ALCALDÍA MAYOR
DE BOGOTÁ D.C.
DESARROLLO ECONÓMICO
Instituto para la Economía Social

IPES

GESTION DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SUBDIRECCIÓN DE DISEÑO Y ANÁLISIS ESTRATÉGICO

PROCESO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS

Bogotá 2018

Elaboró:	Reviso:	Aprobó:
John Jair Garzón Delgado Yamel Orlando Martínez Balaguera	Clarisa Díaz García	Clarisa Díaz García
Profesional Especializado – SDAE CPS 60/2018	Subdirectora de Diseño y Análisis Estratégico	Subdirectora de Diseño y Análisis Estratégico

TABLA DE CONTENIDO

1 INTRODUCCION

El crecimiento de los riesgos de seguridad digital, asociados al uso y masificación de las tecnologías de información y comunicaciones y considerando que la información es un activo esencial para la toma de decisiones encaminadas al cumplimiento de los objetivo y misionalidad el Instituto para la Economía Social - IPES, considera la necesidad de definir, implementar, mantener y mejorar un sistema de gestión de seguridad de la información que le permita contar con niveles apropiados de integridad, confidencialidad y disponibilidad de sus activos de información.

Un componente fundamental desde la planificación del sistema de gestión de seguridad de la información es la definición e implementación de una metodología para la gestión de riesgos de seguridad y privacidad de la información, que permita determinar, valorar y tratar los riesgos asociados a los activos de información institucional.

2 JUSTIFICACION

El desarrollo de la metodología para la gestión de riesgos de seguridad y privacidad de la información permite al Instituto para la Encomia Social – IPES, planear, implementar, mantener y mejorar las acciones encaminadas a proteger los activos de información institucional, a través de herramientas para la identificación de riesgos para prevenir o reducir efectos no deseados, valoración de riesgos a partir de la definición de criterios para la aceptación y valoración que produzcan resultados consistentes, tratamiento de riesgos para determinar acciones y seleccionar controles apropiados teniendo en cuenta la valoración del riesgo.

3 OBJETIVO

Establecer la metodología para la gestión de riesgos de seguridad y privacidad de la información en el Instituto para la Economía Social – IPES, para prevenir o reducir efectos indeseados, lograr la mejora continua, valorar y tratar los riesgos, sus consecuencias potenciales y la probabilidad de ocurrencia.

4 ALCANCE

Aplica para la identificación, clasificación, análisis, evaluación, control y valoración de los riesgos de seguridad de la información en la entidad, este instructivo complementa al instructivo IN-004 “ELABORACIÓN MATRIZ MAPA DE RIESGOS”, en lo referente a la identificación de riesgos de seguridad y privacidad de la información.

5 RESPONSABILIDADES

La Subdirección de Diseño y Análisis Estratégico como responsable de liderar el desarrollo e implementación del Sistema Integrado de Gestión se encargará de revisar y adecuar la metodología de administración de riesgos propuesta por el DAFP a las

necesidades del IPES, también brindará la asesoría y las herramientas a los procesos para su correcta elaboración

El equipo de la SDAE SISTEMAS será el encargado de brindar acompañamiento en el desarrollo e implementación del componente de Administración del Riesgo, este deberá recoger iniciativas, responsabilidades y armonizar los diferentes ejercicios para la implementación de un proceso de Administración del Riesgo más efectivo.

El equipo del SIG se encargará recoger iniciativas, responsabilidades y armonizar los diferentes ejercicios para la implementación de la metodología de Administración del Riesgo, a través de los referentes de los diferentes procesos serán los encargados de diligenciar la Matriz Mapa de Riesgos con el fin de elaborar el mapa de riesgos de una manera simplificada, así como del seguimiento.

El equipo de seguimiento y evaluación está conformado por el/la Asesor/a de Control Interno, los servidores públicos y contratistas de su oficina asesora, quienes velarán por la adecuada elaboración e implementación del mapa de riesgos de cada proceso, promoviendo su apropiación, entendimiento y evaluación del mismo.

