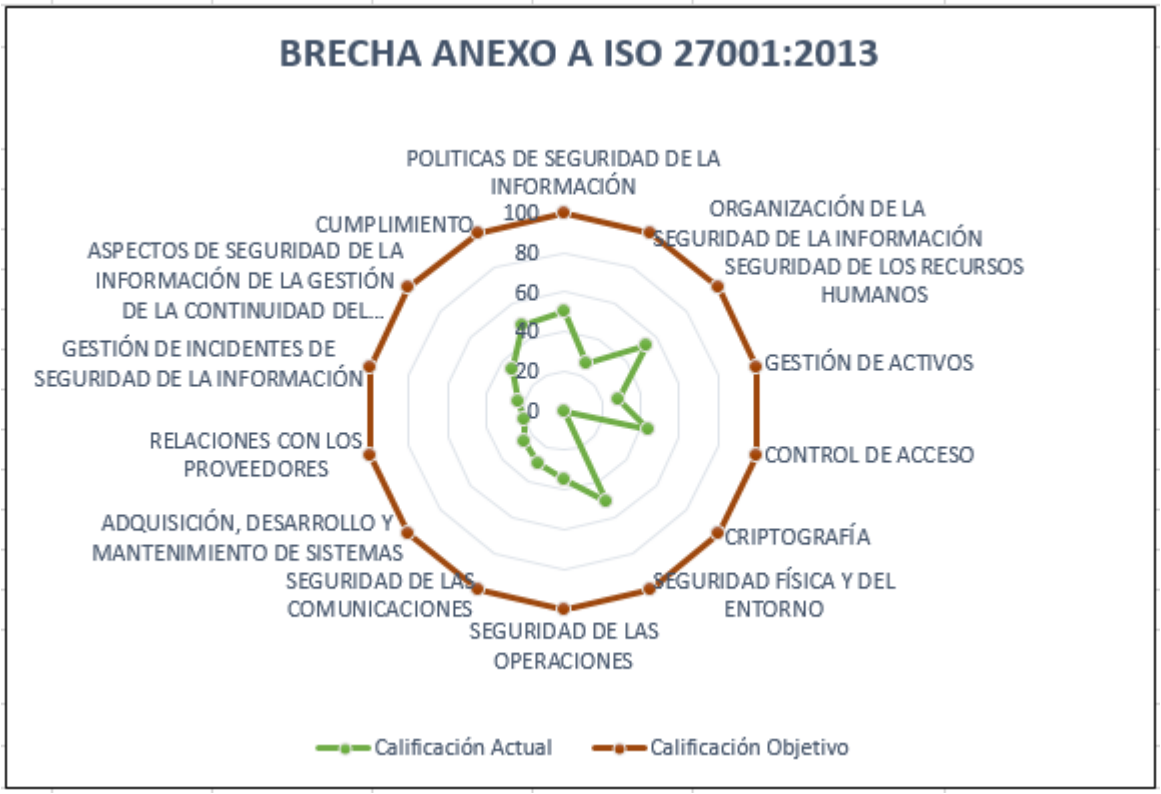
1. NIVEL DE MADUREZ

Se presenta a continuación el cuadro resumen de la Evaluación de efectividad de los controles de la ***Norma ISO/IEC 27001:2013***

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	50	100	EFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	27	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	53	100	EFECTIVO
A.8	GESTIÓN DE ACTIVOS	28	100	REPETIBLE
A.9	CONTROL DE ACCESO	44	100	EFECTIVO
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	51	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	35	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	30	100	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	25	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	20	100	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	23	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	34	100	REPETIBLE
A.18	CUMPLIMIENTO	47,5	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		33	100	REPETIBLE

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

En cuanto a la brecha que presenta el HOMIL con respecto al Anexo de la ***Norma ISO /IEC 27001:2013*** se puede ver en la siguiente gráfica, donde se evidencia el rezago en cuanto al calificativo objetivo que presenta la norma.



A continuación, se presenta el informe detallado de las vulnerabilidades técnicas y administrativas identificadas.

2. VULNERABILIDADES IDENTIFICADAS

A.5 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

A.5.1.1 Políticas de seguridad de la Información

Nivel de Cumplimiento **60 /100**

Evidencia**:**

La Política de SGSI se puede consultar en la intranet (Politica.pdf (homil.gov.co)) y la página web del Hospital Militar (Inicio - Hospital Militar Central) -> modulo Mi portal-> modulo Transparencia Institucional-> 6. Planeación -> 6.1. Políticas, lineamientos y manuales-> 6.1.1. Políticas y lineamientos sectoriales e institucionales-> Política de Seguridad de la Información (PDF).

Recomendación:

Validar en la política de seguridad de la información:

a) Que esté definido que es seguridad de la información.
b) La asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos;
c) Los procesos para manejar las desviaciones y las excepciones.
Indague sobre los responsables designados formalmente por la dirección para desarrollar, actualizar y revisar las políticas.
Verifique cada cuanto o bajo qué circunstancias se revisan y actualizan, verifique la última fecha de emisión de la política frente a la fecha actual y que cambios a sufrido, por lo menos debe haber una revisión anual.

A.5.1.2 Revisión de las políticas de seguridad de la Información

Nivel de Cumplimiento **40 /100**

Evidencia:

La Política de SGSI se puede consultar en la intranet (Politica.pdf (homil.gov.co)) y la página web del Hospital Militar (Inicio - Hospital Militar Central) -> modulo Mi portal-> modulo Transparencia Institucional-> 6. Planeación -> 6.1. Políticas, lineamientos y manuales-> 6.1.1. Políticas y lineamientos sectoriales e institucionales-> Política de Seguridad de la Información (PDF).

Se evidencia que, en la Política de Seguridad de la información, en cada uno de sus ítems hacen referencia a los controles de la Norma ISO/IEC 27001:2005. (A la fecha la Norma vigente en Colombia es la ISO/IEC 27001:2013 (11/12/2013)).

Recomendación:

Realizar la revisión y/o actualización de la política de seguridad de la información vigente, en periodos anuales.

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

A.6.1.1 Roles y responsabilidades para la seguridad de la información

Nivel de Cumplimiento **40 /100**

Evidencia**:**

Se evidencia que están definidos en la Política de Seguridad de la Información Ítem 7. MISIONES PARTICULARES, los Roles y Responsabilidades
Acto Administrativo: NO hay
1) Se evidencia que el SGSI tiene el suficiente apoyo de la alta dirección, porque se ve reflejado en comités donde se discutan temas como la política de SI, los riesgos o incidentes.
2) Se evidencia que están n claramente definidos los roles y responsabilidades y asignados a personal con las competencias requeridas.
3) Están identificadas los responsables y responsabilidades para la protección de los activos? (Una práctica común es nombrar un propietario para cada activo, quien entonces se convierte en el responsable de su protección)
4)Si están definidas las responsabilidades para la gestión del riesgo de SI y la aceptación de los riesgos residuales. Se ve reflejado en el Mapa de Riesgos Institucionales PL-0APL-PO-FT-02
5) No están definidos y documentados los niveles de autorización.
6) Si se cuenta con un presupuesto formalmente asignado a las actividades del SGSI (por ejemplo, campañas de sensibilización en seguridad de la información.

Recomendación:

Verificar en la política lo siguiente:

1) los roles y responsabilidades frente a la ciberseguridad han sido establecidos.

2) los roles y responsabilidades de seguridad de la información han sido coordinados y alineados con los roles internos y las terceras partes externas.

3) Los a) proveedores, b) clientes, c) socios, d) funcionarios, e) usuarios privilegiados, f) directores y gerentes (mandos senior), g) personal de seguridad física, h) personal de seguridad de la información entienden sus roles y responsabilidades, i) Están claros los roles y responsabilidades para la detección de incidentes.

Solicite el acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o e que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección.

Revise la estructura del SGSI:

5)Definir y documentar los niveles de autorización

6) Ejecutar el presupuesto formalmente asignado a las actividades del SGSI (por ejemplo, en campañas de sensibilización en seguridad de la información).

A.6.1.2 Separación de deberes

Nivel de Cumplimiento **40 /100**

Evidencia:

Hay controles LDAP para los usuarios.
También hay actas de entrega de los activos en los cuales los usuarios se hacen responsables del activo asignado.

Recomendación:

Se deben considerar controles compensatorios como revisión periódica de, los rastros de auditoría y la supervisión de cargos superiores.

A.6.1.3 Contacto con las autoridades

Nivel de Cumplimiento **20 /100**

Evidencia:

Se tiene contacto, pero no está documentado

Recomendación:

Crear los procedimientos establecidos que especifiquen cuándo y a través de que autoridades se debería contactar a las autoridades.

A.6.1.4 Contacto con grupos de interés especiales

Nivel de Cumplimiento **60 /100**

Evidencia:

Se tiene membresía con el COLCERT y el CSIRT

Recomendación:

Crear un archivo con las membresías en grupos o foros de interés especial en seguridad de la información en los que se encuentran inscritos las personas responsables de la Seguridad Información.

A.6.1.5 Seguridad de la información en la gestión de proyectos

Nivel de Cumplimiento **40 /100**

Evidencia:

a) Los objetivos de la seguridad de la información si se incluyen en los objetivos de los proyectos, Están incluidos dentro de: ECO Dinámica 2021, DOCX- Estudio previo de contratación Dinámica.

b) La valoración de los riesgos de seguridad de la información si se lleve a cabo en una etapa temprana del proyecto, para identificar los controles necesarios, Exactamente en el estudio previo de los proyectos (pendiente entrega del documento)

c)La seguridad de la información NO es parte de todas las fases de la metodología del proyecto aplicada.

Recomendación:

Asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de un proyecto. Esto se aplica generalmente a cualquier proyecto, independientemente de su naturaleza, por ejemplo, un proyecto para un proceso del negocio principal, TI, gestión de instalaciones y otros procesos de soporte.

A.6.2.1 Política para dispositivos móviles

Nivel de Cumplimiento **20 /100**

Evidencia:

Dentro de la política de Seguridad de la información, se referencia en los ítems:

13.USO ADECUADO DE LOS ACTIVOS DE INFORMACION

19 SEGURIDAD Y MANTENIMIENTO DE LOS EQUIPO

30 COMPUTACION MOVIL

Todo lo relacionado con Dispositivos Móviles.

Recomendación:

Adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.

A.6.2.2 Teletrabajo

Nivel de Cumplimiento **0 /100**

Evidencia:

No existe política

Recomendación:

Implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.

A.7 SEGURIDAD DE LOS RECURSOS HUMANOS

A.7.1 Antes de asumir el empleo

A.7.1.1 Selección

Nivel de Cumplimiento **60 /100**

Evidencia:

PROCEDIMIENTO: SELECCIÓN DE CONTRATISTAS POR PRESTACIÓN DE SERVICIOS GH-SECO-PR-3
FT- Lista de chequeo documentación requerida para vinculación GH-SECO-PR-01-FT-01
PR – CONTRATACIÓN POR PRESTACIÓN DE SERVICIOS CON PERSONAS NATURALES Cód. GH-SECO-PR-01.
GH-ADP-PR-1 Empleados de planta

Recomendación:

* Validar el procedimiento si la contratación se realiza con una persona jurídica

* Dentro del procedimiento de contratación no se evidencia el proceso que se realiza en SECOP II

A.7.2 Durante la ejecución del empleo

A.7.2.1 Responsabilidades de la dirección

Nivel de Cumplimiento **60 /100**

Evidencia:

Se evidencia en la Política de seguridad de la información – Ítem: 11.2 Acuerdos de Intercambio de Información y Software

Recomendación:

Ninguna

A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información

Nivel de Cumplimiento **60 /100**

Evidencia:

a) Desarrollar campañas, elaborar folletos y boletines. SE ENVIAN CAPSULAS DE SEGURIDAD

NO HAY PLANES FORMALIZADOS. SE TIENEN CURSO VIRTUAL. CON FUTURAS MEJORAS

b) Los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están aprobados y documentados, por la alta Dirección SI ESTAN APROBADOS.

c) Verifique que nuevos empleados y contratistas son objeto de sensibilización en SI. NO SON SENSIBILIZADOS.

d) Indague cada cuanto o con qué criterios se actualizan los programas de toma de conciencia. NO SE HACE.

e) Verifique que en las evidencias se puede establecer los asistentes al programa y el tema impartido. NO HAY EVIDENCIA

Recomendación:

Crear un curso de formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.

A.7.2.3 Proceso disciplinario

Nivel de Cumplimiento **80 /100**

Evidencia:

Se rige por la Ley 734 de 2002 Código Disciplinario Único, Artículo 48 en su Numeral 43 (Causar daño a los equipos estatales de informática, alterar, falsificar, introducir, borrar, ocultar o desaparecer información en cualquiera de los sistemas de información oficial contenida en ellos o en los que se almacene o guarde la misma, o permitir el acceso a ella a personas no autorizadas.

A través de un proceso disciplinario se determina la sanción al infractor (PROCEDIMIENTO: CONTROL DISCIPLINARIO ORDINARIO CÓDIGO: GH-OCDI-PR-01)

Recomendación:

Ninguna.

A.7.3 Terminación y cambio de empleo

A.7.3.1 Terminación o cambio de responsabilidades de empleo

Nivel de Cumplimiento **40 /100**

Evidencia:

Se evidencia que está en la Política de Seguridad de la Información en el Ítem:

11.1 Acuerdos de Confidencialidad.

CONTRATACIÓN POR PRESTACIÓN DE SERVICIOS CON PERSONAS NATURALES GH-SECO-PR-01 ENTREVISTA TERMINACIÓN DE CONTRATO cód. GH-SECO-PR-01-FT-07.

Recomendación:

Revisar los acuerdos de confidencialidad, verificando que deben acordar que después de terminada la relación laboral o contrato seguirán vigentes por un periodo de tiempo.

A.8 GESTIÓN DE ACTIVOS

A.8.1.1. Inventario de activos

Nivel de Cumplimiento **40 /100**

Evidencia:

Se evidencia la existencia de un Procedimiento: Inventario y clasificación de activos TI-GESU-PR-02, el cual maneja un Formato llamado Inventario de Activos de la Información FT-TI-GESU-PR-02-FT-01. Los cuales son utilizados para realizar el inventario de activos.

No fue presentado el inventario de activos, por lo cual no se puede verificar si contiene la información requerida, ni si fue revisado y aprobado por la alta dirección.

No se determinó quien es el responsable de actualizar y revisar dicho inventario.

Recomendación:

Presentar el inventario de activos para determinar:

1) Ultima vez que se actualizó.

2) Que señale bajo algún criterio la importancia del activo

3) Que señale el propietario del activo

Indague quien(es) el(los) encargado(s) de actualizar y revisar el inventario de activos y cada cuanto se realiza esta revisión.

De acuerdo a NIST se deben considerar como activos el personal, dispositivos, sistemas e instalaciones físicas que permiten a la entidad cumplir con su misión y objetivos, dada su importancia y riesgos estratégicos.

El inventario de activos de información de la entidad debería especificar para cada activo:

- Información básica del activo (nombre, observaciones, proceso, entre otras).
- El nivel de clasificación de la información.
- Información relacionada con su ubicación, tanto física como electrónica.
- Su propietario y su custodio.
- Los usuarios y derechos de acceso.

Seguir la siguiente guía
Guía No.5 - Guía para la Gestión y Clasificación de Activos de Información.
(https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf)

A.8.1.2. Propiedad de los activos

Nivel de Cumplimiento **40 /100**

Evidencia:

Se evidencia la existencia de un Procedimiento: Inventario y clasificación de activos TI-GESU-PR-02, el cual maneja un Formato llamado Inventario de Activos de la Información FT-TI-GESU-PR-02-FT-01. Los cuales son utilizados para realizar el inventario de activos.

No fue presentado el inventario de activos, por lo cual no se puede verificar si contiene la información requerida, ni si fue revisado y aprobado por la alta dirección.

