


	INFORME DE AUDITORÍA Y SEGUIMIENTO	Código: EC-PR-002-FR-004	
	Macroproceso: Evaluación y Control	Versión: 03	
	Proceso: Gestión de Evaluación y Control	Fecha de Aprobación: 05/12/2022	

Consecutivo No.	32	Fecha de Emisión del Informe	Día	9	Mes	9	Año	2024
-----------------	----	------------------------------	-----	---	-----	---	-----	------

**SEGUIMIENTO A LA IMPLEMENTACIÓN DEL SUBSISTEMA DE SEGURIDAD DE LA INFORMACIÓN - UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS**

<b>Proceso/Dependencia:</b>	Subsistema de Seguridad de la Información	<b>Líder:</b>	Rectoría
		<b>Responsable:</b>	Secretaría General.
<b>Objetivo:</b>	Realizar seguimiento a la implementación del Subsistema de Gestión de Seguridad de la Información, con el propósito de verificar el nivel de avance del mismo.		
<b>Alcance:</b>	Evaluar el Subsistema de Seguridad de la Información de la Universidad Distrital Francisco José de Caldas, para la vigencia 2023 y 2024		
<b>Criterios:</b>	<ul style="list-style-type: none"> <li>• <u>Resolución 632 de 2015</u> “Por la cual se crea el Subsistema de Gestión de Seguridad de la Información SGSI de la Universidad Distrital Francisco José de Caldas”.</li> <li>• <u>Resolución 163 del 2019</u> “Por la cual se ajusta el Sistema Integrado de Gestión de la Universidad Distrito/ Francisco José de Caldas -SIGUD, e implementa el Modelo Integrado de Planeación y Gestión - MIPG, como su Marco de Referencia...”</li> <li>• <u>Resolución 678 del 2011</u> “Por la cual se adopta la política para de seguridad de la información de la Universidad Distrital y se otorgan funciones en relación con esta al Comité de Informática y Telecomunicaciones”.</li> <li>• <u>Resolución 297 del 2019</u> “Por la cual se reglamenta el funcionamiento y operativización de los Equipos Técnicos de Gestión y Desempeño Institucional, ...”</li> <li>• <u>Resolución 581 del 2022</u> “Por la cual se adopta el plan indicativo para el periodo 2022-2025 de la Universidad...”</li> <li>• <u>Mapa de Riesgos</u> Universidad Distrital Francisco José de Caldas</li> <li>• Plan Estratégico de las Tecnologías de la Información y las Comunicaciones <u>PETIC 2019-2023</u></li> <li>• Modelo de Seguridad y Privacidad de la Información <u>MSPi</u> de MINTIC</li> </ul>		

	INFORME DE AUDITORÍA Y SEGUIMIENTO	Código: EC-PR-002-FR-004	
	Macroproceso: Evaluación y Control	Versión: 03	
	Proceso: Gestión de Evaluación y Control	Fecha de Aprobación: 05/12/2022	

Muestra (opcional):	N/A
<b>1. ASPECTOS GENERALES:</b>	

Para entrar en contexto y lograr mayor comprensión del documento es necesario hacer claridad en algunos conceptos técnicos que son relevantes con el objetivo y alcance de la auditoría:

### **Seguridad de la Información:**

Se entiende por seguridad de la información al conjunto de medidas, tácticas, técnicas y procedimientos tanto preventivos como reactivos implementados en una entidad u organización, con la finalidad de controlar y resguardar todos los datos e información crítica, valiosa y sensible almacenada y tratada dentro de la misma.

### **Privacidad de la Información:**

Se deben identificar con claridad la tipología de los datos para hacer uso adecuado de los mismos,



- **Datos Abiertos:** Son los datos que están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, (Ley 1712 de 2014, art 6)
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos:** Es el dato que no es privado o sensible. Son considerados datos públicos los relativos al estado civil de las personas, su profesión u oficio y a su calidad de comerciante o de servidor público. (Decreto 1377 de 2013, art 3)
- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- **Datos Personales Sensibles:** Son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos (Decreto 1377 de 2013, art 3)

### **MSPI – Modelo de Seguridad y Privacidad de la Información**

Es un documento de lineamiento de buenas prácticas elaborado por MinTIC (Ministerio de Tecnologías de la Información y las Comunicaciones), el cual contempla su operación en el ciclo **PHVA** (Planear, Hacer, Verificar y Actuar), al igual que establece los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento con el fin de contribuir en el desarrollo del plan estratégico institucional y del plan estratégico de tecnologías de la información y las comunicaciones al interior de las entidades.