6 CONDICIONES GENERALES

- Cumplimiento de la Política de Administración de Riesgos de Seguridad y Privacidad de la Información de la Entidad.
- Utilizar la metodología propuesta por el Departamento Administrativo de la Función Pública “Guía de Administración de Riesgos 7”.
- Utilizar la Herramienta “Matriz Mapa de Riesgos” para la elaboración del Mapa de Riesgos.
    - Utilizar el instructivo “Gestión de riesgos de seguridad de la información”
- Implementación de mecanismos reales para la Administración de Riesgos de Seguridad de la Información en el IPES.

7 DEFINICIONES

1. **Activo:** Cualquier cosa que pueda ser de valor para la entidad. Nota. Algunos tipos de activos incluyen, pero no se limitan a:
    - Información.
    - Software.
    - Recursos físicos.
    - Servicios.

- Personas y sus cualificaciones, habilidades y experiencias.
- Elementos intangibles como la reputación y la imagen.

2. **Activo de Información:** Conocimiento o datos que son de valor para la entidad. Ver modelo estándar de control interno para el Estado Colombiano, MECI 1000:2005, Numeral 2.2 Componente Información

3. **Amenaza:** Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema o la entidad.

4. **Causas:** (Amenaza o Vulnerabilidad): Aquello que se considera como fundamento u origen de algo.

5. **Confidencialidad:** Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados

6. **Consecuencia:** resultado, efecto o impacto de un riesgo o un evento.

7. **Control:** Proceso, política, dispositivo, practica u otra acción existente que actúa para minimizar un riesgo negativo o potenciar oportunidades positivas.

8. **Control correctivo:** Es el control que se realiza para eliminar la (s) causa (s) de una no conformidad detectada u otra situación indeseable.

9. **Control preventivo:** Es el control que se realiza para eliminar la (s) causa (s) de una no conformidad potencial u otra situación potencialmente indeseable.

10. **Disponibilidad:** propiedad de que la información sea accesible y utilizable por solicitud de un individuo, entidad o proceso autorizado.

11. **Evento de seguridad de la información:** Ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha en el cumplimiento de la política de seguridad de la información, falla de un control de seguridad de la información o una condición no identificada con anterioridad que puede ser relevante para la seguridad de la información.

12. **Evaluación del Riesgo:** Proceso utilizado para determinar las prioridades de la administración del riesgo, comparando el nivel de un determinado riesgo con respecto a un estándar determinado, es decir, calificar el riesgo de acuerdo a su impacto con respecto a la probabilidad.

13. **Frecuencia:** es el número de veces que se repite un evento o un hecho en el tiempo.

14. **Identificación del Riesgo:** Proceso para determinar las causas internas y/o externas (debido a…), evento (lo que puede suceder…riesgo) y la consecuencia (lo que podría ocasionar que…).

15. **Impacto:** Efecto positivo o negativo producido por un acontecimiento, evento o riesgo.

16. **Incidente de seguridad de la información:** Un evento o serie de eventos de seguridad de la información que tiene una probabilidad significativa de comprometer las operaciones de la entidad y amenazar la seguridad de la información.

17. **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.

18. **Monitorear:** Comprobar, supervisar, observar o registrar la forma que se lleva a cabo una actividad con el fin de identificar posibles cambios.

19. **Probabilidad:** Cualidad de probable, que puede suceder.

20. **Riesgo de seguridad de la información:** Potencialidad de que una amenaza puede explotar una vulnerabilidad de un activo o grupo de activos y en consecuencia cause daño a la entidad.

21. **Riesgo Residual:** Riesgo remanente después de la implementación del tratamiento del riesgo.

22. **Valoración del Riesgo:** Es el producto de confrontar los resultados de la evaluación del riesgo con los controles identificados en el elemento de control.