No se determinó quien es el responsable de actualizar y revisar dicho inventario.

Recomendación:

Presentar el inventario de activos para determinar:

1) Ultima vez que se actualizó.

2) Que señale bajo algún criterio la importancia del activo

3) Que señale el propietario del activo

Indague quien(es) el(los) encargado(s) de actualizar y revisar el inventario de activos y cada cuanto se realiza esta revisión.

De acuerdo a NIST se deben considerar como activos el personal, dispositivos, sistemas e instalaciones físicas que permiten a la entidad cumplir con su misión y objetivos, dada su importancia y riesgos estratégicos.

Seguir la siguiente guía
Guía No.5 - Guía para la Gestión y Clasificación de Activos de Información.
(https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

A.8.1.3. Uso aceptable de los activos

Nivel de Cumplimiento **40 /100**

Evidencia:

Se evidencia en la Política de Seguridad de la información en los Ítems:

7.7DUEÑOS O RESPONSABLES DE LOS ACTIVOS DE INFORMACION.

13.USO ADECUADO DE LOS ACTIVOS DE INFORMACION.

20 SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES.

21 TRASLADO DE PROPIEDAD.

30 COMPUTACION MOVIL.

Recomendación:

Validar la política, procedimiento, directriz o lineamiento que defina el uso aceptable de los activos.

Verificar que es conocida por los empleados y usuarios de partes externas que usan activos de la Entidad o tienen acceso a ellos.

A.8.1.4. Devolución de activos

Nivel de Cumplimiento **60 /100**

Evidencia:

Se usa el FORMATO: PAZ Y SALVO DESVINCULACIÓN CONTRATISTAS CÓDIGO: GH-SECO-PR-01-FT-11,en el cual la persona que se desvincula debe proceder a recoger las firmas de las distintas unidades

Recomendación:

Implementar un Procedimiento o Directriz para los siguientes casos:

En caso de que un funcionario o tercero sea el dueño del activo indague como se asegura la transferencia de la información a la Entidad y el borrado seguro de la información de la Entidad.

En caso en que un empleado o usuario de una parte externa posea conocimientos que son importantes para las operaciones regulares, esa información se debería documentar y transferir a la Entidad.

Durante el período de notificación de la terminación, la Entidad debería controlar el copiado no autorizado de la información pertinente (por ejemplo, la propiedad intelectual) por parte de los empleados o contratistas que han finalizado el empleo.

A.8.2.1 Clasificación de la información

Nivel de Cumplimiento **40 /100**

Evidencia:

Se evidencia que existe el Procedimiento: Inventario y clasificación de activos TI-GESU-PR-02 y el formato Inventario de Activos de la Información FT-TI-GESU-PR-02-FT-01.

No se presenta el inventario de activos.

Recomendación:

Validar el procedimiento mediante el cual se clasifican los activos de información y evaluar:

1) Que las convenciones y criterios de clasificación sean claros y estén documentados

2) Que se defina cada cuanto debe revisarse la clasificación de un activo

3) La clasificación debería valorarse analizando la confidencialidad, integridad y disponibilidad.

Solicitar muestras de inventarios de activos de información clasificados y evalué que se aplican las políticas y procedimientos de clasificación definidos. Evalué si los procesos seleccionados aplican de manera consistente estas políticas y procedimientos.

Seguir la siguiente guía
Guía No.5 - Guía para la Gestión y Clasificación de Activos de Información.
(https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

A.8.2.2 Etiquetado de la información

Nivel de Cumplimiento **20 /100**

Evidencia:

No se evidencia que este documentado el procedimiento en cuestión

Recomendación:

Si no existe implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.

Si existe, presentar el procedimiento para el etiquetado de la información para poder:

1) Aplica a activos en formatos físicos y electrónicos (etiquetas físicas, metadatos)

2) Que refleje el esquema de clasificación establecido

3) Que las etiquetas se puedan reconocer fácilmente

4) Que los empleados y contratistas conocen el procedimiento de etiquetado

Revisar en una muestra de activos el correcto etiquetado.

Seguir la siguiente guía
Guía No.5 - Guía para la Gestión y Clasificación de Activos de Información.
(https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

A.8.2.3 Manejo de activos

Nivel de Cumplimiento **20 /100**

Evidencia:

No se evidencia que este documentado el procedimiento en cuestión

Recomendación:

Si no existen implementar los procedimientos para el manejo, procesamiento, almacenamiento y comunicación de información.

Si existe presentar los procedimientos para el manejo, procesamiento, almacenamiento y comunicación de información de conformidad con su clasificación.

De acuerdo a las mejores prácticas evidencie si se han considerado los siguientes asuntos:

a) Restricciones de acceso que soportan los requisitos de protección para cada nivel de clasificación;

b) Registro formal de los receptores autorizados de los activos;

c) Protección de copias de información temporal o permanente a un nivel coherente con la protección de la información original;

d) Almacenamiento de los activos de TI de acuerdo con las especificaciones de los fabricantes;

e) Marcado claro de todas las copias de medios para la atención del receptor autorizado.

f) De acuerdo a NIST la información almacenada (at rest) y en tránsito debe ser protegida.

A.8.3.1 Gestión de medios removibles

Nivel de Cumplimiento **20/100**

Evidencia:

No existe el procedimiento.

Pero se enuncia en la Política de Seguridad de la información. Ítem 29 GESTION DE MEDIOS REMOVIBLES

Recomendación:

Crear las directrices, guías, lineamientos y procedimientos para la gestión de medios removibles, que consideren:

a) Si ya no se requiere, el contenido de cualquier medio reusable que se vaya a retirar de la organización se debe remover de forma que no sea recuperable;

b) cuando resulte necesario y práctico, se debe solicitar autorización para retirar los medios de la organización, y se debe llevar un registro de dichos retiros con el fin de mantener un rastro de auditoría;

d) si la confidencialidad o integridad de los datos se consideran importantes, se deben usar técnicas criptográficas para proteger los datos que se encuentran en los medios removibles;

f) se deben guardar varias copias de los datos valiosos en medios separados, para reducir aún más el riesgo de daño o pérdida casuales de los datos;

h) sólo se deben habilitar unidades de medios removibles si hay una razón de valida asociada a los procesos la Entidad para hacerlo;

i) En donde hay necesidad de usar medios removibles, se debería hacer seguimiento a la transferencia de información a estos medios (Por ejemplo, DLP).

A.8.3.2 Disposición de los medios

Nivel de Cumplimiento **0 /100**

Evidencia:

No se evidencia que este documentado el procedimiento en cuestión

Recomendación:

Crear los procedimientos existentes para garantizar que los medios a desechar o donar, no contienen información confidencial que pueda ser consultada y copiada por personas no autorizadas.

Verificar si se ha realizado esta actividad y si existen registros de la misma.

A.8.3.3 Transferencia de medios físicos

Nivel de Cumplimiento **0 /100**

Evidencia:

No se evidencia que este documentado el procedimiento en cuestión

Recomendación:

Crear las directrices las cuales definan la protección de medios que contienen información durante el transporte. Verifique de acuerdo a las mejores prácticas que se contemple:

a) El uso de un transporte o servicios de mensajería confiables.

b) Procedimientos para verificar la identificación de los servicios de mensajería.

c) Indague y evidencie como es el embalaje el cual debe proteger el contenido contra cualquier daño físico que pudiera presentarse durante el tránsito, y de acuerdo con las especificaciones de los fabricantes, por ejemplo, protección contra cualquier factor ambiental que pueda reducir la eficacia de la restauración del medio, tal como exposición al calor, humedad o campos electromagnéticos;

d) Solicite los registros que dejen evidencia del transporte donde se identifique el contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte, y el recibo en su destino.

A.9 CONTROL DE ACCESO

A.9.1.1. Política de control de acceso

Nivel de Cumplimiento **20 /100**

Evidencia:

No se evidencia que este documentada la política de control de acceso

Recomendación:

Crear de la Política de Control de Acceso en la cual se incluya lo que se requiere en la Norma ISO 27002. Control A9.1.1.

a) los requisitos de seguridad para las aplicaciones del negocio.

b) las políticas para la divulgación y autorización de la información, y los niveles de seguridad de la información y de clasificación de la información.

c) la coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes.

d) la legislación pertinente y cualquier obligación contractual concerniente a la limitación del acceso a datos o servicios.

e) la gestión de los derechos de acceso en un entorno distribuido y en red, que reconoce todos los tipos de conexiones disponibles.

f) la separación de los roles de control de acceso, (solicitud de acceso, autorización de acceso, administración del acceso).

g) los requisitos para la autorización formal de las solicitudes de acceso.

h) los requisitos para la revisión periódica de los derechos de acceso.

i) el retiro de los derechos de acceso.

j) el ingreso de los registros de todos los eventos significativos concernientes al uso y gestión de identificación de los usuarios, e información de autenticación secreta, en el archivo permanente.

k) los roles de acceso privilegiado.

A.9.1.2. Acceso a redes y a servicios en red

Nivel de Cumplimiento **40 /100**

Evidencia:

Se evidencia que existen los siguientes documentos:

PROCEDIMEINTO CREACION DE USUARIOS Y ASIGNACION DE PERMISOS CÓDIGO: GT-UNIN-PR-04

formato Único de Solicitud de Acceso a las Tecnologías de la Información Cód.: IM-UNIN-FT-02

Recomendación:

Realizar la respectiva documentación a las actividades que se están realizando, y que no tienen las guías respectivas de las operaciones necesarias para llevar a cabo dichos procedimientos.

Faltan en el procedimiento con los controles y procedimientos de gestión para proteger el acceso a las conexiones de red y a los servicios de red.

A.9.2.1 Registro y cancelación del registro de usuarios

Nivel de Cumplimiento **40 /100**

Evidencia:

Se evidencia que existen los siguientes documentos:

PROCEDIMEINTO CREACION DE USUARIOS Y ASIGNACION DE PERMISOS CÓDIGO: GT-UNIN-PR-04

formato Único de Solicitud de Acceso a las Tecnologías de la Información Cód.: IM-UNIN-FT-02

Recomendación:

Realizar la respectiva documentación a las actividades que se están realizando, y que no tienen las guías de las operaciones necesarias para llevar a cabo dichos procedimientos.

Faltan en el procedimiento relacionar estas actividades:

c) identificar y eliminar o deshabilitar periódicamente las identificaciones de usuario redundantes.

d) asegurar que las identificaciones de usuario redundantes no se asignen a otros usuarios

A.9.2.2 Suministro de acceso de usuarios

Nivel de Cumplimiento **40 /100**

Evidencia:

Se evidencia que usan los siguientes documentos:

PROCEDIMEINTO CREACION DE USUARIOS Y ASIGNACION DE PERMISOS CÓDIGO: GT-UNIN-PR-04

formato Único de Solicitud de Acceso a las Tecnologías de la Información Cód.: IM-UNIN-FT-02

PROCEDIMIENTO: GESTION TECNOLÓGICA -INCO CÓDIGO: GT-INCO-PR-02 (Realizar la Administración de los Servicios de TI (Directorio Activo, Correo Electrónico, File Server, FTP, Servidor de Impresión, DHCP y DNS))

Recomendación:

1) Realizar la respectiva documentación a las actividades que se están realizando, y que no tienen las guías de las operaciones necesarias para llevar a cabo dichos procedimientos

2)mantener un registro central de los derechos de acceso suministrados a una identificación de usuario para acceder a sistemas de información y servicios;

3) revisar periódicamente los derechos de acceso con los propietarios de los sistemas de información o servicios.

A.9.2.3 Gestión de derechos de acceso privilegiado

Nivel de Cumplimiento **20 /100**

Evidencia:

No existe el procedimiento el cual describa el proceso de autorización formal que este alineado a la Política de Control de Acceso

Recomendación:

Crear la política en la cual se cumplan los requerimientos que pide la Norma ISO 27002 en este control.

Revisar la asignación de derechos de acceso privilegiado a través de un proceso de autorización formal de acuerdo con la política de control de acceso pertinente. el proceso debe incluir los siguientes pasos:

a) Identificar los derechos de acceso privilegiado asociados con cada sistema o proceso, (sistema operativo, sistema de gestión de bases de datos, y cada aplicación) y los usuarios a los que es necesario asignar.

b) definir o establecer los derechos de acceso privilegiado a usuarios con base en la necesidad de uso y caso por caso, alineada con la política de control de acceso.

c) mantener un proceso de autorización y un registro de todos los privilegios asignados. Sólo se debe suministrar derechos de acceso cuando el proceso de autorización esté completo.

d) definir los requisitos para la expiración de los derechos de acceso privilegiado.

e) establecer los derechos de acceso privilegiado a través de una identificación de usuario diferente de la usada para las actividades regulares del negocio. Las actividades regulares del negocio no se ejecutan desde una identificación privilegiada.

f) tener las competencias de los usuarios con derechos de acceso privilegiado y su revisión periódica para verificar si están en línea con sus deberes.

g) establecer y mantener procedimientos genéricos para evitar el uso no autorizado de identificaciones de usuario de administración genérica, de acuerdo con las capacidades de configuración del sistema.

h) establecer la confidencialidad de la información de autenticación secreta, para las identificaciones de usuario de administración genérica, cuando se comparta (cambiar las contraseñas con frecuencia, y cuando un usuario privilegiado ha dejado el trabajo o cambia de trabajo, comunicarlas entre los usuarios privilegiados con los mecanismos apropiados).

A.9.2.4 Gestión de información de autenticación secreta de usuarios

Nivel de Cumplimiento **20 /100**

Evidencia:

No existe el procedimiento el cual describa la Gestión de información de autenticación secreta de usuarios.

Recomendación:

Crear la política en cual se detalle el procedimiento de Gestión de información de autenticación secreta de usuarios, que incluya:

a) establecer la firma de una declaración para mantener confidencial la información de autenticación secreta personal, y mantener la información de autenticación secreta del grupo (cuando es compartida) únicamente dentro de los miembros del grupo; esta declaración firmada se puede incluir en los términos y condiciones del empleo para todos los que los usuarios.

b) estipular que todos los usuarios deben mantener su propia información de autenticación secreta, y se les suministra una autentificación secreta temporal segura, que se obligue a cambiar al usarla por primera vez.

c) establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle la nueva información de autenticación secreta de reemplazo o temporal.

d) definir que la información de autenticación secreta temporal se suministra a los usuarios de una manera segura; y se evitar utilizar partes externas o de mensajes de correo electrónico no protegidos (texto claro).

e) establecer que la información de autenticación secreta temporal es única para un individuo y no es fácil de adivinar.

f) definir que los usuarios deben acusar recibo de la información de autenticación secreta.

g) establecer que la información de autenticación secreta por defecto, del fabricante, se modifica después de la instalación de los sistemas o software.

A.9.2.5 Revisión de los derechos de acceso de usuarios

Nivel de Cumplimiento **40 /100**

Evidencia:

Se evidencia que se usa el siguiente documento:

PROCEDIMIENTO: GESTION TECNOLÓGICA -INCO CÓDIGO: GT-INCO-PR-02

Realizar la Administración de los Servicios de TI (Directorio Activo, Correo Electrónico, File Server, FTP, Servidor de Impresión, DHCP y DNS)

Recomendación:

Se debe documentar el proceso de Revisión de los derechos de acceso de usuarios, documentar los procedimientos que se realizan para llevar a cabo de esta actividad el cual incluya:

a) examinar los derechos de acceso de los usuarios periódicamente y después de cualquier cambio, promoción, cambio a un cargo a un nivel inferior, o terminación del empleo;

b) establecer que los derechos de acceso de usuario se revisan y reasignan cuando pasan de un rol a otro dentro de la misma organización;

c) definir las autorizaciones para los derechos de acceso privilegiado y revisar periódicamente;

d) verificar las asignaciones de privilegios periódicamente, para asegurar que no se hayan obtenido privilegios no autorizados;

e) revisar y registrar los cambios a las cuentas privilegiadas periódicamente.