### **Activos Tecnológicos y/o Informáticos:**

Se considera cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos

	INFORME DE AUDITORÍA Y SEGUIMIENTO	Código: EC-PR-002-FR-004	
	Macroproceso: Evaluación y Control	Versión: 03	
	Proceso: Gestión de Evaluación y Control	Fecha de Aprobación: 05/12/2022	

informáticos, personal humano, soportes físicos de información, redes de comunicación, servicios de nube, equipamiento auxiliar o instalaciones.



## 2. DESARROLLO DE LA AUDITORIA

Dentro de los activos de toda organización la información es uno de los activos mas importantes y relevantes ya que es transversal en todas las actividades de la entidad, por lo que se hace necesario implementar políticas, procedimientos, protocolos, controles y demás estrategias con el objetivo de minimizar los riesgos y vulnerabilidades que presentan los sistemas informáticos que afecten la **Confidencialidad, Integridad y Disponibilidad** tanto de la información como del mismo sistema en todos los elementos que lo conforman.

Estas estrategias administrativas deben estar articuladas con los objetivos misiones y estratégicos, a la vez que hacen parte esencial del plan de desarrollo, del plan indicadito y del plan operativo de la Universidad; por otra parte, deben estar alineadas con las políticas y objetivos de la Gestión de Calidad en su Modelo de Operación por Procesos el cual establece 4 macroprocesos y 22 procesos e implementa a su vez el Sistema Integrado de Gestión de la Universidad Distrital (SIGUD)



Figura 1 – <http://planeacion.udistrital.edu.co:8080/sigud/s/sgsi> - 27/08/2024

	INFORME DE AUDITORÍA Y SEGUIMIENTO	Código: EC-PR-002-FR-004	
	Macroproceso: Evaluación y Control	Versión: 03	
	Proceso: Gestión de Evaluación y Control	Fecha de Aprobación: 05/12/2022	

## 2.1 Modelo de Seguridad y Privacidad de la Información - MSPI

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos de sector tecnológico, y definió la estrategia de **Gobierno en Línea**, con el fin de contribuir con la construcción de un Estado más participativo, eficiente y transparente. Y es por ello que elaboro el MSPI, el cual conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo y establece el ciclo de funcionamiento del modelo de seguridad en 5 fases:

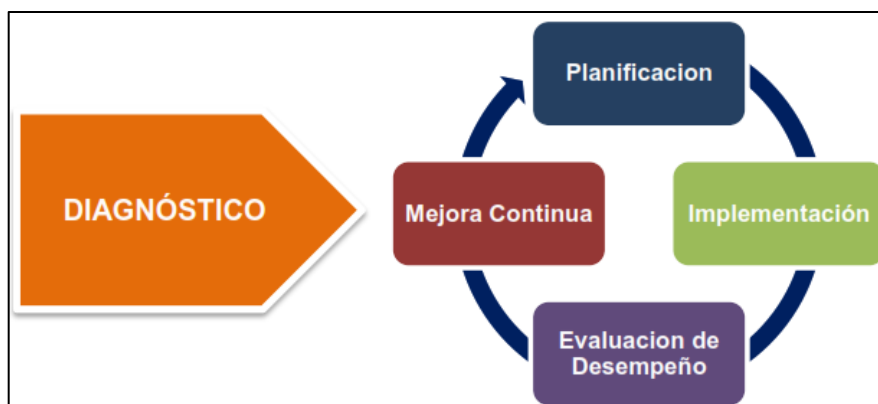




Figura 2 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

Tomado el objetivo y alcance de la presente auditoria nos centraremos en las 3 fases iniciales que son:

- Fase de Diagnóstico: el objetivo es identificar el estado actual y nivel de madurez de la entidad respecto a la adopción del MSPI,
- Fase de Planificación: Determina las necesidades y objetivos de seguridad y privacidad de la información según el mapa de procesos, el tamaño y el contexto interno y externo de la entidad.
- Fase de Implementación: Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información.