Tipos de Riesgos:

- **Riesgo Estratégico:** Se asocia con la forma en que se administra la entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

- **Riesgos Operativos:** Comprende los riesgos relacionados tanto con la parte operativa como con la técnica de la entidad, incluye riesgos provenientes de deficiencias en los sistemas de información, en la definición de los procesos y la ejecución de los procedimientos en la estructura de la entidad, la desarticulación entre dependencias, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.

- **Riesgos Financieros:** Se relacionan con el manejo de los recursos de la entidad, que incluye la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes de cada entidad. De la eficiencia y transparencia en el manejo de los recursos, así como de su interacción con las demás áreas, dependerá en gran parte el éxito o fracaso de toda entidad.

- **Riesgos de Cumplimiento:** Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

- **Riesgos de Conocimiento:** son aquellos que se relacionan con el daño generado por la pérdida de conocimiento e información vital para el desarrollo de las actividades de la entidad y organismo distrital. En esta clasificación se encuentran los riesgos en los activos y la seguridad de la información.

- **Riesgos Normativos:** son aquellos que se relacionan tanto con los daños generados por la violación de una prescripción u obligación legal, incumplimientos a políticas internas, como con la volatilidad normativa.

  Dentro de este tipo se pueden agrupar los incumplimientos a obligaciones tributarias, a tiempos en la presentación de estados financieros a solicitudes de información y demás incumplimientos legales aplicables.

  Riesgos de Tecnología: Se asocian con la capacidad de la entidad para que la tecnología disponible satisfaga sus necesidades actuales, futuras y soporte el cumplimiento de la misión.

23. **Seguridad de la información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información. Además puede involucrar otras propiedades como como: autenticidad, trazabilidad, no repudio y fiabilidad.

24. **Vulnerabilidad:** Debilidad de un activo o un control que puede ser explotada por una amenaza.

8 DESARROLLO

A continuación se describen las actividades que se desarrollan para realizar la identificación y valoración de los riesgos de seguridad y privacidad de la información.

Una vez se han identificado y valorado los riesgos de seguridad de la información, los resultados se consolidan utilizando el instructivo “IN-004 APLICACIÓN DE LA METODOLOGIA GESTIÓN DE RIESGO OPERATIVO” para generar la “Matriz Mapa de Riesgos” del IPES

8.1 Identificación de los riesgos

8.1.1 Determinar el proceso al cual se le va a realizar el análisis de riesgos

La evaluación de riesgos de seguridad y privacidad de la información debe iniciar con la identificación y selección del proceso a evaluar, es necesario contar con la mayor cantidad posible de información del proceso a evaluar como: descripción del proceso, procedimientos que lo componen, instructivos y cualquier documentación que ayude a entender el alcance y características del proceso.

1. El proceso o activo seleccionado para evaluación se documenta en el campo 1. Dominio/Proceso de la “Matriz Mapa de Riesgos”.

2. Colocar el objetivo del Proceso en el campo 2. de la “Matriz Mapa de Riesgos”.

Identificar los activos que apoyan el proceso seleccionado

Se considera como activo cualquier cosa que tiene valor para la entidad, se debe tener en cuenta que los procesos se apoyan en sistemas de información que además de software y hardware también están compuestos por documentos (registros, instrucciones de trabajo, procedimientos), personas (responsables de actividades en el proceso o administradores de componentes de tecnología) y directrices que guían el proceso en sí mismo.

Del proceso de identificación de activos resulta un inventario de activos de información con un responsable identificado del activo. Los activos se usan para identificar los riesgos de seguridad de la información.

8.1.2 Clasificar los riesgos

Una vez que se ha descrito el evento de riesgo en términos de causa, evento y consecuencia se deben clasificar de acuerdo con la lista aprobada por el sistema integrado de gestión del IPES:

- Estratégico.
- Operativo.
- Financiero.
- Normativo.
- Tecnológico.
- Conocimiento.
- Ambiental y de salud ocupacional.