A.9.2.6 Retiro o ajuste de los derechos de acceso

Nivel de Cumplimiento **40 /100**

Evidencia:

Se evidencia que se usa el siguiente documento:

PROCEDIMIENTO: GESTION TECNOLÓGICA -INCO CÓDIGO: GT-INCO-PR-02

Realizar la Administración de los Servicios de TI (Directorio Activo, Correo Electrónico, File Server, FTP, Servidor de Impresión, DHCP y DNS)

Recomendación:

Se debe documentar el proceso de Retiro o ajuste de los derechos de acceso

Revisar los derechos de acceso a la información y a los activos asociados con instalaciones de procesamiento de información, antes de que el empleo termine o cambie, dependiendo de la evaluación de factores de riesgo que incluya:

a) terminación o cambio lo inicia el empleado, el usuario de la parte externa o la dirección, y la razón de la terminación;

b) revisar las responsabilidades actuales del empleado, el usuario de la parte externa o cualquier otro usuario;

c) verificar el valor de los activos accesibles en la actualidad.

A.9.3.1 Uso de información de autenticación secreta

Nivel de Cumplimiento **60 /100**

Evidencia:

Se evidencia que se usa lo siguiente:

Se encuentra estipulado en la Política de Seguridad de la Información ítem 33 ADMINISTRACION DE CONTRASEÑAS.

y además se le envían TIPS a los usuarios vía email

Recomendación:

Documentar las características definidas para las contraseñas que se van a emplear.

Actualizar la Política de Seguridad de la Información, en el ITEM 33 Administración de Contraseñas. Pues no se evidencia el procedimiento de Gestión de Usuarios y Contraseñas

A.9.4.1 Restricción de acceso a la información

Nivel de Cumplimiento **60 /100**

Evidencia:

Se evidencia que se usan los siguientes documentos:

PROCEDIMEINTO CREACION DE USUARIOS Y ASIGNACION DE PERMISOS CÓDIGO: GT-UNIN-PR-04

formato Único de Solicitud de Acceso a las Tecnologías de la Información Cód.: IM-UNIN-FT-02

b) mediante los perfiles asignados se controla a qué datos puede tener acceso un usuario particular.

c) mediante los perfiles asignados se controlan los derechos de acceso de los usuarios, (a leer, escribir, borrar y ejecutar).

d) mediante los perfiles asignados se controlan los derechos de acceso de otras aplicaciones.

e) mediante los perfiles asignados se limita la información contenida en los elementos de salida.

f) mediante los perfiles asignados se provee controles de acceso físico o lógico para el aislamiento de aplicaciones, datos de aplicaciones o sistemas críticos.

Las solicitudes de acceso llegan por Correo electrónico al Jefe de la Unidad de Informática, quien posteriormente envía el caso a la Mesa de Servicio.

INCO: Controla el acceso por VPN, a nivel de Directorio Activo.

GEAM: Gestiona los permisos sobre aplicativos (Dinámica gerencial hospitalaria), Ruaf

Recomendación:

Validar que en la política de control de acceso definida este incluido los siguientes temas:

a) suministrar menús para controlar el acceso a las funciones de sistemas de aplicaciones.

b) controlar a qué datos puede tener acceso un usuario particular.

c) controlar los derechos de acceso de los usuarios, (a leer, escribir, borrar y ejecutar).

d) controlar los derechos de acceso de otras aplicaciones.

e) limitar la información contenida en los elementos de salida.

f) proveer controles de acceso físico o lógico para el aislamiento de aplicaciones, datos de aplicaciones o sistemas críticos.

A.9.4.2 Procedimiento de ingreso seguro

Nivel de Cumplimiento **40 /100**

Evidencia:

Se realiza en el 50 % de las aplicaciones.

Recomendación:

Generar política que contenga el procedimiento de ingreso que incluya:

a) no visualizar los identificadores del sistema o de la aplicación sino hasta que el proceso de ingreso se haya completado exitosamente;

b) visualizar una advertencia general acerca de que sólo los usuarios autorizados pueden acceder al computador;

c) evitar los mensajes de ayuda durante el procedimiento de ingreso, que ayudarían a un usuario no autorizado;

d) validar la información de ingreso solamente al completar todos los datos de entrada. ante una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta;

e) proteger contra intentos de ingreso mediante fuerza bruta;

f) llevar un registro con los intentos exitosos y fallidos;

g) declarar un evento de seguridad si se detecta un intento potencial o una violación exitosa de los controles de ingreso;

h) visualizar la siguiente información al terminar un ingreso seguro:

1) registrar la fecha y la hora del ingreso previo exitoso;

2) registrar los detalles de cualquier intento de ingreso no exitoso desde el último ingreso exitoso;

i) no visualizar una contraseña que se esté ingresando;

j) no transmitir contraseñas en un texto claro en una red;

k) terminar sesiones inactivas después de un período de inactividad definido, especialmente en lugares de alto riesgo tales como áreas públicas o externas por fuera de la gestión de seguridad de la organización o en dispositivos móviles;

l) restringir los tiempos de conexión para brindar seguridad adicional para aplicaciones de alto riesgo y para reducir la ventana de oportunidad para acceso no autorizado.

A.9.4.3 Sistema de gestión de contraseñas

Nivel de Cumplimiento **60 /100**

Evidencia:

Se cumple en la plataforma de Windows y en el Correo Electrónico. Además, está inmerso en la política de seguridad informáticas

Recomendación:

Revisar el sistema de gestión de contraseñas que incluya:

a) cumplir el uso de identificaciones y contraseñas de usuarios individuales para mantener la rendición de cuentas;

b) permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluyan un procedimiento de confirmación para permitir los errores de entrada;

c) Exigir por que se escojan contraseñas de calidad;

d) Forzar a los usuarios cambiar sus contraseñas cuando ingresan por primera vez;

e) Exigir por que se cambien las contraseñas en forma regular, según sea necesario:

f) llevar un registro de las contraseñas usadas previamente, e impedir su reusó;

g) no visualizar contraseñas en la pantalla cuando se está ingresando;

h) almacenar los archivos de las contraseñas separadamente de los datos del sistema de aplicaciones;

i) almacenar y transmitir las contraseñas en forma protegida.

A.9.4.4 Uso de programas utilitarios privilegiados

Nivel de Cumplimiento **40 /100**

Evidencia:

Se cumple en la plataforma de Windows y además está inmerso en la política de seguridad informática ítem 13.7 Uso de recursos tecnológicos - sub ítem a

Recomendación:

Crear las directrices para el uso de programas utilitarios con la capacidad de anular los controles de sistemas y de aplicaciones, que incluyan.

a) utilizar procedimientos de identificación, autenticación y autorización para los programas utilitarios;

b) separar los programas utilitarios del software de aplicaciones;

c) limitar el uso de programas utilitarios al número mínimo práctico de usuarios confiables y autorizados;

d) autorizar el uso adhoc de programas utilitarios;

e) limitar la disponibilidad de los programas utilitarios;

f) registrar el uso de los programas utilitarios;

g) definir y documentar los niveles de autorización para los programas utilitarios;

h) retirar o deshabilitar todos los programas utilitarios innecesarios;

i) No poner a disposición los programas utilitarios a los usuarios que tengan acceso a aplicaciones en sistemas en donde se requiera la separación de deberes.

A.9.4.5 Control de acceso a códigos fuente de programas

Nivel de Cumplimiento **60 /100**

Evidencia:

a)si hay repositorios en GitHub. De algunos códigos fuentes. Queda por definir donde se va a centralizar.

b) No esta documento gestionar los códigos fuente de los programas y las librerías de las fuentes de los programas se debería hacer de acuerdo con procedimientos establecidos

c) solo una persona tiene acceso restringido a las librerías de las fuentes de los programas.

d) Se tiene definido que la actualización de las librerías de fuentes de programas y elementos asociados, y la entrega de fuentes de programas a los programadores sólo se deben hacer una vez que se haya recibido autorización apropiada.

e) se tienen los listados de programas se deben mantener en un entorno seguro

f) No se conserva un registro de auditoría de todos los accesos a las librerías de fuentes de programas

g) se mantienen y se copian las bibliotecas de fuentes de programas a través de procedimientos estrictos de control de cambios

Recomendación:

Definir repositorio de los códigos fuentes

Definir personas autorizadas para el acceso a esta información

Crear registro de auditoria sobre el acceso a los códigos fuente

Tener copias, preferiblemente zipiadas con contraseña

A.10 CRIPTOGRAFÍA

A.10.1.1. Política sobre el uso de controles criptográficos

Nivel de Cumplimiento **0 /100**

Evidencia:

No existe Política

Recomendación:

Crear la política sobre el uso de la criptográfica, que incluya:

a) establecer el enfoque de la dirección con relación al uso de controles criptográficos en toda la organización, incluyendo los principios generales bajo los cuales se deben proteger la información del negocio;

b) realizar una valoración de riesgos, que identifique el nivel de protección requerida, teniendo en cuenta el tipo, fortaleza y calidad del algoritmo de encriptación requerido.

c) utilizar la encriptación para la protección de información transportada por dispositivos de encriptación móviles o removibles, o a través de líneas de comunicación;

d) gestionar las llaves y los métodos para la protección de llaves criptográficas y la recuperación de información encriptada, en el caso de llaves perdidas, llaves cuya seguridad está comprometida, o que están dañadas;

e) establecer roles y responsabilidades, quién es responsable por:

1) la implementación de la política.

2) la gestión de llaves, incluida la generación de llaves;

f) establecer las normas que se van a adoptar para la implementación efectiva en toda la organización (procesos del negocio);

g) definir el impacto de usar información encriptada en los controles que dependen de la inspección del contenido.

A.10.1.2. Gestión de llaves

Nivel de Cumplimiento **0 /100**

Evidencia:

No existe Política

Recomendación:

Revisar el sistema de gestión de llaves que debe estar basado en un grupo establecido de normas, procedimientos y métodos seguros para:

a) generar llaves para diferentes sistemas criptográficos y diferentes aplicaciones;

b) generar y obtener certificados de llaves públicas;

c) distribuir llaves a las entidades previstas, incluyendo la forma de recibir y activar las llaves;

d) almacenar las llaves, incluyendo la forma en que los usuarios autorizados obtienen acceso a ellas;

e) cambiar o actualizar las llaves, incluyendo las reglas sobre cuándo se deben cambiar y cómo hacerlo;

f) dar tratamiento a las llaves cuya seguridad está comprometida;

g) revocar las llaves, incluyendo la forma de retirarlas o desactivarlas, cuando la seguridad de las llaves ha estado comprometida, o cuando un usuario deja la organización;

h) recuperar las llaves que estén pérdidas o dañadas;

i) hacer copias de respaldo de las llaves o archivarlas;

j) destruir las llaves;

k) registrar y auditar las actividades relacionadas con gestión de llaves.

A.11 SEGURIDAD FÍSICA Y DEL ENTORNO

A.11.1.1. Perímetro de seguridad física

Nivel de Cumplimiento **60 /100**

Evidencia:

Se evidencia que se utilizan:

CONTROL DE ACCESO A DATACENTER EDIFICIO PRINCIPAL

- control de acceso biométrico (huella digital o clave)

- planilla de acceso (pendiente formato)

CONTROL DE ACCESO A DATACENTER CONTAINER

- Tarjeta de acceso, y candados.

- planilla de acceso (pendiente formato)

Recomendación:

Se debe implementar un PROCEDIMIENTO DE PROTECCIÓN DE ACTIVOS:

Este procedimiento debe contener los pasos con los cuales los equipos son protegidos por la entidad. Se recomienda que este procedimiento indique como se determina la ubicación de los equipos que procesan información confidencial, como se aseguran dichas las instalaciones, los controles que se aplican para minimizar riesgos de desastres naturales, amenazas físicas, daños, por polvo, agua, interferencias, descargas eléctricas etc…

Se debe implementar PROCEDIMIENTO DE CONTROL DE ACCESO FÍSICO:

En este procedimiento se debe describir como se ejecutan los diferentes pasos para garantizar el control de acceso seguro a las instalaciones al personal autorizado. Este procedimiento puede incluir registros de fecha y hora de ingreso, seguimiento de los libros o plataforma de registro. Se debe contemplar la solicitud de permiso a áreas restringidas, quien los otorga y que debe hacerse para poder tener acceso a las áreas etc.

A.11.1.2. Controles físicos de entrada

Nivel de Cumplimiento **60 /100**

Evidencia:

Se evidencia que se utilizan:

CONTROL DE ACCESO A DATACENTER EDIFICIO PRINCIPAL

- control de acceso biométrico (huella digital o clave)

- planilla de acceso (pendiente formato)

CONTROL DE ACCESO A DATACENTER CONTAINER

- Tarjeta de acceso, y candados.

- planilla de acceso (pendiente formato)

Recomendación:

Se debe implementar PROCEDIMIENTO DE CONTROL DE ACCESO FÍSICO:

En este procedimiento se debe describir como se ejecutan los diferentes pasos para garantizar el control de acceso seguro a las instalaciones al personal autorizado. Este procedimiento puede incluir registros de fecha y hora de ingreso, seguimiento de los libros o plataforma de registro. Se debe contemplar la solicitud de permiso a áreas restringidas, quien los otorga y que debe hacerse para poder tener acceso a las áreas etc.

A.11.1.3. Seguridad de oficinas, recintos e instalaciones

Nivel de Cumplimiento **60 /100**

Evidencia:

Si se cumple con un control de acceso por parte de vigilancia privada

Recomendación:

Revisar o crear, en caso de no existir, una política con las siguientes directrices relacionadas con la seguridad a oficinas, recintos e instalaciones:

a) establecer que las instalaciones clave deben estar ubicadas de manera que se impida el acceso del público;

b) definir donde sea aplicable, las edificaciones deben ser discretas y dar un indicio mínimo de su propósito, sin señales obvias externas o internas, que identifiquen la presencia de actividades de procesamiento de información;

c) establecer que las instalaciones deben estar configuradas para evitar que las actividades o información confidenciales sean visibles y audibles desde el exterior. El blindaje electromagnético también se debe ser el apropiado;

d) definir los directorios y guías telefónicas internas que identifican los lugares de las instalaciones de procesamiento de información confidencial no deben ser accesibles a ninguna persona no autorizada.

A.11.1.4. Protección contra amenazas externas y ambientales

Nivel de Cumplimiento **60 /100**

Evidencia:

Contra ataques maliciosos o accidentes . Se tiene implementado un firewall contra ataques externos. Se tienen implementadas restricciones de acceso a las instalaciones del HOMIL (entrada y a las distintas oficinas)

Se cumple la protección, pero no se encuentra documentada.

Recomendación:

Se debe implementar un PROCEDIMIENTO DE PROTECCIÓN DE ACTIVOS:

Este procedimiento debe contener los pasos con los cuales los equipos son protegidos por la entidad. Se recomienda que este procedimiento indique como se determina la ubicación de los equipos que procesan información confidencial, como se aseguran dichas las instalaciones, los controles que se aplican para minimizar riesgos de desastres naturales, amenazas físicas, daños, por polvo, agua, interferencias, descargas eléctricas etc…

Se debe implementar PROCEDIMIENTO DE CONTROL DE ACCESO FÍSICO:

En este procedimiento se debe describir como se ejecutan los diferentes pasos para garantizar el control de acceso seguro a las instalaciones al personal autorizado. Este procedimiento puede incluir registros de fecha y hora de ingreso, seguimiento de los libros o plataforma de registro. Se debe contemplar la solicitud de permiso a áreas restringidas, quien los otorga y que debe hacerse para poder tener acceso a las áreas etc.