## 2.2 FASE DE DIAGNOSTICO – NIVEL DE MADUREZ E INFORME DE BRECHAS

Se tomo como punto de referencia los ejes transformadores del [PLAN IDICATIVO 2022-2025](#). Con el fin de tener un lineamiento estratégico que garantice transparencia y acciones efectivas en la transformación que proyecta la Universidad Distrital FJC a nivel TIC



	INFORME DE AUDITORÍA Y SEGUIMIENTO	Código: EC-PR-002-FR-004	
	Macroproceso: Evaluación y Control	Versión: 03	
	Proceso: Gestión de Evaluación y Control	Fecha de Aprobación: 05/12/2022	

Esta fase de diagnóstico proyecta una metodología basada en pruebas, consiste en recopilar la información necesaria que permita identificar los activos tecnológicos asociados a los procesos, de igual forma debe dar a conocer el contexto estratégico de la entidad; una vez realizadas las pruebas y análisis a determinados elementos y conceptos propuestos por el mismo modelo se logran identificar los riesgos, vulnerabilidades y debilidades del actual sistema logrando así determinar el nivel de madurez y la brecha en la implementación del sistema de seguridad de acuerdo al objetivo y alcance propuesto del mismo

Una vez aplicada la metodología mencionada en el actual sistema de seguridad de la información de la Universidad, se evaluaron 42 elementos principales los cuales se segmentaron en elementos de Dirección- Gestión y en elementos de Infraestructura Tecnológica

Elemento	ITEMS EVALUADO	Ítems Cumplidos		Ítems No Cumplidos		% Cumplimiento
		Totalmente	Parcialmente	No implementado	No Aplica	
1 Objetivos de seguridad de la información	11	10	0	1	0	91%
2 Principios política general	12	12	0	0	0	100%
3 Recomendaciones política general.	11	9	0	2	0	82%
4 Implementación política general	10	5	1	3	1	55%
5 Políticas específicas recomendadas para la implementación de controles de seguridad de la información	21	4	0	17	0	19%
6 Procedimientos de seguridad de la información.	22	11	1	10	0	52%
7 Indicadores de gestión para la seguridad de la información.	16	5	4	7	0	44%
8 Integrantes del equipo de gestión MSPI	8	3	1	4	0	44%
9 Integrantes comité de seguridad de la información.	9	6	0	3	0	67%
10 Actores que intervienen y conforman el proceso de atención de Incidentes.	5	4	0	1	0	80%
11 Equipo de trabajo IPv6	5	4	0	1	0	80%
12 Roles y perfiles atención de incidentes.	6	3	1	1	1	58%
13 Actividades de gestión del riesgo del MSPI.	7	0	7	0	0	50%
14 Actividades de gestión del riesgo transición IPv4 a IPv6	4	0	0	4	0	0%
15 Marco Continuidad del Negocio	12	0	8	4	0	33%
16 Auditoría del MSPI.	7	3	0	4	0	43%
17 Métricas de seguridad según el MEMSI.	12	8	0	4	0	67%
18 Actividades Evaluación del desempeño del MSPI.	16	0	7	9	0	22%
19 Documentación Evaluación del Desempeño MSPI.	8	0	3	5	0	19%
20 Documentación Mejora Continua MSPI	4	0	1	3	0	13%
21 Lineamientos terminales de áreas financieras MSPI.	28	22	0	6	0	79%
22 Fases plan de sensibilización, capacitación y comunicación.	4	1	0	3	0	25%
23 Elementos plan de capacitación y sensibilización.	11	9	2	0	0	91%
24 Presupuesto plan de capacitaciones	3	0	2	1	0	33%
25 Temáticas para sensibilización del personal en seguridad de la información	20	0	0	20	0	0%

Figura 3 – Evaluación de los elementos de Dirección y Gestión

	INFORME DE AUDITORÍA Y SEGUIMIENTO	Código: EC-PR-002-FR-004	
	Macroproceso: Evaluación y Control	Versión: 03	
	Proceso: Gestión de Evaluación y Control	Fecha de Aprobación: 05/12/2022	