Es importante aclarar que los riesgos de seguridad de la información no son necesariamente tecnológicos, existen riesgos de seguridad de la información que también pueden ser de tipo normativo, operativo, estratégico o de conocimiento.

8.1.3 Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas

Se considera como vulnerabilidad una debilidad en un activo o un control que puede ser explotada (aprovechada) por una amenaza. La identificación de vulnerabilidades sobre los activos se realiza con pruebas técnicas o auditorias (pruebas con herramientas de software, pruebas de ingeniería social o herramientas de auditoría como la inspección y la observación) de cumplimiento de la fortaleza del activo o el control. Las fuentes de información en donde se pueden detectar vulnerabilidades que pueden afectar a los sistemas de información incluyen:

- Documentación de los procesos y procedimientos
- Rutinas de administración de activos
- Personal responsable de la administración de los activos
- Información de la configuración de equipos y sistemas
- Evaluación del entorno físico y lógico del activo

Para la evaluación de la existencia de vulnerabilidades se debe considerar la existencia o no de controles en el activo y la calidad de los controles implementados. La existencia de una vulnerabilidad no implica automáticamente la existencia de un riesgo, es necesario que exista una amenaza que esté en capacidad de aprovechar la vulnerabilidad.

En el anexo B de este documento encuentra una lista de posibles vulnerabilidades que pueden afectar a los activos de información del IPES.

Las vulnerabilidades también se deben considerar como causas de riesgos y se pueden diligenciar en el campo 4 de la matriz Mapa Riesgos. Las vulnerabilidades se registran como amenazas internas.

8.1.4 Identificar las amenazas que pueden afectar a los activos

Se considera como amenaza (causa) cualquier agente externo al activo que puede aprovechar una vulnerabilidad del mismo para causar daño y que afectará la seguridad de la información. La identificación de amenazas se realiza mediante la evaluación de fuentes de información como:

- Experiencia de los dueños de los activos que se están evaluando
- Experiencia de especialistas externos
- Bases de datos públicas sobre amenazas de seguridad de la información
- Reportes de listas de interés en seguridad de la información

- Recomendaciones de las normas ISO 27005:2009, NTC-GP 1000, MECI
- Experiencia de los administradores del SGSI mediante el tratamiento de incidentes de seguridad

En el anexo A de este documento encuentra una lista de posibles amenazas que pueden afectar a los activos de información del IPES

- Las amenazas se consideran como causas externos y se pueden diligenciar en el campo 4 de matriz mapa de riesgos.

8.1.5 Identificar los Eventos

Los eventos son las situaciones que se generan a partir de la combinación de una amenaza y una vulnerabilidad. Para describir el evento se usa el METALENGUAJE de la herramienta “Matriz Mapa de Riesgos” el cual está en la hoja del mismo nombre.

Para describir el evento, tome un activo del proceso que está en análisis y describa en términos del metalenguaje, que ocurre con el activo si la amenaza aprovecha la vulnerabilidad.

8.1.6 Identificar las Consecuencias

Las consecuencias son los hechos que se derivan del evento identificado. A nivel de los riesgos de la seguridad de la información, las consecuencias se describen en términos de los tres componentes de la seguridad de la información:

Pérdida de Disponibilidad

Pérdida de Integridad

Pérdida de Confidencialidad

Las consecuencias se diligencian en el campo 6 de la “Matriz Mapa de Riesgos”

8.1.7 Identificar los impactos

En primera instancia se debe calcular el valor del activo afectado para luego determinar el impacto del riesgo sobre el activo.

8.1.8 Calcular el valor del activo

El valor del activo se calcula como la suma de los valores de confidencialidad, integridad y disponibilidad usando las siguientes tablas.