A.11.1.5. Trabajo en áreas seguras

Nivel de Cumplimiento **60 /100**

Evidencia:

Se evidencia que se utilizan:

CONTROL DE ACCESO A DATACENTER EDIFICIO PRINCIPAL

- control de acceso biométrico (huella digital o clave)

- planilla de acceso (pendiente formato)

CONTROL DE ACCESO A DATACENTER CONTAINER

- Tarjeta de acceso, y candados.

- planilla de acceso (pendiente formato)

CONTROL DE ACCESO A EDIFICIO PRINCIPAL

con vigilancia privada

Recomendación:

Revisar o crear, en caso de no existir, un Procedimiento con las siguientes directrices:

a) establecer que el personal solo debe conocer de la existencia de un área segura o de actividades dentro de un área segura, con base en lo que necesita conocer.

b) definir que el trabajo no supervisado en áreas seguras se debe evitar tanto por razones de seguridad como para evitar oportunidades para actividades malintencionadas.

c) establecer que las áreas seguras vacías deben estar cerradas con llave y se revisan periódicamente.

d) no se permite el ingreso y uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello.

.

A.11.1.6. Áreas de despacho y carga

Nivel de Cumplimiento **0 /100**

Evidencia:

Se evidencia que se tiene el documento PROCEDIMIENTO: INFORMACION GENERAL E INGRESO DE USUARIOS AL ÁREA HOSPITALARIA CÓDIGO: SL-COIN-PR-04, donde se detalla el procedimiento de ingreso de personal a las diferentes áreas del HOMIL. Además, se estipula:

Proveedores: El horario de atenciones de las 07:30 hasta las 16:30 y el ingreso de productos se realiza por la zona de descargue sótano 1

Otro control que se tiene en el acceso al HOMIL, es por parte del personal militar.

Recomendación:

Continuar con los controles.

Revisar, y si es necesario complementar con las siguientes directrices:

a) establecer que el acceso al área de despacho y de carga desde el exterior de la edificación se debería restringir al personal identificado y autorizado.

b) definir que el área de despacho y carga se debe diseñar de manera que los suministros se puedan cargar y descargar sin que el personal de despacho tenga acceso a otras partes de la edificación.

c) establecer que las puertas externas de un área de despacho y carga se aseguran cuando las puertas internas están abiertas.

d) definir que el material que ingresa se inspecciona y examina para determinar la presencia de explosivos, químicos u otros materiales peligrosos, antes de que se retiren del área de despacho y carga.

e) establecer que el material que ingresa se registra de acuerdo con los procedimientos de gestión de activos al entrar al sitio.

f) definir que los despachos entrantes y salientes se están separados físicamente, en donde sea posible.

g) establecer que el material entrante se inspecciona para determinar evidencia de manipulación durante el viaje. Si se descubre esta manipulación, se debería reportar de inmediato al personal de seguridad.

A.11.2.1 Ubicación y protección de los equipos

Nivel de Cumplimiento **60 /100**

Evidencia:

Se evidencia que se utilizan:

CONTROL DE ACCESO A DATACENTER EDIFICIO PRINCIPAL

- control de acceso biométrico (huella digital o clave)

- planilla de acceso (pendiente formato)

CONTROL DE ACCESO A DATACENTER CONTAINER

- Tarjeta de acceso, y candados.

- planilla de acceso (pendiente formato)

Recomendación:

Revisar o crear, en caso de no existir, Procedimiento con las siguientes directrices para proteger los equipos:

a) establecer que los equipos están ubicados de manera que se minimice el acceso innecesario a las áreas de trabajo;

b) definir que las instalaciones de procesamiento de la información que manejan datos sensibles están ubicadas cuidadosamente para reducir el riesgo de que personas no autorizadas puedan ver la información durante su uso;

c) establecer que las instalaciones de almacenamiento se aseguran para evitar el acceso no autorizado;

d) definir que los elementos que requieren protección especial se salvaguardan para reducir el nivel general de protección requerida;

e) establecer los controles para minimizar el riesgo de amenazas físicas y ambientales, (robo, incendio, explosivos, humo, agua (o falla en el suministro de agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo);

f) establecer directrices acerca de comer, consumir líquidos y fumar en cercanías de las instalaciones de procesamiento de información;

g) hacer seguimiento de las condiciones ambientales tales como temperatura y humedad, para determinar las condiciones que puedan afectar adversamente las instalaciones de procesamiento de información;

h) proteger contra descargas eléctricas atmosféricas se debe aplicar a todas las edificaciones y se deben colocar filtros a todas las líneas de comunicaciones y de potencia entrantes, para la protección contra dichas descargas;

i) considerar el uso de métodos de protección especial, tales como membranas para teclados, para equipos en ambientes industriales;

j) proteger los equipos para procesamiento de información confidencial para minimizar el riesgo de fuga de información debido a emanaciones electromagnéticas.

A.11.2.2 Servicios de suministro

Nivel de Cumplimiento **60 /100**

Evidencia:

Se SI SE CUMPLE se tiene:

redundancia e UPS

AIRE ACONDINCIONADO

Redundancia en servicio de internet

Redundancia en Cableado para servicios críticos

Recomendación:

Revisar los servicios de suministro (electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado) para que cumplan:

a) cumplir con las especificaciones de los fabricantes de equipos y con los requisitos legales locales;

b) evaluar regularmente en cuanto a su capacidad para estar al ritmo del crecimiento e interacciones del negocio con otros servicios de soporte;

c) inspeccionar y probar regularmente para asegurar su funcionamiento apropiado;

d) si es necesario, contar con alarmas para detectar mal funcionamiento;

e) si es necesario, tener múltiples alimentaciones con diverso enrutado físico.

A.11.2.3 Seguridad del cableado

Nivel de Cumplimiento **60 /100**

Evidencia:

Se establece que las líneas de potencia y de telecomunicaciones que entran a instalaciones de procesamiento de información deben ser subterráneas en donde sea posible, o deben contar con una protección alternativa adecuada.

b) Se establece que los cables de potencia están separados de los cables de comunicaciones para evitar interferencia.

c) definir para sistemas sensibles o críticos los controles adicionales que se deben considerar incluyen:

1) Se establece que la instalación de conduit apantallado y recintos o cajas con llave en los puntos de inspección y de terminación.

2) Se usa de blindaje electromagnético para proteger los cables.

3) el inicio de barridos técnicos e inspecciones físicas de dispositivos no autorizados que se conectan a los cables. SI SE CUMPLE

Recomendación:

Realizar revisiones anuales para dar cumplimiento de las directrices para la seguridad del cableado.

A.11.2.4 Mantenimiento de equipos

Nivel de Cumplimiento **60 /100**

Evidencia:

Se evidencia que se usa el siguiente documento:

PROCEDIMIENTO: MANTENIMIENTO PREVENTIVO DE SOFTWARE Y HARDWARE CÓDIGO: TI-GERE-PR-02

Se informa por parte de Guillermo Chacón, que los mantenimientos preventivos y correctivos son realizados por parte de una empresa externa.

Estos mantenimientos se comenzaron en el mes de agosto. Por medio de un contrato de mantenimiento

Se presenta el Orden de Compra # 73307 de la empresa COMSISTELCO S.A.S de fecha 28/07/2021. (750 equipos)

Recomendación:

Crear un formato para la programación de los mantenimientos donde se pueda establecer las fechas de programación de los mantenimientos y la ejecución de los mismos. Asi como llevar un registro de los equipos a los cuales se les va a realizar dicho mantenimiento.

Revisar o crear, en caso de no existir, una política con las siguientes directrices para mantenimiento de equipos:

a) mantener los equipos de acuerdo con los intervalos y especificaciones de servicio recomendados por el proveedor;

b) establecer que solo el personal de mantenimiento autorizado debería llevar a cabo las reparaciones y el servicio a los equipos;

c) llevar registros de todas las fallas reales o sospechadas, y de todo el mantenimiento preventivo y correctivo;

d) implementar los controles apropiados cuando el equipo está programado para mantenimiento, teniendo en cuenta si éste lo lleva a cabo el personal en el sitio o personal externo a la organización; en donde sea necesario, la información confidencial se debe borrar del equipo, o el personal de mantenimiento debería retirarse (cleared) lo suficientemente de la información;

e) cumplir todos los requisitos de mantenimiento impuestos por las políticas de seguros;

f) establecer que antes de volver a poner el equipo en operación después de mantenimiento, se debería inspeccionar para asegurarse de que no ha sido alterado y que su funcionamiento es adecuado.

A.11.2.5 Retiro de activos

Nivel de Cumplimiento **0 /100**

Evidencia:

Se evidencia que no existe procedimiento documentado:

Recomendación:

Revisar o crear, en caso de no existir, una política con las siguientes directrices para el retiro de activos:

a) identificar a los empleados y usuarios de partes externas que tienen autoridad para permitir el retiro de activos del sitio;

b) establecer los límites de tiempo para el retiro de activos y verificar que se cumplen las devoluciones;

c) definir cuando sea necesario y apropiado, registrar los activos se retiran del sitio y cuando se hace su devolución;

d) documentar la identidad, el rol y la filiación de cualquiera que maneje o use activos, y devolver esta documentación con el equipo, la información y el software.

A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones

Nivel de Cumplimiento **20 /100**

Evidencia:

Se nombra en la política de la seguridad de la información ítem 20 SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES

PERO no se han establecido procedimientos o mecanismos de control

Recomendación:

Establecer una política con las directrices para proteger los equipos fuera de las instalaciones:

a) establecer que los equipos y medios retirados de las instalaciones no se deben dejar sin vigilancia en lugares públicos;

b) seguir en todo momento las instrucciones del fabricante para proteger los equipos, (contra exposición a campos electromagnéticos fuertes);

c) controlar los lugares fuera de las instalaciones, tales como trabajo en la casa, teletrabajo y sitios temporales se deben determinar mediante una valoración de riesgos y se deben aplicar los controles adecuados según sean apropiados, (gabinetes de archivo con llave, política de escritorio limpio, controles de acceso para computadores y comunicación segura con la oficina);

d) establecer que cuando el equipo que se encuentra afuera de las instalaciones es transferido entre diferentes individuos y partes externas, llevar un registro que defina la cadena de custodia para el equipo, que incluya al menos los nombres y las organizaciones de los responsables del equipo.

A.11.2.7 Disposición segura o reutilización de equipos

Nivel de Cumplimiento **0 /100**

Evidencia:

No existe política

Recomendación:

Crear una política con las directrices del proceso de borrado de discos y de encriptación del disco (para evitar la divulgación de la información confidencial cuando se dispone del equipo o se le da un destino diferente, siempre y cuando):

a) establecer que el proceso de encriptación sea suficientemente fuerte y abarque todo el disco (incluido el espacio perdido, archivos temporales de intercambio, etc.);

b) definir que las llaves de encriptación sean lo suficientemente largas para resistir ataques de fuerza bruta;

c) establecer que las llaves de encriptación se mantengan confidenciales.

A.11.2.8 Equipos de usuario desatendidos

Nivel de Cumplimiento **60 /100**

Evidencia:

Se nombra en la política de la seguridad de la información ítem 34 BLOQUEO DE SESION, ESCRITORIO Y PANTALLA LIMPIA

Recomendación:

Continuar con el control. Y hacer auditoría para saber la efectividad del mismo.

A.11.2.9 Política de escritorio limpio y pantalla limpia

Nivel de Cumplimiento **60 /100**

Evidencia:

Se nombra en la política de la seguridad de la información ítem 34 BLOQUEO DE SESION, ESCRITORIO Y PANTALLA LIMPIA

Recomendación:

Continuar con el control. Y hacer auditoría para saber la efectividad del mismo.

A.12 SEGURIDAD DE LAS OPERACIONES

A.12.1.1. Procedimientos de operación documentados

Nivel de Cumplimiento **20 /100**

Evidencia:

Se evidencia que no existe procedimientos documentados.

Cabe resaltar que los procedimientos operativos deben quedar documentados con instrucciones detalladas, teniendo en cuenta el procesamiento y manejo de información, instrucciones para el manejo de errores, contactos de soporte en caso de dificultades técnicas u operativas inesperadas, así como instrucciones para el manejo de medios y exposición de resultados especiales y de carácter confidencial.

Recomendación:

Revisar o implementar, en caso de no existir, los procedimientos de operación con instrucciones operacionales, que incluyen:

a) instalar y configurar sistemas;

b) establecer el procesamiento y manejo de información, tanto automático como manual;

c) establecer la gestión de las copias de respaldo;

d) definir los requisitos de programación, incluidas las interdependencias con otros sistemas, los tiempos de finalización del primer y último trabajos;

e) establecer las instrucciones para manejo de errores u otras condiciones excepcionales que podrían surgir durante la ejecución del trabajo, incluidas las restricciones sobre el uso de sistemas utilitarios;

f) definir contactos de apoyo y de una instancia superior, incluidos los contactos de soporte externo, en el caso de dificultades operacionales o técnicas inesperadas;

g) establecer las instrucciones sobre manejo de medios y elementos de salida, tales como el uso de papelería especial o la gestión de elementos de salida confidenciales, incluidos procedimientos para la disposición segura de elementos de salida de trabajos fallidos;

h) definir los procedimientos de reinicio y recuperación del sistema para uso en el caso de falla del sistema;

i) definir la gestión de la información de rastros de auditoria y de información del log del sistema;

j) establecer los procedimientos de seguimiento.

A.12.1.2. Gestión de cambios

Nivel de Cumplimiento **60 /100**

Evidencia:

Se evidencia que se usan los documentos:

PROCEDIMIENTO: GESTION DEL CAMBIO EN INFORMÁTICA CÓDIGO: GT-UNIN-PR-01

Se tiene Formato, el cual no está oficializado por calidad, el formato: Formato de RFC

Recomendación:

Continuar con el control. Y hacer auditoría para saber la efectividad del mismo. Formalizar el Formato RFC

A.12.1.3. Gestión de capacidad

Nivel de Cumplimiento **40 /100**

Evidencia:

Se evidencia que utilizan los documentos :

PROCEDIMIENTO: GESTION TECNOLÓGICA -INCO CÓDIGO: GT-INCO-PR-02

PROCEDIMIENTO: ADMINISTRACION DE BASES DE DATOS CÓDIGO: GT-UNIN-PR-02

Recomendación:

Revisar o implementar, en caso de no existir, los procedimientos detallados para la gestión de la demanda de capacidad, que incluyen:

a) Eliminar datos obsoletos (espacio en disco).

b) realizar cierre definitivo de aplicaciones, sistemas, bases de datos o ambientes.

c) optimizar cronogramas y procesos de lotes.

d) optimizar las consultas de bases de datos o lógicas de las aplicaciones.

e) realizar una negación o restricción de ancho de banda a servicios ávidos de recursos, si estos no son críticos para el negocio (por ejemplo, video en tiempo real).

A.12.1.4. Separación de los ambientes de desarrollo, pruebas y operación

Nivel de Cumplimiento **60 /100**

Evidencia:

Se cumple con INCO, para la generación de los ambientes de trabajo (hypervisores) . Se cumple por medio del Marco de Referencia V1.0 Sistemas de Información en el LINEAMIENTO de Ambientes independientes en el ciclo de vida de los sistemas de información - LI.SIS.11 (MINTIC)

GEAM cumple al definir y documentar las reglas para la transferencia de software del estatus de desarrollo al de operaciones.

GEAM cumple al establecer que el software de desarrollo y de operaciones debe funcionar en diferentes sistemas o procesadores de computador y en diferentes dominios o directorios.