Elemento	ITEMS EVALUADO	Ítems Cumplidos		Ítems No Cumplidos		% Cumplimiento
		Totalmente	Parcialmente	No implementado	No Aplica	
26) Aplicación normatividad técnica colombiana sobre gestión documental.	17	5	8	4	0	53%
27) Instrumentos de gestión documental.	2	2	0	0	0	100%
28) Actividades para obtener el inventario de activos de información.	4	0	2	2	0	25%
29) Elementos del inventario de activos de información	32	8	18	6	0	53%
30) Publicación Índice de información Reservada y Clasificada.	2	0	0	2	0	0%
31) Adopción y publicación del Esquema de publicación de Información.	3	0	0	3	0	0%
32) Requisitos bases de datos con datos personales	8	8	0	0	0	100%
33) Entregables y actividades Fase I de planeación de IPv6.	17	2	13	2	0	50%
34) Entregables y actividades Fase II de implementación de IPv6.	8	1	6	1	0	50%
35) Entregables y actividades Fase III pruebas de funcionalidad de IPv6.	6	0	3	3	0	25%
36) Lineamientos de seguridad IPv6.	28	14	5	9	0	59%
37) Servicios Impactados en Seguridad para IPv6.	16	10	1	1	4	66%
38) Lineamientos de seguridad IPv6 en la nube.	15	11	3	1	0	83%
39) Controles de seguridad de los datos en la nube	10	3	4	3	0	50%
40) Elementos del proceso de atención de incidentes de seguridad.	18	15	3	0	0	92%
41) Elementos del proceso de evidencia digital.	7	7	0	0	0	100%
42) Controles del estándar ISO/IEC 27001.	112	74	26	0	0	78%

Figura 4 – Evaluación de los elementos de Infraestructura Tecnológica



En la Figura 3 y Figura 4 podemos observar el consolidado de los elementos del sistema de seguridad evaluados y calificados de acuerdo al cumplimiento total o parcial dentro del actual sistema de información de la Universidad, lo que nos lleva a determinar que **el nivel de madurez del sistema se encuentra en un nivel de definición intermedio** que se está documentando, actualizando, evaluando, aprobando e implementando a medida que va evolucionando.

Por otra parte, **la brecha en la implementación del sistema de seguridad se encuentra en un 54%** de acuerdo al promedio de evaluación de los elementos que requiere el sistema.

**Nota:** La información que se presentó con relación al avance en la implementación del sistema de seguridad fue avalada por el Comité institucional de Gestión y Desempeño – Sesión No. 7 que se realizó en la Sede Paiba el 21 de agosto del 2024.

## 2.3 FASE DE PLANEACION

En esta fase se definen los procedimientos para los elementos de seguridad que según la fase de diagnóstico presentan vulnerabilidades, riesgos o debilidades; se hace énfasis en reforzar y/o construir estrategias controles y seguimientos de los elementos que se consideran críticos para

	INFORME DE AUDITORÍA Y SEGUIMIENTO	Código: EC-PR-002-FR-004	
	Macroproceso: Evaluación y Control	Versión: 03	
	Proceso: Gestión de Evaluación y Control	Fecha de Aprobación: 05/12/2022	

la Universidad y que afecten el normal funcionamiento de la misma

### 2.3.1 IDENTIFICACION DE LOS ACTIVOS DE INFORMACION



Para implementar un sistema de seguridad de la información eficiente y confiable debe tener unas bases sólidas en cuanto a estrategias, gestión y control sobre la totalidad de los activos informáticos de la entidad; es esencial disponer de un inventario de activos informáticos actualizado por procesos para garantizar el cumplimiento de los 3 principios esenciales del sistema, que son Confidencialidad, Integridad y Disponibilidad.

Partiendo de este hecho, la OATI elaboró la **Guía Para La Identificación De Los Activos De Información**, la cual presenta la metodología para realizar inventario y clasificación de los activos de información que son manejados por los servidores públicos y contratistas a través de los diferentes procesos de la Universidad Distrital Francisco José de Caldas, con el fin principal de determinar qué activos posee la Institución, cómo deben ser identificados en los procesos, los roles y las responsabilidades que tiene el personal sobre los mismos.

Por otra parte, y como complemento a la Guía Para La Identificación De Los Activos De Información diseñó el **Formato Inventario y Clasificación de Activos de Información**, cuya finalidad es el registro de los activos informáticos que hacen parte de cada uno de los 22 procesos de la entidad; este registro según la guía de identificación de activos se programara al inicio de cada vigencia según lo considere el líder del proceso de seguridad de la información

Se presenta el procedimiento sugerido para realizar el inventario de activos informáticos, los cuales debe ser previamente aprobados



	<b>INFORME DE AUDITORÍA Y SEGUIMIENTO</b>	<b>Código: EC-PR-002-FR-004</b>	
	<b>Macroproceso: Evaluación y Control</b>	<b>Versión: 03</b>	
	<b>Proceso: Gestión de Evaluación y Control</b>	<b>Fecha de Aprobación: 05/12/2022</b>	