Valoración de la Confidencialidad del activo

Valor del activo	Descripción
4	Activos con información clasificada como de CARÁCTER RESERVADO
3	Activos con información clasificada como de ACCESO CONTROLADO
2	Activos con información clasificada como de APOYO
1	Activos con información considerada como de DOMINIO PÚBLICO

Valoración de la Integridad del activo

Valor del activo	Descripción
5	Activos con información oficial que no se pueden alterar bajo ninguna condición
1	Activos con información que aún no es oficial y aún están en proceso de elaboración

Valoración de la Disponibilidad del activo

Valor del activo	Descripción
3	El activo debe estar siempre disponible en el momento en que se necesite
2	El uso del activo puede esperar un tiempo que define el usuario y no se puede modificar ese tiempo de espera
1	El uso del activo puede esperar un tiempo que puede modificar el usuario

- **Valor del activo=** Suma de Confidencialidad, Integridad y Disponibilidad

8.1.9 Calcular el impacto

El cálculo del impacto se realiza usando la tabla siguiente

IMPACTO

Valor	Concepto	Descripción
1	INSIGNIFICANTE	Cuando el valor del activo afectado esta entre 3 y 4
2	MENOR	Cuando el valor del activo afectado esta entre 5 y 6
3	MODERADO	Cuando el valor del activo afectado esta entre 7 y 8
4	MAYOR	Cuando el valor del activo afectado esta entre 9 y 10
5	CATASTROFICO	Cuando el valor del activo afectado esta entre 11 y 12

El valor del impacto identificado se diligencia en la columna 7 “Impacto”

8.1.10 Valorar la posibilidad de ocurrencia (probabilidad)

El cálculo de la probabilidad de ocurrencia se realiza usando la siguiente tabla

DETERMINACIÓN OBJETIVA DE LA PROBABILIDAD		
Valor	**Concepto**	**Descripción**
1	Raro	Puede ocurrir solo en circunstancias excepcionales.
2	Improbable	Pudo ocurrir en algún momento.
3	Moderado (Posible)	Podría ocurrir en algún momento.
4	Probable	Probablemente ocurrirá en la mayoría de las Circunstancias.
5	Casi	Se espera que ocurra en la mayoría de las Circunstancias.
	Certeza	

La probabilidad asignada al riesgo se registra en el campo 8 de la Matriz Mapa de riesgos.

8.1.11 Identificación de controles existentes

Se considera como control un proceso, política, dispositivo, practica u otra acción existente que actúa para minimizar el riesgo negativo o potenciar oportunidades positivas. La identificación de controles existentes de seguridad de la información considera los controles recomendados por la norma técnica Colombiana NTC ISO /IEC 27001:2013. Para realizar la identificación de controles existente se pueden seguir las siguientes actividades:

- Revisar la documentación existente que contiene información sobre los controles implementados a nivel de los procesos de la entidad.

- Indagar con los responsables de los activos la existencia real y correcto funcionamiento de los controles descritos en la documentación.

- Realizar revisiones detalladas de la existencia de controles de seguridad de la información usando listas de verificación de controles de seguridad de la información como ISO 27001:2013 y buenas prácticas de auditoria.

- Revisar los resultados de las evaluaciones de seguridad de la información realizadas.

La norma NTC ISO/IEC 27001:2013 contiene una lista de 114 controles recomendados para la seguridad de la información.

En el instrumento Matriz Mapa de Riesgos, la columna 10 permite el registro de los controles existentes

Para diligenciar el campo 10. Controles existentes, la información debe ser diligenciada en la hoja CONTROLES, teniendo en cuenta las siguientes observaciones:

a) Los riesgos se deben diligenciar en el mismo orden que aparecen en la hoja MATRIZ existan o no controles para estos.

b) Diligenciar el control existente.

c) Si existen controles indicar si es correctivo, preventivo o los dos

d) Si se diligencian controles, es necesario llenar todos los campos de la columna valoración, es decir, si se aplica el control, si es efectivo, si está documentado y si este disminuye el impacto, la probabilidad o ambos; en caso contrario dejar la columna Valoración en blanco.

8.1.12 Estimar los niveles de riesgo

1. Una vez diligenciados los campos 7 y 8, la matriz automáticamente ingresa los datos correspondiente al campo 9. Evaluación (ver hoja MAPEO de la herramienta “Matriz Mapa de Riesgos”).