Recomendación:

Desarrollar los procedimientos para la separación de ambientes, que incluyen:

a) definir y documentar las reglas para la transferencia de software del estatus de desarrollo al de operaciones.

b) establecer que el software de desarrollo y de operaciones debe funcionar en diferentes sistemas o procesadores de computador y en diferentes dominios o directorios.

c) definir que los cambios en los sistemas operativos y aplicaciones se deben probar en un entorno de pruebas antes de aplicarlos a los sistemas operacionales.

d) definir que solo en circunstancias excepcionales, las pruebas no se deben llevar a cabo en los sistemas operacionales.

e) establecer que los compiladores, editores y otras herramientas de desarrollo o utilitarios del sistema no debe ser accesibles desde sistemas operacionales cuando no se requiere.

f) establecer que los usuarios deben usar diferentes perfiles de usuario para sistemas operacionales y de pruebas, y los menús deben desplegar mensajes de identificación apropiados para reducir el riesgo de error.

g) definir que los datos sensibles no se deben copiar en el ambiente del sistema de pruebas, a menos que se suministren controles equivalentes para el sistema de pruebas

A.12.2.1. Controles contra códigos maliciosos

Nivel de Cumplimiento **40 /100**

Evidencia:

Se evidencia las siguientes directrices:

a) Existe la circular y los controles que prohíba el uso de software no autorizado;

b) Existen los controles para evitar o detectar el uso de software no autorizado (listas blancas de aplicaciones);

c) Existen los controles web para evitar o detectar el uso de sitios web malicioso o que se sospecha que lo son (listas negras);

d)Existe la política formal, que se debe actualizar, para proteger contra riesgos asociados con la obtención de archivos y de software ya sea mediante redes externas o cualquier otro medio, indicando qué medidas externas se deben tomar;

e) No existe medio de la gestión de la vulnerabilidad técnica para reducir las vulnerabilidades de las que pueda aprovecharse el software malicioso.

f) No se llevan a cabo revisiones regulares del software y del contenido de datos de los sistemas que apoyan los procesos críticos del negocio; se debería investigar formalmente la presencia de archivos no aprobados o de enmiendas no autorizadas;

g) Existen controles técnicos como una medida para evitar la instalación y actualización de software de detección y reparación del software malicioso en los computadores y medios en forma rutinaria; el análisis realizado debería incluir:

1) Existen los controles con el fin de realizar el análisis de cualquier archivo recibido por la red o por cualquier forma de medio de almacenamiento, para detectar el software malicioso, antes de uso;

2) Existen los controles con el fin de realizar el análisis de los adjuntos y descargas de los correos electrónicos, para determinación del software malicioso antes de uso; este análisis se debería llevar a cabo en diferentes lugares, (los servidores de los correos electrónicos, en los computadores de escritorio) y cuando se ingresar a la red de la organización; el análisis de páginas web, para determinar el software malicioso;

h) No hay definido procedimientos y responsabilidades relacionadas con la protección contra el software malicioso en los sistemas, formación acerca del uso de dichos procedimientos, reporte y recuperación de ataques de software malicioso;

i) Hay un DRT, no aprobado, con los planes de continuidad del negocio apropiados, para la recuperación de ataques de software malicioso, incluidos todos los datos necesarios, copias de respaldo del software y disposiciones para recuperación;

j) Existe la suscripción y los controles implementados para recolectar información en forma regular, (la suscripción a listas de correos o la verificación de sitios web que suministran información acerca de nuevo software malicioso);

k) Existe la suscripción y los controles implementados para verificar información relacionada con el software malicioso, y asegurarse de que los boletines de advertencia sean exactos e informativos;

l) alistar entornos en donde se pueden obtener impactos catastróficos. No se entendió la pregunta

Recomendación:

Revisar y cumplir las siguientes directrices:

e) No existe medio de la gestión de la vulnerabilidad técnica para reducir las vulnerabilidades de las que pueda aprovecharse el software malicioso.

f) No se llevan a cabo revisiones regulares del software y del contenido de datos de los sistemas que apoyan los procesos críticos del negocio; se debería investigar formalmente la presencia de archivos no aprobados o de enmiendas no autorizadas;

h) No hay definido procedimientos y responsabilidades relacionadas con la protección contra el software malicioso en los sistemas, formación acerca del uso de dichos procedimientos, reporte y recuperación de ataques de software malicioso;

l) alistar entornos en donde se pueden obtener impactos catastróficos. No se entendió la pregunta

A.12.3.1. Respaldo de la información

Nivel de Cumplimiento **40 /100**

Evidencia:

Se evidencia que:

Se hacen los respaldos, pero no se encuentran documentados.

Se está realizando la implementación de una nueva herramienta para la ejecución automática de esta tarea.

Recomendación:

Creación de una Política con las siguientes directrices:

a) producir registros exactos y completos de las copias de respaldo, y procedimientos de restauración documentados.

b) establecer la cobertura (copias de respaldo completas o diferenciales) y la frecuencia con que se hagan las copias de respaldo debe reflejar los requisitos del negocio de la organización, los requisitos de la seguridad de la información involucrada, y la criticidad de la información para la operación continua de la organización.

c) definir las copias de respaldo se debe almacenar en un lugar remoto, a una distancia suficiente que permita escapar de cualquier daño que pueda ocurrir en el sitio principal.

d) establecer la información de respaldo y un nivel apropiado de protección física y del entorno, de coherencia con las normas aplicadas en el sitio principal.

e) definir los medios de respaldo se debe poner a prueba regularmente para asegurar que se puede depender de ellos para uso de emergencia en caso necesario; esto se debería combinar con una prueba de los procedimientos de restauración, y se debe verificar contra el tiempo de restauración requerido.

f) definir las situaciones en las que la confidencialidad tiene importancia, las copias de respaldo deben estar protegidas por medio de encriptación.

A.12.4.1. Registro de eventos

Nivel de Cumplimiento **20 /100**

Evidencia:

No se realiza a pesar que existe un procedimiento de GESTIÓN TECNOLÓGICA INCO GT-INCO-PR-02, donde la Actividad 2 se especifica Revisar el Log de eventos y analizar los errores y/o alertas que se reflejan para tomar las acciones correctivas correspondientes. En la actividad 5 Revisar los Log y reportes establecidos en los Firewall y Servidor de Antivirus, con el fin de Monitorear que las políticas definidas funcionan de manera adecuada.

Recomendación:

Revisar o crear, en caso de no existir, un procedimiento de Revisión los registros de eventos que incluyan:

a) identificar los usuarios.

b) establecer las actividades del sistema.

c) definir las fechas, horas y detalles de los eventos clave, (entrada y salida).

d) identificar el dispositivo o ubicación, si es posible, e identificador del sistema.

e) tener registros de intentos de acceso al sistema exitosos y rechazados.

e) definir registros de datos exitosos y rechazados y otros intentos de acceso a recursos.

g) establecer los cambios a la configuración del sistema.

h) definir el uso de privilegios.

i) establecer el uso de utilitarios y aplicaciones del sistema;

j) definir los archivos a los que se tuvo acceso, y el tipo de acceso.

k) establecer las direcciones y protocolos de red.

l) definir las alarmas accionadas por el sistema de control de acceso.

m) activar y desactivar los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusión.

A.12.4.2. Protección de la información de registro

Nivel de Cumplimiento **20 /100**

Evidencia:

Está establecido en el PROCEDIMIENTO: GESTION TECNOLÓGICA -INCO CÓDIGO: GT-INCO-PR-02 . Actividad 5. Pero no se realiza.

Recomendación:

Revisar o crear, en caso de no existir, una Política donde se incluya los procedimientos de revisión y controles dirigidos a proteger contra cambios no autorizados de la información del registro y contra problemas con la instalación de registro, que incluya:

a) verificar todas las alteraciones a los tipos de mensaje que se registran.

b) establecer los archivos log que son editados o eliminados.

c) verificar cuando se excede la capacidad de almacenamiento del medio de archivo log, lo que da como resultado falla en el registro de eventos, o sobre escritura de eventos pasados registrados.

A.12.4.3. Registros del administrador y del operador

Nivel de Cumplimiento **20 /100**

Evidencia:

Está establecido en el PROCEDIMIENTO: GESTION TECNOLÓGICA -INCO CÓDIGO: GT-INCO-PR-02 . Actividad 5. Pero no se realiza.

Recomendación:
Revisar o crear, en caso de no existir, un procedimiento donde se revisen los registros de las actividades del administrador y del operador del sistema, los registros se deben proteger y revisar con regularidad.

A.12.4.4. Sincronización de relojes

Nivel de Cumplimiento **60 /100**

Evidencia:

Se realiza contra el Directorio Activo.

Recomendación:

Crear un procedimiento donde se detalle las actividades que se realizan para hacer esta tarea. También se debe determinar los periodos de tiempo en los cuales se realiza esta sincronización.

A.12.5.1. Instalación de software en sistemas operativos

Nivel de Cumplimiento **40 /100**

Evidencia:

Se evidencia que se utiliza el siguiente documento:

PROCEDIMIENTO: GESTION TECNOLÓGICA -INCO CÓDIGO: GT-INCO-PR-02 Actividad 2

Pero en este documento no se detalla las actividades.

Recomendación:

Revisar o Establecer, en caso de no existir, una política con las siguientes directrices para control de software operacional:

a) actualizar el software operacional, aplicaciones y bibliotecas de programas solo la debe llevar a cabo administradores entrenados, con autorización apropiada de la dirección;

b) definir que los sistemas operacionales sólo deben contener códigos ejecutables aprobados, no el código de desarrollo o compiladores;

c) establecer que las aplicaciones y el software del sistema operativo solo se debe implementar después de pruebas extensas y exitosas; los ensayos deben abarcar la usabilidad, la seguridad, los efectos sobre otros sistemas y la facilidad de uso, y se debe llevar a cabo en sistemas separados; se debe asegurar que todas las bibliotecas de fuentes de programas correspondientes hayan sido actualizadas;

d) usar un sistema de control de la configuración para mantener el control de todo el software implementado, al igual que la documentación del sistema;

e) establecer una estrategia de retroceso (rollback) antes de implementar los cambios;

f) mantener un log de auditoría de todas las actualizaciones de las bibliotecas de programas operacionales;

g) definir las versiones anteriores del software de aplicación se deben conservar como una medida de contingencia;

h) establecer que las versiones de software anteriores se deben llevar al archivo permanente, junto con toda la información y parámetros, procedimientos, detalles de configuración y software de soporte anteriores, en tanto los datos permanezcan en el archivo permanente.

A.12.6.1. Gestión de las vulnerabilidades técnicas

Nivel de Cumplimiento **40 /100**

Evidencia:

Revisar las siguientes directrices para vulnerabilidades técnicas:

a) definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad, la colocación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida; **SE TIENEN LOS ROLES, PERO SE DEBEN ACTUALIZAR LAS FUNCIONES EN EL MANUAL DE FUNCIONES**

b) definir los recursos de información que se usarán para identificar las vulnerabilidades técnicas pertinentes y para mantener la toma de conciencia acerca de ellos se debe identificar para el software y otra tecnología; **NO SE TIENE FORMALIZADO**

c) una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas pertinentes potencialmente; **NO SE TIENE**

d) establecer que una vez que se haya identificado una vulnerabilidad técnica potencial, la organización debería identificar los riesgos asociados y las acciones por tomar; esta acción puede involucrar la colocación de parches de sistemas vulnerables o la aplicación de otros controles; Si no es posible colocar controles se deben documentar en los riesgos de acuerdo a su probabilidad e impacto y colocarlo como riesgo aceptado. **NO SE TIENE FORMALIZADO**

e) definir dependiendo de la urgencia con la que se necesite tratar una vulnerabilidad técnica, la acción tomada se debería llevar a cabo de acuerdo con los controles relacionados con la gestión de cambios, o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información; **NO SE TIENE FORMALIZADO**

f) establecer, si está disponible un parche de una fuente legítima, se debe valorar los riesgos asociados con la instalación del parche (los riesgos que acarrea la vulnerabilidad se debe comparar con el riesgo de instalar el parche); **NO SE TIENE**

g) establecer que los parches se deben probar y evaluar antes de su instalación, para asegurarse de que son eficaces y no producen efectos secundarios que no se puedan tolerar; si no hay parches disponibles, se debe considerar otros controles como: **NO SE TIENE FORMALIZADO**

1) dejar de operar los servicios o capacidades relacionados con la vulnerabilidad;

2) adaptar o adicionar controles de acceso, (cortafuegos, en los límites de la red);

3) incrementar el seguimiento para detectar ataques reales;

4) tomar conciencia sobre la vulnerabilidad;

h) llevar un log de auditoría para todos los procedimientos realizados; **NO SE TIENE FORMALIZADO**

i) hacer seguimiento y evaluación regulares del proceso de gestión de vulnerabilidad técnica, con el fin de asegurar su eficacia y eficiencia; **NO SE TIENE**

j) abordar primero los sistemas que están en alto riesgo; **NO SE TIENE FORMALIZADO**

k) establecer un proceso de gestión eficaz de la vulnerabilidad técnica alineada con las actividades de gestión de incidentes para comunicar los datos sobre vulnerabilidades a la función de respuesta a incidentes y suministrar los procedimientos técnicos para realizarse si llegara a ocurrir un incidente; **NO SE TIENE**

l) definir un procedimiento para hacer frente a una situación en la que se ha identificado una vulnerabilidad, pero no hay una contramedida adecuada. En esta situación, la organización debería evaluar los riesgos relacionados con la vulnerabilidad conocida y definir las acciones de detección y correctivas apropiadas. **NO SE TIENE**

Recomendación:

Revisar o crear, en caso de no existir, una política que contenga las siguientes directrices para vulnerabilidades técnicas:

a) definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad, la colocación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida;

b) definir los recursos de información que se usarán para identificar las vulnerabilidades técnicas pertinentes y para mantener la toma de conciencia acerca de ellos se debe identificar para el software y otra tecnología;

c) una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas pertinentes potencialmente;

d) establecer que una vez que se haya identificado una vulnerabilidad técnica potencial, la organización debería identificar los riesgos asociados y las acciones por tomar; esta acción puede involucrar la colocación de parches de sistemas vulnerables o la aplicación de otros controles; Si no es posible colocar controles se deben documentar en los riesgos de acuerdo a su probabilidad e impacto y colocarlo como riesgo aceptado.

e) definir dependiendo de la urgencia con la que se necesite tratar una vulnerabilidad técnica, la acción tomada se debería llevar a cabo de acuerdo con los controles relacionados con la gestión de cambios, o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información;

f) establecer, si está disponible un parche de una fuente legítima, se debe valorar los riesgos asociados con la instalación del parche (los riesgos que acarrea la vulnerabilidad se debe comparar con el riesgo de instalar el parche);

g) establecer que los parches se deben probar y evaluar antes de su instalación, para asegurarse de que son eficaces y no producen efectos secundarios que no se puedan tolerar; si no hay parches disponibles, se debe considerar otros controles como:

1) dejar de operar los servicios o capacidades relacionados con la vulnerabilidad;

2) adaptar o adicionar controles de acceso, (cortafuegos, en los límites de la red);

3) incrementar el seguimiento para detectar ataques reales;

4) tomar conciencia sobre la vulnerabilidad;

h) llevar un log de auditoría para todos los procedimientos realizados;

i) hacer seguimiento y evaluación regulares del proceso de gestión de vulnerabilidad técnica, con el fin de asegurar su eficacia y eficiencia;

j) abordar primero los sistemas que están en alto riesgo;

k) establecer un proceso de gestión eficaz de la vulnerabilidad técnica alineada con las actividades de gestión de incidentes para comunicar los datos sobre vulnerabilidades a la función de respuesta a incidentes y suministrar los procedimientos técnicos para realizarse si llegara a ocurrir un incidente;

l) definir un procedimiento para hacer frente a una situación en la que se ha identificado una vulnerabilidad, pero no hay una contramedida adecuada. En esta situación, la organización debería evaluar los riesgos relacionados con la vulnerabilidad conocida y definir las acciones de detección y correctivas apropiadas.