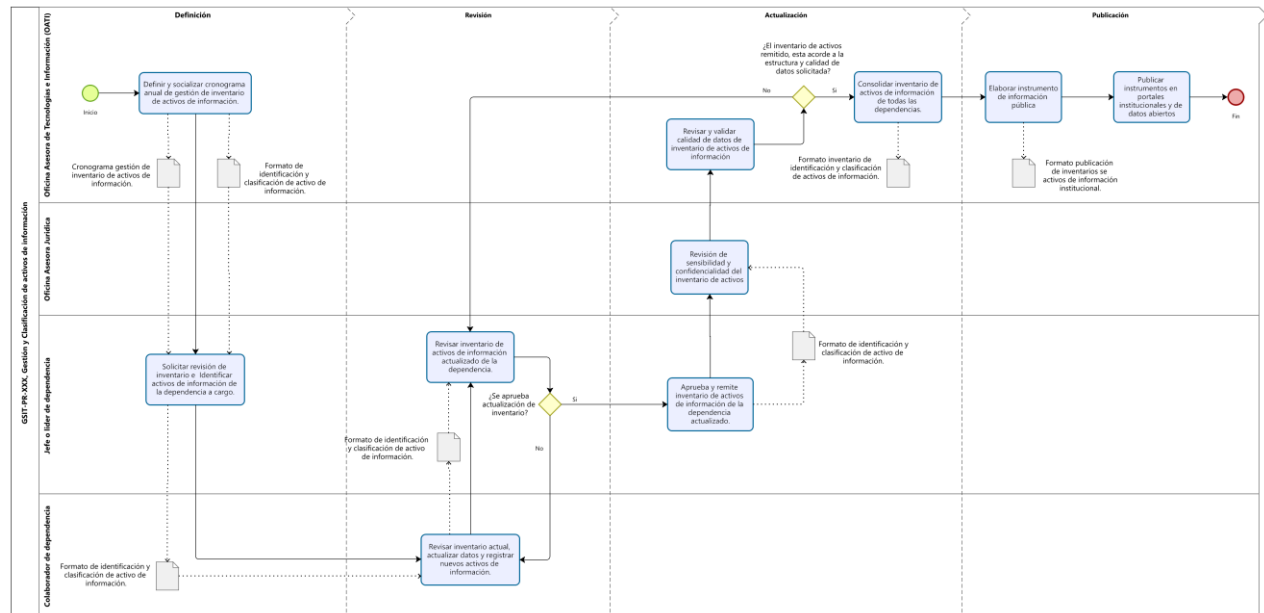


Figura 5 – Procedimiento propuesto para realizar el inventario de activos

### 2.3.2 GESTION DE RIESGOS



A la fecha el mapa integral de riesgos del Subsistema de Seguridad de la Información no presenta ningún avance ni gestión, sin embargo algunos proceso tiene identificados algunos riesgos referentes a la seguridad de la información, pero estos no están articulados entre sí, por lo que la OATI elabora una matriz de riesgos informáticos con el fin de ser evaluada, actualizada y aprobada por cada uno de los 22 proceso con el fin de centralizarlos y unificarlos en una única matriz que defina el Subsistema de Seguridad.

### 2.3.3 CONTINUIDAD DEL NEGOCIO

La continuidad de negocio es la planificación y preparación anticipada que se lleva a cabo para garantizar que una organización tenga la capacidad de seguir realizando sus funciones y actividades críticas durante eventos de emergencia como pueden ser desastres naturales, pandemia, sabotaje, hurto o daño de la infraestructura, algún ataque cibernético de cualquier índole que afecta los sistemas informáticos o la información de la organización.

La continuidad de negocio ayuda a la organización a responder rápidamente a una interrupción de los servicios, permitiendo seguir funcionando al menos a un nivel mínimo durante un evento critico



	INFORME DE AUDITORÍA Y SEGUIMIENTO	Código: EC-PR-002-FR-004	
	Macroproceso: Evaluación y Control	Versión: 03	
	Proceso: Gestión de Evaluación y Control	Fecha de Aprobación: 05/12/2022	

Para poder establecer un correcto procedimiento de continuidad del negocio lo primero es conocer el inventario de activos informáticos de cada uno de los procesos (se hizo mención en el punto 2.3.1) para determinar el nivel de criticidad del mismo y los tiempos de recuperación y acciones alternas de gestión durante la indisponibilidad total o parcial del sistema

se proyectaron dos procedimientos relacionados entre sí, uno enfocado en la **Gestión De Incidentes De Seguridad de la Información** y el otro en **Gestión de la Continuidad del Negocio**