2. La nueva valoración automáticamente aparecerá en la columna 11. Valoración del riesgo en la hoja MATRIZ, si no existen controles dejara la misma valoración obtenida en la evaluación.

3. En la columna 12. Opciones de Manejo la matriz automáticamente ingresará las opciones de acuerdo a su valoración (ver hoja MAPEO de la herramienta “Matriz Mapa de Riesgos”).

4. En la columna 13. Acciones, cada proceso definirá que acciones o como aplicará las opciones de manejo del riesgo que permitirán prevenir o reducir éste.

5. La columna 14. Responsables: corresponde a las dependencias o áreas que intervienen en el proceso, encargadas de adelantar las acciones propuestas.

6. Columna 15. Cronograma: corresponde a las fechas establecidas por los responsables de cada proceso, para implementar las acciones por parte del grupo de trabajo.

7. Columna 16. Indicadores: establecer indicadores de eficacia, impacto o los dos con el fin de realizar control y seguimiento a las acciones implementadas.

8.1.13 Priorización de riesgos a nivel de procesos

Una vez estimados los niveles de riesgo, se ordenan y se seleccionan aquellos que presentan el nivel más alto para ser consolidados en la herramienta “Matriz Mapa de Riesgos a nivel institucional” del Sistema Integrado de gestión del IPES, es decir a la matriz consolidada de riesgos del SIG se llevan los riesgos que presentan niveles más altos y que deben ser supervisados por el Sistema Integrado de Gestión del IPES.

Los riesgos que presenten niveles bajos son administrados internamente por los responsables de los procesos.

9 ANEXOS

Anexo A: Lista de amenazas a la seguridad de la información

Tipo de amenaza	Amenazas
Daños físicos	Fuego
	Daños por agua
	Polución
	Destrucción de equipo o medios
	Polvo, Corrosión, Congelamiento
Eventos naturales	Fenómeno climático
	Fenómeno símico
	Fenómeno volcánico
	Inundación
Perdida de servicios esenciales	Falla de aire acondicionado
	Falla de suministro de agua
	Falla de energía eléctrica
	Falla de equipo de comunicaciones
Perturbaciones por radiación	Electromagnetismo
	Radiación térmica
	Pulso electrónico
Información comprometida	Interceptación de señal

	Espionaje remoto
	Escucha secreta (espionaje telefónico)
	Robo de medios
	Robo de documentos
	Robo de equipos
	Recuperación de basura
	Recuperación de medios descartados

Tipo de amenaza	**Amenazas**
	Revelación de información
	Datos de fuentes no confiables
	Modificación de hardware con fines criminales
	Modificación de software con fines criminales
Fallas técnicas	Falla de equipo
	Funcionamiento deficiente de equipo
	Saturación de sistema
	Funcionamiento deficiente de software
	Falla en el mantenimiento de sistema
Acciones no autorizadas	Uso no autorizado de equipo
	Copia fraudulenta de software
	Copia fraudulenta de datos
	Corrupción de datos
	Procesamiento ilegal de datos
Compromiso de funciones	Error en uso
	Abuso de privilegios
	Olvido de privilegios
	Denegación de acciones
	Brecha en disponibilidad de personal
Amenaza informática humana	Hacker, Cracker
	Cibercrimen
	Terrorismo
	Espionaje industrial
	Infiltrados

Anexo B: Lista de vulnerabilidades que puede afectar a los activos de información

Tipo	**Vulnerabilidad**
Hardware	Falta o ausencia de mantenimiento
	Ausencia de programa de reemplazo de partes
	Susceptibilidad de polvo, humedad, barro
	Sensibilidad a campo electromagnético
	Ausencia de sistema eficiente de control de cambios
	Susceptibilidad a cambios de temperatura
	Bodegas desprotegidas