A.12.6.2. Restricciones sobre la instalación de software

Nivel de Cumplimiento **60 /100**

Evidencia:

Se evidencia que se cumple, en la plataforma de Windows y además está inmerso en la política de seguridad informática ítem 13.7 Uso de recursos tecnológicos - sub ítem a.

Recomendación:

Continuar con el control. Y hacer auditoría para saber la efectividad del mismo.

A.12.7.1. Controles sobre auditorías de sistemas de información

Nivel de Cumplimiento **0 /100**

Evidencia:

Se evidencia que no se cumple o no existe una política al respecto.

Recomendación:

Crear una política con las siguientes directrices para las auditorias de sistemas de información:

a) establecer los requisitos de auditoría para acceso a sistemas y a datos se debe acordar con la dirección apropiada;

b) definir el alcance de las pruebas técnicas de auditoría se debe acordar y controlar;

c) establecer las pruebas de auditoría se debe limitar a acceso a software y datos únicamente para lectura;

d) definir el acceso diferente al de solo lectura solamente se debe prever para copias aisladas de los archivos del sistema, que se deben borrar una vez que la auditoría haya finalizado, o se debe proporcionar información apropiada si hay obligación de mantener estos archivos bajo los requisitos de documentación de auditoría;

e) definir los requisitos para procesos especiales y adicionales se debe identificar y acordar;

f) establecer las pruebas de auditoría que puedan afectar la disponibilidad del sistema se deben realizar fuera de horas laborales;

g) hacer seguimiento de todos los accesos y logged para producir un rastro de referencia.

A.13 SEGURIDAD DE LAS COMUNICACIONES

A.13.1.1 Controles de redes

Nivel de Cumplimiento **40 /100**

Evidencia:

Se evidencia que se utiliza el documento:

PROCEDIMIENTO: GESTION TECNOLÓGICA -INCO CÓDIGO: GT-INCO-PR-02.

Pero en este documento no se detalla el paso a paso de las actividades.

Recomendación:

Revisar o crear, en caso de no existir, una política con las siguientes directrices para la gestión de seguridad de redes.

a) establecer las responsabilidades y procedimientos para la gestión de equipos de redes.

b) definir la responsabilidad operacional por las redes se debería separar de las operaciones informáticas, en donde sea apropiado.

c) establecer controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes públicas o sobre redes inalámbricas, y para proteger los sistemas y aplicaciones conectados.

d) De acuerdo a NIST, Gestionar el acceso remoto.

d) aplicar logging y seguimiento adecuados para posibilitar el registro y detección de acciones que pueden afectar, o son pertinentes a la seguridad de la información.

e) definir las actividades de gestión a coordinar estrechamente tanto para optimizar el servicio de la organización, como para asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información.

f) establecer los sistemas en la red que se autenticar.

g) restringir la conexión de los sistemas a la red.

A.13.1.2 Seguridad de los servicios de red

Nivel de Cumplimiento **40 /100**

Evidencia:

Se evidencia que se utiliza el documento:

PROCEDIMIENTO: GESTION TECNOLÓGICA -INCO CÓDIGO: GT-INCO-PR-02.

Pero en este documento no se detalla el paso a paso de las actividades.

Recomendación:

Revisar o crear, en caso de no existir, una política con las siguientes directrices para la seguridad de los servicios de red:

a) establecer la tecnología aplicada a la seguridad de servicios de red, tales como autenticación, encriptación y controles de conexión de red.

b) definir los parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red.

c) establecer los procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario.

A.13.1.3 Separación en las redes

Nivel de Cumplimiento **40 /100**

Evidencia:

Se evidencia que se utiliza el documento:

PROCEDIMIENTO: GESTION TECNOLÓGICA -INCO CÓDIGO: GT-INCO-PR-02.

Pero en este documento no se detalla el paso a paso de las actividades.

Recomendación:

La ejecución de cualquier actividad asociada con la infraestructura tecnológica para el procesamiento de información, comunicaciones y seguridad informática debe estar soportada por instrucciones o procedimientos operativos documentados, los cuales siempre deben estar a disposición de todos los usuarios que los necesiten para el desarrollo de sus labores.

A.13.2.1 Políticas y procedimientos de transferencia de información

Nivel de Cumplimiento **0 /100**

Evidencia:

Se evidencia que no se cumple o no existe una política al respecto.

Recomendación:

Revisar o crear, en caso de no existir, una política en al cual se contemple lo siguiente:

Se deben mapear los flujos de comunicaciones y datos para poder cumplir con este ítem.

Revisar las siguientes directrices:

a) definir los procedimientos diseñados para proteger la información transferida contra interceptación, copiado, modificación, enrutado y destrucción.

b) definir los procedimientos para la detección de software malicioso y protección contra éste, que puede ser transmitido mediante el uso de comunicaciones electrónicas.

c) definir los procedimientos para proteger información electrónica sensible comunicada que están como adjuntos.

d) establecer la política o directrices que presentan el uso aceptable de las instalaciones de comunicación.

e) definir las responsabilidades del personal, las partes externas y cualquier otro usuario no comprometen a la organización, (por difamación, acoso, suplantación, envío de cadenas, compras no autorizadas, etc.).

f) establecer el uso de técnicas criptográficas, (proteger la confidencialidad, la integridad y la autenticidad de la información).

g) establecer las directrices sobre retención y disposición para toda la correspondencia del negocio, incluidos mensajes, de acuerdo con la legislación y reglamentaciones locales y nacionales.

h) definir los controles y restricciones asociadas con las instalaciones de comunicación, (el reenvío automático de correo electrónico a direcciones de correo externas).

i) brindar asesoría al personal para que tome las precauciones apropiadas acerca de no revelar información confidencial.

j) no dejar mensajes que contengan información confidencial, en las máquinas contestadoras, ya que éstos pueden ser escuchados por personas no autorizadas, almacenados en sistemas comunales o almacenados incorrectamente como resultado de una marcación incorrecta.

k) brindar asesoría al personal acerca de los problemas de usar máquinas o servicios de fax, a saber:

1) acceso no autorizado a almacenes de mensajes built-in para recuperar mensajes.

2) programar las máquinas en forma deliberada o accidental para enviar mensajes a números específicos; enviar documentos y mensajes a un número equivocado, ya sea por marcación errada o por marcar un número almacenado equivocado.

A.13.2.2 Acuerdos sobre transferencia de información

Nivel de Cumplimiento **0 /100**

Evidencia:

Se evidencia que no se cumple o no existe una política al respecto.

Recomendación:

Revisar o crear, en caso de no existir, una política con las siguientes directrices para transferencia segura de la información:

a) establecer las responsabilidades de la dirección para controlar y notificar la transmisión, despacho y recibo;

b) definir los procedimientos para asegurar trazabilidad y no repudio;

c) definir los estándares técnicos mínimos para empaquetado y transmisión;

d) tener certificados de depósito de títulos en garantía;

e) establecer los estándares de identificación de mensajería;

f) definir las responsabilidades y obligaciones en el caso de incidentes de seguridad de la información, tales como pérdidas de datos;

g) establecer el uso de un sistema de etiquetado acordado para información sensible o crítica, que asegure que el significado de la etiqueta se entiende de inmediato, y que la información está protegida apropiadamente;

h) definir las normas técnicas para registro y lectura de información y software;

i) cualquier control especial que se requiera para proteger elementos críticos, tales como criptografía;

j) mantener una cadena de custodia para la información mientras está en tránsito;

k) definir los niveles aceptables de control de acceso.

A.13.2.3 Mensajería electrónica

Nivel de Cumplimiento **40 /100**

Evidencia:

Se evidencia que se utiliza el documento:

PROCEDIMIENTO: GESTION TECNOLÓGICA -INCO CÓDIGO: GT-INCO-PR-02.

Pero en este documento no se detalla el paso a paso de las actividades.

Recomendación:

Revisar o crear, en caso de no existir, una política con las siguientes directrices para mensajería electrónica:

a) definir la protección de mensajes contra acceso no autorizado, modificación o denegación del servicio proporcionales al esquema de clasificación adoptado por la organización;

b) asegurar el direccionamiento y transporte correctos del mensaje.

c) establecer la confiabilidad y disponibilidad del servicio.

d) definir las consideraciones legales, (los requisitos para firmas electrónicas.

e) establecer la obtención de aprobación antes de usar servicios públicos externos como mensajería instantánea, redes sociales o intercambio de información).

f) definir niveles más fuertes de autenticación para control del acceso desde redes accesibles públicamente.

A.13.2.4 Acuerdos de confidencialidad o de no divulgación

Nivel de Cumplimiento **0 /100**

Evidencia:

Se evidencia que existe un acuerdo de confidencialidad en el formato Único de Solicitud de Acceso a las Tecnologías de la Información Cód.: IM-UNIN-FT-02. en este formato la persona solicitante está firmando la solicitud de acceso a la tecnología y a la vez está firmando el acuerdo de confidencialidad el cual viene al respaldo de dicho formato.

Recomendación:

Revisar o crear, en caso de no existir, una política con las siguientes directrices para acuerdos de confidencialidad que se manejan actualmente:

a) definir la información que se va a proteger (información confidencial).

b) determinar la duración esperada de un acuerdo, incluidos los casos en los que podría ser necesario mantener la confidencialidad indefinidamente;

c) establecer las acciones requeridas cuando termina el acuerdo.

d) definir las responsabilidades y acciones de los firmantes para evitar la divulgación no autorizada de información.

e) definir la propiedad de la información, los secretos comerciales y la propiedad intelectual, y cómo esto se relaciona con la protección de información confidencial.

f) definir el uso permitido de información confidencial y los derechos del firmante para usar la información.

g) establecer el derecho a actividades de auditoría y de seguimiento que involucran información confidencial.

h) definir el proceso de notificación y reporte de divulgación no a Revisar o crear, en caso de no existir, una política con las siguientes directrices para acuerdos de confidencialidad que se manejan actualmente:

a) definir la información que se va a proteger (información confidencial).

b) determinar la duración esperada de un acuerdo, incluidos los casos en los que podría ser necesario mantener la confidencialidad indefinidamente.

c) establecer las acciones requeridas cuando termina el acuerdo.

d) definir las responsabilidades y acciones de los firmantes para evitar la divulgación no autorizada de información.

e) definir la propiedad de la información, los secretos comerciales y la propiedad intelectual, y cómo esto se relaciona con la protección de información confidencial.

f) definir el uso permitido de información confidencial y los derechos del firmante para usar la información.

g) establecer el derecho a actividades de auditoría y de seguimiento que involucran información confidencial.

h) definir el proceso de notificación y reporte de divulgación no autorizada o fuga de información confidencial.

i) definir los plazos para que la información sea devuelta o destruida al cesar el acuerdo.

j) establecer las acciones que se espera tomar en caso de violación del acuerdo. utorizada o fuga de información confidencial.

i) definir los plazos para que la información sea devuelta o destruida al cesar el acuerdo.

j) establecer las acciones que se espera tomar en caso de violación del acuerdo.

A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

A.14.1.1 Análisis y especificación de requisitos de seguridad de la información

Nivel de Cumplimiento **20 /100**

Evidencia:

Se evidencia que no se cumple o no existe una política al respecto.

Recomendación:

Revisar o crear, en caso de no existir, una política con las siguientes directrices para análisis y especificaciones de requisitos de seguridad de la información:

a) establecer el nivel de confianza requerido con relación a la identificación declarada de los usuarios, para obtener los requisitos de autenticación de usuario.

b) definir los procesos de suministro de acceso y de autorización para usuarios del negocio, al igual que para usuarios privilegiados o técnicos.

c) informar a los usuarios y operadores sobre sus deberes y responsabilidades.

d) definir las necesidades de protección de activos involucrados, en particular acerca de disponibilidad, confidencialidad, integridad.

e) definir los requisitos obtenidos de los procesos del negocio, tales como los requisitos de ingreso y seguimiento, y de no repudio.

f) establecer los requisitos exigidos por otros controles de seguridad, (interfaces con el ingreso o seguimiento, o los sistemas de detección de fuga de datos).

A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas

Nivel de Cumplimiento **40 /100**

Evidencia:

Se evidencia que se cumple, esto se realiza a través de políticas de control realizadas por el firewall.

Falta documentación.

Recomendación:

Revisar o crear, en caso de no existir, una política con las siguientes directrices para la seguridad de servicios de las aplicaciones en redes públicas:

a) definir el nivel de confianza que cada parte requiere con relación a la identidad declarada por la otra parte, (por medio de autenticación).

b) establecer los procesos de autorización asociados con quien puede aprobar el contenido o expedir o firmar documentos transaccionales clave.

c) asegurar que los socios de comunicación estén completamente informados de sus autorizaciones para suministro o uso del servicio.

d) determinar y cumplir los requisitos para confidencialidad, integridad, prueba de despacho y recibo de documentos clave y el no repudio de los contratos, (asociados con procesos de ofertas y contratos).

e) definir el nivel de confianza requerido en la integridad de los documentos clave.

f) establecer los requisitos de protección de cualquier información confidencial.

g) definir la confidencialidad e integridad de cualquier transacción de pedidos, información de pagos, detalles de la dirección de entrega y confirmación de recibos.

h) definir el grado de verificación apropiado de la información de pago suministrada por un cliente.

i) seleccionar la forma de arreglo de pago más apropiado para protegerse contra fraude.

j) definir el nivel de protección requerido para mantener la confidencialidad e integridad de la información del pedido.

k) evitar la pérdida o duplicación de información de la transacción.

l) definir la responsabilidad civil asociada con cualquier transacción fraudulenta.

m) establecer los requisitos de seguros.

n) De acuerdo a NIST se deben usar mecanismos de chequeo de las integridades para verificar la integridad del software, firmware, e información.

A.14.1.3 Protección de transacciones de los servicios de las aplicaciones

Nivel de Cumplimiento **40 /100**

Evidencia:

Se hace pero no está documentado el proceso

Recomendación:

Revisar o crear, en caso de no existir, una política con las siguientes directrices protección de transacciones de los servicios de las aplicaciones:

a) definir el uso de firmas electrónicas por cada una de las partes involucradas en la transacción;

b) establecer todos los aspectos de la transacción, es decir, asegurar que:

1) definir la información de autenticación secreta de usuario, de todas las partes, se valide y verifique;

2) definir a transacción permanezca confidencial;

3) mantener la privacidad asociada con todas las partes involucradas;

c) definir la trayectoria de las comunicaciones entre todas las partes involucradas esté encriptada;

d) definir los protocolos usados para comunicarse entre todas las partes involucradas estén asegurados;

e) asegurar que el almacenamiento de los detalles de la transacción esté afuera de cualquier entorno accesible públicamente, (en una plataforma de almacenamiento existente en la intranet de la organización, y no retenido ni expuesto en un medio de almacenamiento accesible directamente desde Internet);

f) utilizar una autoridad confiable (para los propósitos de emitir y mantener firmas digitales o certificados digitales), la seguridad está integrada e incluida en todo el proceso de gestión de certificados/firmas de un extremo a otro.