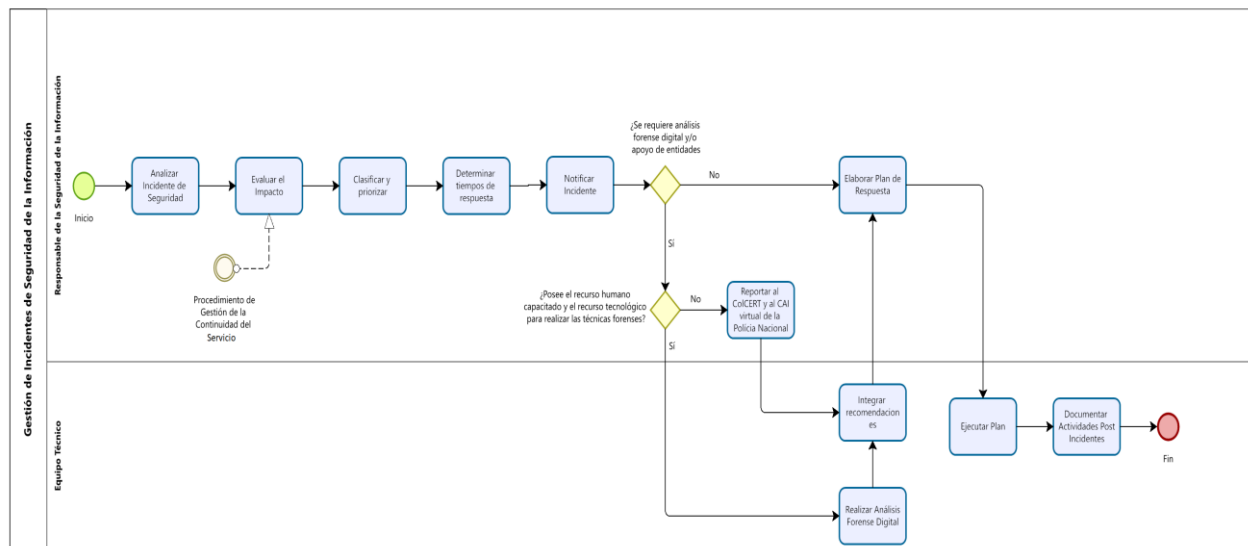




Figura 6 – Procedimiento Incidentes de Seguridad de la Información

Este procedimiento (Figura 6), hace referencia a las acciones que se deben seguir para atender el incidente, identificar y hacer seguimiento a la causa raíz de tal forma que permita elaborar planes de respuesta y generar recomendaciones y acciones que prevengan la reincidencia por vulnerabilidad, debilidad o falta de controles efectivos

	<b>INFORME DE AUDITORÍA Y SEGUIMIENTO</b>	<b>Código: EC-PR-002-FR-004</b>	
	<b>Macroproceso: Evaluación y Control</b>	<b>Versión: 03</b>	
	<b>Proceso: Gestión de Evaluación y Control</b>	<b>Fecha de Aprobación: 05/12/2022</b>	