Tipo	Vulnerabilidad
	Ausencia de procedimiento de destrucción de medios
	Copias no controladas
Software	Ausencia de procesos detallados de pruebas
	Fallas conocidas en el software
	Sesiones abiertas sin usuario presente
	Reúso de medios sin procedimiento de borrado seguro
	Ausencia de pistas de auditoría
	Incorrecta asignación de privilegios
	Distribución masiva de software
	Interfaces de usuario complejas
	Ausencia de documentación
	Parámetros incorrectos de configuración
	Fechas incorrectas
	Ausencia de mecanismos para identificación y autenticación de usuarios
	Tablas de claves desprotegidas
	Servicios innecesarios habilitados
	Gestión deficiente de claves
	Software inmaduro
	Especificaciones incompletas, incorrectas o no documentadas para desarrolladores
	Ausencia de proceso efectivo de control de cambios
	Uso no controlado de software descargado
	Ausencia de copias de respaldo
	Ausencia de protecciones físicas en puertas y ventanas
	Ausencia de reportes de gestión
Redes	Ausencia de prueba de envío o recepción de mensaje
	Líneas de comunicación desprotegidas
	Tráfico de datos sensibles no protegido
	Cableado deficiente
	Puntos únicos de falla
	Ausencia de identificación de transmisor y receptor
	Infraestructura de red insegura
	Transmisión de claves sin protección
Tipo	**Vulnerabilidad**
	Inadecuada gestión de elementos de red
	Conexiones a redes públicas desprotegidas
Personal	Ausencia de personal
	Procedimientos de selección de personal deficientes
	Entrenamiento en seguridad de la información deficiente o insuficiente
	Ausencia de conciencia en seguridad de la información
	Ausencia de mecanismos de monitoreo de personal
	Ausencia de políticas de uso correcto de activos de información
	Uso deficiente de controles de acceso a sedes
	Ubicación en una sede susceptible a inundación

Tipo	Vulnerabilidad
Sedes	Redes eléctricas inestables
	Ausencia de protecciones físicas en sedes
Organización	Ausencia de procedimientos formales para registro y eliminación de usuarios
	Ausencia de procedimientos formales para revisión de privilegios
	Ausencia de cláusulas sobre seguridad de la información en contratos con terceros
	Ausencia de procedimientos formales para supervisar el procesamiento de información
	Ausencia de auditorías regulares de seguridad de la información
	Ausencia de procedimientos efectivos para gestión de riesgos
	Ausencia de procedimientos para revisión de registros de auditoría
	Inadecuados tiempos de respuesta para servicios de mantenimiento
	Acuerdo de niveles de servicio desactualizados
	Ausencia de procedimientos para control de Información
	Ausencia de procedimientos para la revisión de la seguridad
	Ausencia de procedimientos para clasificación de información
	Ausencia de responsabilidades sobre la seguridad de la información
	Planes de continuidad desactualizados
	Ausencia de procedimientos para el control de paso a producción de software
	Ausencia de cláusulas sobre la seguridad de la información en los contratos de funcionarios
	Políticas de seguridad de la información desactualizadas

10 CONTROL DE CAMBIOS

VERSIÓN	FECHA	ÍTEM MODIFICADO	DESCRIPCIÓN DEL CAMBIO

11 REFERENCIAS BIBLIOGRAFICAS

a) Instituto Colombiano de Normas Técnicas- ICONTEC Norma Técnica Colombiana NTC-ISO/IEC27002- 2013

b) Instituto Colombiano de Normas Técnicas- ICONTEC Norma Técnica Colombiana NTC-ISO/IEC27001- 2013

c) Consejo Nacional de Política Económica y Social –Política de Seguridad Digital CONPES 3854 – 2016

d) Departamento Administrativo de la Función Publica - Guía para la Administración de Riesgos – Versión 3 de 2014

e) IN-004 “ELABORACIÓN MATRIZ MAPA DE RIESGOS

f) Seguridad y Privacidad de la Información – Guía de Gestión de Riesgos