A.14.2.1 Política de desarrollo seguro

Nivel de Cumplimiento **40 /100**

Evidencia:

Revisar las siguientes directrices política de desarrollo seguro:

a) definir la seguridad del ambiente de desarrollo; **EL AMBIENTE DE DESARROLLO SE ENCUENTRA AISLADO A NIVEL DE INFRAESTRUCTURA EN UNA VLAN INDEPENDIENTE**

b) orientar la seguridad en el ciclo de vida de desarrollo del software:

1) definir la seguridad en la metodología de desarrollo de software; **FALTA DOCUMENTAR**

2) establecer las directrices de codificación seguras para cada lenguaje de programación usado; **NO SE APLICA EN LA ENTIDAD**

c) definir los requisitos de seguridad en la fase diseño; **NO SE APLICA EN LA ENTIDAD**

d) definir los puntos de chequeo de seguridad dentro de los hitos del proyecto; **NO SE APLICA EN LA ENTIDAD**

e) establecer los depósitos seguros; **SE TIENE COPIAS SEGURAS, PERO NO ESTÁ DEFINIDO EL REPOSITORIO (FALTA DOCUMENTACIÓN)**

f) definir la seguridad en el control de la versión**; SI SE REALIZA, EL DESARROLLADOR ENVÍA LA ACTUALIZACIÓN A LA UNIN, Y LA UNIN LO PONE EN PRODUCCIÓN**

g) establecer el conocimiento requerido sobre seguridad de la aplicación; **NO ESTÁ ESTABLECIDO**

h) definir la capacidad de los desarrolladores para evitar, encontrar y resolver las vulnerabilidades. **NO SE HACE**

Recomendación:

Revisar o crear, en caso de no existir, una política con las siguientes directrices de desarrollo seguro:

a) definir la seguridad del ambiente de desarrollo;

b) orientar la seguridad en el ciclo de vida de desarrollo del software:

1) definir la seguridad en la metodología de desarrollo de software;

2) establecer las directrices de codificación seguras para cada lenguaje de programación usado;

c) definir los requisitos de seguridad en la fase diseño;

d) definir los puntos de chequeo de seguridad dentro de los hitos del proyecto;

e) establecer los depósitos seguros;

f) definir la seguridad en el control de la versión;

g) establecer el conocimiento requerido sobre seguridad de la aplicación;

h) definir la capacidad de los desarrolladores para evitar, encontrar y resolver las vulnerabilidades.

A.14.2.2 Procedimientos de control de cambios en sistemas

Nivel de Cumplimiento **60 /100**

Evidencia:

Se evidencia que se usan los documentos:
PROCEDIMIENTO: GESTION DEL CAMBIO EN INFORMÁTICA CÓDIGO: GT-UNIN-PR-01
Se tiene Formato, el cual no está oficializado por calidad, el formato: Formato de RFC

Recomendación:

Continuar con el control. Y hacer auditoría para saber la efectividad del mismo.

Validar en el PROCEDIMIENTO: GESTION DEL CAMBIO EN INFORMÁTICA CÓDIGO: GT-UNIN-PR-01, que se cumplan las siguientes directrices:

a) llevar un registro de los niveles de autorización acordados;

b) asegurar que los cambios se presenten a los usuarios autorizados;

c) revisar los controles y procedimientos de integridad para asegurar que no se vean comprometidos por los cambios;

d) identificar todo el software, información, entidades de bases de datos y hardware que requieren corrección;

e) identificar y verificar el código crítico de seguridad para minimizar la posibilidad de debilidades de seguridad conocidas;

f) obtener aprobación formal para propuestas detalladas antes de que el trabajo comience;

g) revisar antes de la implementación, asegurar que los usuarios autorizados aceptan los cambios;

h) asegurar que el conjunto de documentación del sistema está actualizado al completar cada cambio, y que la documentación antigua se lleva al archivo permanente, o se dispone de ella;

i) mantener un control de versiones para todas las actualizaciones de software;

j) mantener un rastro de auditoría de todas las solicitudes de cambio;

k) asegurar que la documentación de operación y los procedimientos de los usuarios experimenten los cambios que les permitan seguir siendo apropiados;

l) asegurar que la implementación de los cambios ocurre en el momento correcto y no afecta los procesos de negocio involucrados.

A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación

Nivel de Cumplimiento 60 /100
Evidencia:

Se evidencia que se usan los documentos:

PROCEDIMIENTO: GESTION DEL CAMBIO EN INFORMÁTICA CÓDIGO: GT-UNIN-PR-01
Se tiene Formato, el cual no está oficializado por calidad, el formato: Formato de RFC

Recomendación:

Validar en el PROCEDIMIENTO: GESTION DEL CAMBIO EN INFORMÁTICA CÓDIGO: GT-UNIN-PR-01, que se cumplan las siguientes directrices revisión técnica de las aplicaciones después de cambios en la plataforma de operación:

a) revisar los procedimientos de integridad y control de aplicaciones para asegurar que no estén comprometidos debido a los cambios en las plataformas de operaciones;

b) asegurar que la notificación de los cambios en la plataforma operativa se hace a tiempo para permitir las pruebas y revisiones apropiadas antes de la implementación;

c) asegurar que se hacen cambios apropiados en los planes de continuidad del negocio.

A.14.2.4 Restricciones en los cambios a los paquetes de software

Nivel de Cumplimiento **60 /100**

Evidencia:

Se evidencia que se usan los documentos:

PROCEDIMIENTO: GESTION DEL CAMBIO EN INFORMÁTICA CÓDIGO: GT-UNIN-PR-01
Se tiene Formato, el cual no está oficializado por calidad, el formato: Formato de RFC

Recomendación:

Validar en el PROCEDIMIENTO: GESTION DEL CAMBIO EN INFORMÁTICA CÓDIGO: GT-UNIN-PR-01, que se cumplan las siguientes directrices y/o restricciones en los cambios a los paquetes de software:

a) definir el riesgo de que los procesos de integridad y los controles incluidos se vean comprometidos;

b) obtener el consentimiento del vendedor;

c) obtener del vendedor los cambios requeridos, a medida que se actualiza el programa estándar;

d) evaluar el impacto, si la organización llega a ser responsable del mantenimiento futuro del software como resultado de los cambios;

e) definir la compatibilidad con otro software en uso.

A.14.2.5 Principios de construcción de sistemas seguros

Nivel de Cumplimiento **20 /100**

Evidencia:

No se realiza. Pendiente evidencia

Recomendación:

Revisar la documentación y los principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.

Evidenciar los principios para la construcción de sistemas seguros que se están aplicando.

A.14.2.6 Ambiente de desarrollo seguro

Nivel de Cumplimiento **60 /100**

Evidencia:

Se evidencia que se cumplen las siguientes directrices para ambiente de desarrollo seguro:

a) carácter sensible de los datos que el sistema va a procesar, almacenar y transmitir; SE TIENE A NIVEL DE DB

b) definir los requisitos externos e internos aplicables, (reglamentaciones o políticas); SE REALIZA, PERO NO ESTA DOCUMENTADO

c) definir los controles de seguridad ya implementados por la organización, que brindan soportar al desarrollo del sistema; SE REALIZA, PERO NO ESTA DOCUMENTADO

d) establecer la confiabilidad del personal que trabaja en el ambiente; SE DA CON PERMISO AVALADO POR UN SUPERIOR DE ACUERDO AL FORMATO ESTABLECIDO POR LA UNIN

e) definir el grado de contratación externa asociado con el desarrollo del sistema; EL GRADO ES BAJO.

f) definir la necesidad de separación entre diferentes ambientes de desarrollo; LOS AMIBENTES SON: DESARROLLO, PRUEBAS Y PRODUCCION

g) definir el control de acceso al ambiente de desarrollo; ESTA DEFINIDO, PERO NO ESTA DOCUMENTADO

h) establecer el seguimiento de los cambios en el ambiente y en los códigos almacenados ahí; SOLAMENTE HAY SEGUIMIENTO EN PRODUCCION

i) definir las copias de respaldo se almacenan en lugares seguros fuera del sitio; A NIVEL DEL APLICATIVO DINAMICA Y CONTROLDOC SE TIENE. EL RESTO NO SE TIENE

j) definir el control sobre el movimiento de datos desde y hacia el ambiente. SOLAMENTE HAY CONTROL EN PRODUCCION

Recomendación:

Realizar la documentación respectiva que hace falta para cumplir con el control.

Revisar que se cumplan con las siguientes directrices para ambiente de desarrollo seguro:

a) carácter sensible de los datos que el sistema va a procesar, almacenar y transmitir.

b) definir los requisitos externos e internos aplicables, (reglamentaciones o políticas).

c) definir los controles de seguridad ya implementados por la organización, que brindan soportar al desarrollo del sistema.

d) establecer la confiabilidad del personal que trabaja en el ambiente.

e) definir el grado de contratación externa asociado con el desarrollo del sistema.

f) definir la necesidad de separación entre diferentes ambientes de desarrollo.

g) definir el control de acceso al ambiente de desarrollo;

h) establecer el seguimiento de los cambios en el ambiente y en los códigos almacenados ahí.

i) definir las copias de respaldo se almacenan en lugares seguros fuera del sitio.

j) definir el control sobre el movimiento de datos desde y hacia el ambiente.

A.14.2.7 Desarrollo contratado externamente

Nivel de Cumplimiento **40 /100**

Evidencia:

Revisar las siguientes directrices desarrollo contratado externamente:

a) definir los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente; **POR CONTRATO (ESTA DEFINIDO POR EL ECO-ESTUDIO DE CONVENIENCIA Y OPORTUNIDAD. DONDE SE PLASMA LO QUE SE REQUIRE) O POR INVESTIGACION 8 SE DEFINEN POR MESAS DE TRABAJO - DONDE SE INDICA LOS LINEAMIENTOS).**

b) establecer los requisitos contractuales para prácticas seguras de diseño, codificación y pruebas; **SE HACE, PERO NO SE TIENE DOCUMENTADO**

c) definir el suministro del modelo de amenaza aprobado, al desarrollador externo; **NO SE TIENE**

d) realizar los ensayos de aceptación para determinar la calidad y exactitud de los entregables; POR INVESTIGACION - **DIRECTAMENTE ELLOS HACEN LAS PRUEBAS. LUEGO PASA A LA UNIN DONDE SE DA EL VoBo DE LA APLICACION**

e) definir la evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad; **NO ESTA DEFINIDA**

f) definir la evidencia de que se han hecho pruebas suficientes para proteger contra contenido malicioso intencional y no intencional en el momento de la entrega; **NO ESTA DEFINIDA**

g) definir la evidencia de que se han hecho pruebas suficientes para proteger contra la presencia de vulnerabilidades conocidas; **NO ESTA DEFINIDA**

h) definir los certificados de depósito de títulos en garantía; (el código fuente ya no está disponible); **NO ESTA DEFINIDA**

i) establecer el derecho contractual con relación a procesos y controles de desarrollo de auditorías; **NO ESTA ESATBLECIDO**

j) documentar eficaz del ambiente de construcción usado para crear entregables; **NO ESTA DOCUMENATADO**

k) establecer que la organización es responsable de la conformidad con las leyes aplicables y con la verificación de la eficiencia del control. SI SE REALIZA - ALINEADOS AL MINTIC

Recomendación:

Realizar la documentación respectiva que hace falta para cumplir con el control

Revisar que se cumplan con las siguientes directrices desarrollo contratado externamente:

a) definir los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente;

b) establecer los requisitos contractuales para prácticas seguras de diseño, codificación y pruebas;

c) definir el suministro del modelo de amenaza aprobado, al desarrollador externo;

d) realizar los ensayos de aceptación para determinar la calidad y exactitud de los entregables;

e) definir la evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad;

f) definir la evidencia de que se han hecho pruebas suficientes para proteger contra contenido malicioso intencional y no intencional en el momento de la entrega;

g) definir la evidencia de que se han hecho pruebas suficientes para proteger contra la presencia de vulnerabilidades conocidas;

h) definir los certificados de depósito de títulos en garantía; (el código fuente ya no está disponible);

i) establecer el derecho contractual con relación a procesos y controles de desarrollo de auditorías;

j) documentar eficaz del ambiente de construcción usado para crear entregables;

k) establecer que la organización es responsable de la conformidad con las leyes aplicables y con la verificación de la eficiencia del control.

A.14.2.8 Pruebas de seguridad de sistemas

Nivel de Cumplimiento **0 /100**

Evidencia:

Se indica que no se realizan.

Recomendación:

Durante el desarrollo se debe llevar a cabo pruebas de funcionalidad de la seguridad.

Verifique en una muestra que para pasar a producción los desarrollos se realizan pruebas de seguridad. También verifique que los procesos de detección de incidentes son probados periódicamente.

A.14.2.9 Prueba de aceptación de sistemas

Nivel de Cumplimiento **60 /100**

Evidencia:

Se realizan las pruebas antes de pasarlo a producción.

Recomendación:

Revisar las pruebas de aceptación de sistemas, para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.

A.14.3.1 Protección de datos de prueba

Nivel de Cumplimiento **0 /100**

Evidencia:

No se hace.

Recomendación:

Revisar o crear, en caso de no existir, una política con las siguientes directrices para protección de datos de prueba:

a) establecer los procedimientos de control de acceso, que se aplican a los sistemas de aplicación operacionales, se debe aplicar también a los sistemas de aplicación de pruebas;

b) tener una autorización separada cada vez que se copia información operacional a un ambiente de pruebas;

c) definir que la información operacional se debe borrar del ambiente de pruebas inmediatamente después de finalizar las pruebas;

d) establecer que el copiado y uso de la información operacional se debe logged para suministrar un rastro de auditoría.

A.15 RELACIONES CON LOS PROVEEDORES

A.15.1. Seguridad de la información en las relaciones con los proveedores

Nivel de Cumplimiento **20 /100**

Evidencia:

Se evidencia que se está haciendo pero no existe una política al respecto con los controles ante los diferentes riesgos..

Se nombra de la Política de Seguridad de la Información, en el ítem 11. GESTION DE TERCEROS - Ref: ISO/IEC 27001:2005 CL A.6.2.2

Recomendación:

Revisar o crear, en caso de no existir, una política que cumpla lo siguiente:

1) La política de seguridad de la información para las relaciones con los proveedores, que indique los requisitos de Seguridad Informática para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización, esta política debe reflejarse en los acuerdos con los proveedores que deben estar documentados.

Evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta entre otros los siguientes aspectos:

• El tipo de acceso requerido (físico, lógico y a qué recurso)

• Los motivos para los cuales solicita el acceso

• El valor de la información

• Los controles empleados por la tercera parte

• La incidencia de este acceso en la seguridad de la información de las dependencias o entidades.

2) Verifique en la muestra de proveedores con acceso a los activos de información (no necesariamente son proveedores de tecnología de la información, por ejemplo, pueden ser proveedores que tengan por ejemplo un proceso de nómina en outsourcing), se hayan suscrito acuerdos (ANS) formales donde se establezcan y acuerden todos los requisitos de seguridad de la información pertinentes con cada proveedor.

3) Verifique para los proveedores si se tiene en cuenta los riesgos de SI asociados a la cadena de suministro, por ejemplo, para los proveedores en la nube es muy común que se apoyen en otros proveedores para proporcionar las instalaciones y se deben manejar los riesgos asociados a este tercero con el cual la entidad no tiene una relación comercial directa. Solicite que le indiquen como identifican para cada proveedor su cadena de suministro y obtenga evidencia de este hecho.

A.15.2. Gestión de la prestación de servicios de proveedores

Nivel de Cumplimiento **20 /100**

Evidencia:

Se evidencia que no se cumple o no existe una política al respecto.

Recomendación:

1) Indagar y solicitar evidencia en una muestra de proveedores seleccionada, como la entidad hace seguimiento, revisa y audita con regularidad de acuerdo a la política la prestación de servicios de los proveedores y el cumplimiento de los compromisos respecto a la seguridad de la información.

2) Indagar y evidenciar como se gestionan los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, los incidentes de seguridad de la información y la revaloración de los riesgos.

A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

A.16.1.1 Responsabilidades y procedimientos

Nivel de Cumplimiento 0 /100

Evidencia:

Se evidencia que no se cumple o no existe una política al respecto.

Recomendación:

Revisar o crear, en caso de no existir, una política que contenga las siguientes directrices responsabilidades y procedimientos:

a) establecer las responsabilidades de gestión, para asegurar que los siguientes procedimientos se desarrollan y comunican adecuadamente dentro de la organización:

1) los procedimientos para la planificación y preparación de respuesta a incidentes.

2) los procedimientos para seguimiento, detección, análisis y reporte de eventos e incidentes de seguridad de la información.