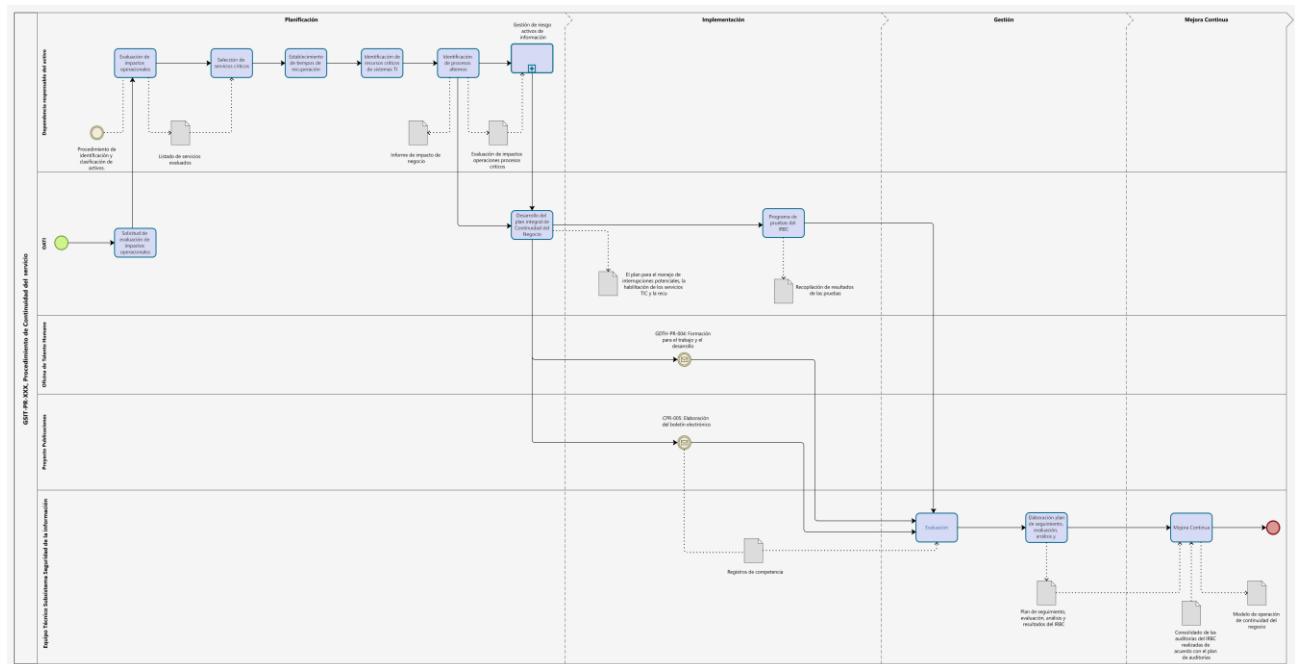


Figura 7 – Procedimiento Continuidad del Negocio



En este procedimiento (figura 7) contemplan variables importantes para identificar el impacto, el nivel la afectación, la magnitud de la pérdida de datos, la prioridad y tiempos de recuperación total o parcial, se identifican procesos alternos y tiempo máximo de inactividad, con fin de priorizar y atender con oportunidad cualquier incidente que se presente.

Se proyectaran y crearán indicadores para estos procedimientos que permitan evaluar la confiabilidad y solidez del sistema de seguridad, niveles de respuesta ante emergencias, cantidad de incidente registrados, y demás información relevante al procedimiento de continuidad del negocio; y finalmente contara con medios audiovisuales, como Manuales de uso y Videos Tutoriales que faciliten a los colaboradores la identificación y clasificación correcta de los activos informáticos y la gestión del formato de registro de los mismos

Estos procedimientos enfocados a garantizar la continuidad del negocio fueron avalados por el Comité institucional de Gestión y Desempeño – Sesión No. 7 la cual se realizó en la Sede Paiba el 21 de agosto del 2024.

#### 2.3.4. PRIORIZACIÓN DE NECESIDADES EN LA IMPLEMENTACIÓN DEL SGSI

Como punto de partida para establecer qué elementos se requieren para que el sistema de seguridad de la información de la Universidad Distrital FJC se han tenido en cuenta la Guía para

	INFORME DE AUDITORÍA Y SEGUIMIENTO	Código: EC-PR-002-FR-004	
	Macroproceso: Evaluación y Control	Versión: 03	
	Proceso: Gestión de Evaluación y Control	Fecha de Aprobación: 05/12/2022	

la implementación del MSPI y los controles de seguridad y privacidad de la información publicados por el MinTIC. Estos permiten priorizar las necesidades por categorías en función de su impacto y relevancia, facilitando así la asignación eficiente de recursos en función de la planificación estratégica.

CONSOLIDADO DE NECESIDADES PRIORIZADAS EN NIVEL 1 QUE REQUIEREN ATENCIÓN AL 100%				
Categoría	Ítem	% de cumplimiento	Priorización	% de Meta
SEGURIDAD DE LA INFORMACIÓN	Objetivos de seguridad de la información	91%	1	100%
	Políticas específicas recomendadas para la implementación de controles de seguridad de la información	76%	1	100%
GESTIÓN DEL PERSONAL Y EQUIPOS	Integrantes del equipo de gestión MSPI	44%	1	100%
	Ajustes de integrantes del equipo técnico de gestión y desempeño institucional del subsistema de seguridad de la información	67%	1	100%
GESTIÓN DEL RIESGO Y CONTINUIDAD DEL NEGOCIO	Actividades de gestión del riesgo del MSPI	50%	1	100%
DOCUMENTACIÓN Y NORMATIVAS	Documentación evaluación del desempeño MSPI	19%	1	100%
IMPLEMENTACIÓN TECNOLÓGICA	Equipo de trabajo IPv6 en seguridad de la información	80%	1	100%