3) los procedimientos para logging las actividades de gestión de incidentes.

4) los procedimientos para el manejo de evidencia forense.

5) los procedimientos para la valoración y toma de decisiones sobre eventos de seguridad de la información y la valoración de debilidades de seguridad de la información.

6) los procedimientos para respuesta, incluyendo aquellos para llevar el asunto a una instancia superior, recuperación controlada de un incidente y comunicación a personas u organizaciones internas y externas.

b) establecer los procedimientos para asegurar que:

1) el personal competente maneje las cuestiones relacionadas con incidentes de seguridad de la información dentro de la organización.

2) se implemente un punto de contacto para la detección y reporte de incidentes de seguridad.

3) se mantengan contactos apropiados con las autoridades, grupos de interés o foros externos que manejen las cuestiones relacionadas con incidentes de seguridad de la información.

c) definir el reporte de procedimientos debería incluir:

1) la preparación de formatos de reporte de eventos de seguridad de la información para apoyar la acción de reporte y ayudar a la persona que reporta a recordar todas las acciones necesarias en caso de un evento de seguridad de la información.

2) el procedimiento que se va a seguir en el caso de un evento de seguridad de la información, (tomar nota inmediatamente de todos los detalles, tales como el tipo de no conformidad o violación, mal funcionamiento, mensajes en la pantalla y reporte inmediato al punto de contacto y realizar solamente acciones coordinadas).

3) referencia a un proceso disciplinario formal establecido para ocuparse de los empleados que cometen violaciones a la seguridad.

4) los procesos de retroalimentación adecuados para asegurar que las personas que reportan eventos de seguridad de la información sean notificadas de los resultados después de que la cuestión haya sido tratada y cerrada.

A.16.1.2. Reporte de eventos de seguridad de la información

Nivel de Cumplimiento 40/100

Evidencia:

Se evidencia que se enuncia en la Política de Seguridad de la Información ítem 39 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIONA.12.6. , sub ítem b.

Recomendación:

Revisar o crear, en caso de no existir, una política con las siguientes directrices de reporte de eventos de seguridad de la información:

a) establecer un control de seguridad ineficaz;

b) definir la violación de la integridad, confidencialidad o expectativas de disponibilidad de la información;

c) definir los errores humanos;

d) definir las no conformidades con políticas o directrices;

e) definir las violaciones de acuerdos de seguridad física;

f) establecer los cambios no controlados en el sistema;

g) definir mal funcionamiento en el software o hardware;

h) definir violaciones de acceso.

A.16.1.3. Reporte de debilidades de seguridad de la información

Nivel de Cumplimiento 40 /100

Evidencia:

Se realiza pero, no se encuentra documentado.

Recomendación:

Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.

Observar si los eventos son reportados de forma consistente en toda la entidad de acuerdo a los criterios establecidos.

A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos

Nivel de Cumplimiento 20/100

Evidencia:

No se realiza.

Se evidencia que se enuncia en la Política de Seguridad de la Información ítem 38 GESTION DE VULNERABILIDADES TECNICAS - Ref: ISO/IEC 27001:2005 CL.

A.12.6. , sub ítem b

Recomendación:

Revisar si los eventos de Seguridad Informática detectados son analizados para determinar si constituyen un incidente de seguridad de la información y entender los objetivos del ataque y sus métodos.

Evidenciar si los incidentes son categorizados y se cuenta con planes de respuesta para cada categoría.

A.16.1.5. Respuesta a incidentes de seguridad de la información

Nivel de Cumplimiento 60 /100

Evidencia:

Están aprobados, pero se deben actualizar.

Recomendación:

Revisar o crear, en caso de no existir, una política con las siguientes directrices para respuesta a incidentes de seguridad de la información:

a) Los incidentes son contenidos y la probabilidad de que vuelvan a ocurrir mitigada.

b) Se debe contar con un plan de recuperación de incidentes durante o después del mismo.

c) recolectar evidencia lo más pronto posible después de que ocurra el incidente.

d) llevar a cabo análisis forense de seguridad de la información, según se requiera

e) llevar el asunto a una instancia superior, según se requiera.

f) asegurar que todas las actividades de respuesta involucradas se registren adecuadamente para análisis posterior.

g) comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o externo a las organizaciones que necesitan saberlo.

h) tratar las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente.

i) establecer que una vez que el incidente se haya tratado lo suficiente, cerrarlo formalmente y hacer un registro de esto.

j) de acuerdo a la NIST se deben investigar las notificaciones de los sistemas de detección.

A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información

Nivel de Cumplimiento 0 /100

Evidencia:

Se evidencia que no se cumple o no existe una política al respecto.

Recomendación:

Documentar los incidentes de seguridad de la información presentados, analizarlos y así entender cuál fue el impacto del incidente. Para que con este conocimiento se pueda reducir la posibilidad o el impacto de incidentes futuros.

A.16.1.7. Recolección de evidencia

Nivel de Cumplimiento 0 /100

Evidencia:

Se evidencia que no se cumple o no existe una política al respecto.

Recomendación:

Definir las siguientes directrices para recolección de evidencia:

a) definir la cadena de custodia.

b) establecer la seguridad de la evidencia.

c) definir la seguridad del personal.

d) definir los roles y responsabilidades del personal involucrado.

e) establecer la competencia del personal.

f) realizar la documentación.

g) definir las sesiones informativas.

A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

A.17.1.1 Planificación de la continuidad de la seguridad de la información

Nivel de Cumplimiento 40 /100

Evidencia:

Se evidencia que se tiene actualmente borrador BCP Y DRP

Recomendación:

Determine si aplica para procesos críticos solamente o se han incluido otros procesos o por lo menos se ha reconocido la necesidad de ampliarlo a otros procesos (para determinar el nivel de madurez)

Evalúe si se ha incluido en estos planes y procedimientos los requisitos de seguridad de la información.

Tenga en cuenta que, en ausencia de una planificación formal de continuidad de negocio y recuperación de desastres, la dirección de seguridad de la información debería suponer que los requisitos de seguridad de la información siguen siendo los mismos en situaciones adversas, en comparación con las condiciones operacionales normales. Como alternativa, una organización puede llevar a cabo un análisis de impacto en el negocio de los aspectos de seguridad de la información, para determinar los requisitos de seguridad de la información aplicables a situaciones adversas.

De acuerdo a la NIST también se deben tener planes de respuesta a incidentes y recuperación de incidentes.

Posteriormente gestionar la revisión y posterior aprobación de los borradores existentes.

A.17.1.2 Implementación de la continuidad de la seguridad de la información

Nivel de Cumplimiento **20 /100**

Evidencia:

Se evidencia que no se cumple o no existe una política al respecto

Recomendación:

Establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.

Validar lo siguiente:

a) Una estructura organizacional adecuada para prepararse, mitigar y responder a un evento contingente, usando personal con la autoridad, experiencia y competencia necesarias.

b) Personal formalmente asignado de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para manejar un incidente y mantener la seguridad de la información.

c) Planes aprobados, procedimientos de respuesta y recuperación documentados, en los que se especifique en detalle como la organización gestionará un evento contingente y mantendrá su seguridad de la información en un límite predeterminado, con base en los objetivos de continuidad de seguridad de la información aprobados por la dirección.

Revisar si los controles de seguridad de la información que se han implementado continúan operando durante un evento contingente. Si los controles de seguridad no están en capacidad de seguir brindando seguridad a la información, se la Entidad debe establecer, implementar y mantener otros controles para mantener un nivel aceptable de seguridad de la información.

A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

Nivel de Cumplimiento 20 /100

Evidencia:

Se evidencia que no se cumple o no existe una política al respecto

Recomendación:

Crear el procedimiento en el cual se incluya la Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

Posteriormente evidenciar la realización de pruebas de la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información, para asegurar que son coherentes con los objetivos de continuidad de la seguridad de la información.

Tenga en cuenta que la verificación de los controles de continuidad de la seguridad de la información es diferente de las pruebas y verificación generales de seguridad de la información. Si es posible, es preferible integrar la verificación de los controles de continuidad de negocio de seguridad de la información con las pruebas de recuperación de desastres y de continuidad de negocio de la organización.

A.17.2.1 Disponibilidad de instalaciones de procesamiento de información.

Nivel de Cumplimiento **40 /100**

Evidencia:

Se evidencia que se cumple:

Si hay redundancia. Se cuenta con 2 Datacenter (Principal - Conteiner y secundario en edificio Principal

Hay redundancia a nivel de:

- Datacenter nivel Eléctrico

- A nivel de Firewall (interno y perimetral)

- A nivel de Base de Datos

- A nivel de Networking (Core y distribución)

- A Nivel de centros de cableado

- A nivel de ISP (ETB Y IFX)

- A nivel de Directorio Activo

Recomendación:

Realizar las pruebas necesarias para asegurar que un componente redundante funciona de la forma prevista durante una emergencia o falla.

Los procedimientos operativos deben quedar documentados con instrucciones detalladas, teniendo en cuenta el procesamiento y manejo de información, instrucciones para el manejo de errores, contactos de soporte en caso de dificultades técnicas u operativas inesperadas, así como instrucciones para el manejo de medios y exposición de resultados especiales y de carácter confidencial.

A.18 CUMPLIMIENTO

A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales.

Nivel de Cumplimiento 80 /100

Evidencia:

Se puede evidenciar que:

Se puede consultar por la página web **https://hospitalmilitar.gov.co**/ -> Módulo transparencia-> 6.1 Política de la seguridad de la información ->ítem 4 referencias normativas.

Existe un Normograma que lo maneja la oficina de jurídica. que se puede consultar página web **https://hospitalmilitar.gov.co**/ -> ítem 4 NORMATIVIDAD ->ITEM 4,7 Normograma 2021 (el cual se puede bajar.)

Recomendación:

Verificar si hay nuevas leyes de cumplimiento que se puedan anexar

A.18.1.2 Derechos de propiedad intelectual.

Nivel de Cumplimiento **80 /100**

Evidencia:

Se puede evidenciar que:

1) Se habla en la política de seguridad de la información en el ítem 13.7 Uso de recursos tecnológicos, sobre el cumplimiento de los requisitos y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.

2) Existe la Circular 03 de febrero 3 de 2015 - Política y Directrices relacionados con el uso del Software.

3) La entidad controla que no se instale software ilegal, dando permisos estándar a los usuarios.

4)Si se tiene una herramienta (LANDSWIPER) la cual tiene un inventario de software instalado y se compara con el número de licencias adquiridas para asegurar que no se incumplen los derechos de propiedad intelectual. Tenga en cuenta los controles que deben existir para asegurar que no se exceda ningún número máximo de usuarios permitido dentro de la licencia.

Recomendación:

Crear los procedimientos para el cumplimiento de los requisitos y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.

A.18.1.3 Protección de registros.

Nivel de Cumplimiento **60/100**

Evidencia:

Se evidencia que se cuentan con las Tablas de Retención Documental que especifican los registros y el periodo por el cual se deberían retener; éstas están aprobadas por el Comité de Gestión y Desempeño .Y se encuentran actualmente pendientes para aprobación por parte del Archivo General de la Nación.

Recomendación:
Verificar las tablas de retención documental que especifiquen los registros y el periodo por el cual se deberían retener, además del almacenamiento, manejo y destrucción. Posibles tipos de registros pueden ser registros contables, registros de bases de datos, logs de transacciones, logs de auditoría y procedimientos operacionales,

los medios de almacenamiento permitidos pueden ser papel, microfichas, medios magnéticos, medios ópticos etc.

A.18.1.4 Protección de los datos y privacidad de la información relacionada con los datos personales.

Nivel de Cumplimiento **40 /100**

Evidencia:

Se puede evidenciar que:

https://intranet.homil.gov.co/recursos_user/Documentos%20Administrativa/Informatica/Politicas%20de%20Seguridad%20Informacion/Politica%20de%20Tratamiento%20de%20Datos%20Personales.pdf

Recomendación:

Verificar que la política cubre todos los temas.

A.18.2.1 Revisión independiente de la seguridad de la información.

Nivel de Cumplimiento **20 /100**

Evidencia:

No se ha hecho nunca revisión la por parte de alguien externo. se tiene contemplado para el año 2022 contratar una persona o firma independiente para realizar esta labor.

Recomendación:

Realizar revisiones independientes (por personas diferentes o no vinculadas a un proceso o área que se revisa), de la conveniencia, la adecuación y la eficacia continuas de la gestionar la seguridad de la información.

A.18.2.2 Cumplimiento con las políticas y normas de seguridad.

Nivel de Cumplimiento **20 /100**

Evidencia:

Se evidencia que se tiene:

PLAN DE ACCION DE AUDITORIAS 2021 programada para el mes de diciembre 2021

Resultados auditoria 2020 Auditoria área gestión de respuesta a requerimientos e incidentes de la Unidad de Informática

Oportunidades de Mejora:

se obtuvo un informe y el plan de mejora el cual se cumplió.

(Informe Auditoria EM-OCIN-PR-01-FT-07 - Operación del área de Gestión de Respuesta a Requerimientos e Incidentes en el primer semestre de 2020 (27/11/2020))

* Hallazgo No. 1: LIMITACION EN EL ALCANCE DE AUDITORIA

* Hallazgo No. 2: INCUMPLIMIENTO DEL PROCEDIMIENTO: GESTIÓN DE INCIDENTES MESA DE AYUDA, CODIGO TIGERE-PR-01

* Hallazgo No. 3: INCUMPLIMIENTO EN LA MEDICION DE NIVELES DE SERVICIO DEL CONTRATO No.048 DE 2020

Plan de Mejora: PM Gestión de Incidentes.xlsx

Hacen auditoria para el tema de derechos de autor cada año.

Informe Auditoria EM-OCIN-PR-01-FT-07 - Operación del área de Gestión de Respuesta a Requerimientos e Incidentes en el primer semestre de 2020.

Recomendación:

Revisar por parte de Control Interno se deben hacer las siguientes actividades:

1) Verificar si los gerentes aseguran que todos los procedimientos de seguridad dentro de su área de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento de las políticas y estándares de seguridad.

2) Verificar la revisión periódica del cumplimiento del centro de cómputo con las políticas y normas de seguridad establecidas.

3) Verificar si los sistemas de información son revisados regularmente para asegurar el cumplimiento de las normas de seguridad de la información.

A.18.2.3 Revisión de cumplimiento técnico.

Nivel de Cumplimiento **20 /100**

Evidencia:

Se evidencia que:

No se realiza, si no cuando hay sospecha de alguna vulnerabilidad.

Recomendación:

Chequear los sistemas de información regularmente para el cumplimiento con los estándares de implementación de la seguridad.

CONCLUSION

Se evidencia que la gran falencia que se presenta en el SGSI es la falta de documentación de políticas y procedimientos de muchas de las actividades que se realizan dentro del HOMIL. Las tareas a seguir son lograr concertar reuniones con las diferentes personas encargadas de las diferentes unidades, coordinar las actividades necesarias para lograr la documentación necesaria; con el fin solucionar los problemas actuales, optimizar los controles actuales y a su vez de mejorar la calificación en el nivel de madurez de los diferentes controles de la Norma ISO/IEC 27001:2013.

APROBACIÓN				
	NOMBRE	**CARGO**	**FECHA**	**FIRMA**
ELABORÓ	**Ing.** Luis Carlos Monroy	Especialista en Seguridad Informática Orden Prestación de Servicios – Unidad de Informática	Enero de 2022	Original Firmado
REVISÓ	**Ing.** Fabio Alvarado	Jefe de Unidad - Unidad de Informática	Enero de 2022	Original Firmado
	TC (RA) Ricardo Arturo Hoyos Lanziano	Subdirector Administrativo	Enero de 2022	Original Firmado
APROBÓ	El presente informe se encuentra aprobado por el Comité Institucional de Gestión y Desempeño (***Acta de Aprobación No 01 del 26 de Enero 2021***)			