Figura 8 – Consolidado de Ítems que deben implementarse al 100%

Figura 8 - De acuerdo a la a priorización de necesidades y a la meta de implementación se determinó que estas 7 necesidades se deben desarrollar de carácter prioritario logrando alcanzar su meta del 100% en lo que resta del año 2024

Existen otras necesidades que son importantes y relevantes para el avance del proyecto las cuales tienen una meta menor por lo que se van desarrollando y consolidando a medida que se avanza en la implantación del sistema

CONSOLIDADO DE NECESIDADES PRIORIZADAS EN NIVEL 1 QUE REQUIEREN ATENCIÓN MENOR AL 81%				
Categoría	Ítem	% de cumplimiento	Priorización	% de Meta
SEGURIDAD DE LA INFORMACIÓN	Indicadores de gestión para la seguridad de la información	44%	1	80%
DOCUMENTACIÓN Y NORMATIVAS	Documentación mejora continua MSPI (planeación e implementación)	13%	1	80%
	Aplicación normatividad técnica colombiana sobre gestión documental	53%	1	60%
IMPLEMENTACIÓN TECNOLÓGICA	Entregables y actividades Fase I de planeación de IPv6	50%	1	80%
	Entregables y actividades Fase II de implementación de IPv6	50%	1	70%
	Entregables y actividades Fase III pruebas de funcionalidad de IPv6	25%	1	60%

Figura 9 – Necesidades con prioridad 1 y porcentaje de meta < 100%

	INFORME DE AUDITORÍA Y SEGUIMIENTO	Código: EC-PR-002-FR-004	
	Macroproceso: Evaluación y Control	Versión: 03	
	Proceso: Gestión de Evaluación y Control	Fecha de Aprobación: 05/12/2022	

Estas últimas necesidades y/o categorías están proyectadas para alcanzar la meta deseada en la próxima vigencia 2025. Es importante darle continuidad a la fase de planificación para lograr el objetivo deseado en los tiempos establecidos.

### 2.3.5. PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN DE SEGURIDAD DE LA INFORMACIÓN



Se identificaron algunas temáticas que deben ser socializadas con funcionarios y contratista de la Universidad, con el fin de prevenir que se materialicen los riesgos asociados a la seguridad de la información y concienciar a los colaboradores en las buenas prácticas a nivel informático aplicables en la entidad y vida personal

Tema	Implementado
Administración de contraseñas	X
Uso y manejo de inventario	X
Malware y sus diferentes tipos	X
Software permitido/prohibido en la entidad	X
Políticas organizacionales relacionadas con seguridad de la información	X
Uso de dispositivos de la entidad fuera de las instalaciones	X
Uso de correo electrónico e identificación de correos sospechosos	X
Seguridad en el puesto de trabajo	X
Uso apropiado de internet	X
Temas de control de acceso a los sistemas (privilegios, separación de roles)	X
Política de escritorio limpio	X
Ingeniería social	X
Sanciones por incumplimiento de las políticas	X
Gestión De Incidentes (Como reportar, que puedo reportar)	X
Spam	X
"Shoulder surfing"	X
Backups y recuperación	X
Cambios en los sistemas	X
Amenazas y vulnerabilidades comunes	X
Roles y responsabilidades en la entidad	X

Figura 10 – temáticas objeto de sensibilización

### 2.3.6. REGLAMENTO DE USO DE LA CUENTA DE CORREO INSTITUCIONAL

La OATI y la UDNET (Red de Datos) actualizaron el reglamento para uso de la cuenta de correo institucional con el fin de adaptarse a la política de protección de datos según lo establecido en la resolución N. 432 del 30 de agosto de 2016, por otra parte actualiza los perfiles para asignación de las cuentas, capacidades de almacenamiento, vigencia de las mismas y condiciones de uso;

	INFORME DE AUDITORÍA Y SEGUIMIENTO	Código: EC-PR-002-FR-004	
	Macroproceso: Evaluación y Control	Versión: 03	
	Proceso: Gestión de Evaluación y Control	Fecha de Aprobación: 05/12/2022	

este informe se presentó y expuso al Comité Institucional de Gestión y Desempeño – Sesión No. 7 para su aprobación pero no fue avalado ya que se solicitó sea revisado previamente por el Oficina Jurídica para garantizar que las políticas aquí presentadas se encuentren dentro del marco legal y no vulneren la privacidad e integridad de la información que contiene cada cuenta institucional



### 2.3.7. MAPA DE RIESGOS

Para realizar una correcta implementación del sistema de seguridad de la información es necesario identificar los riesgos, el impacto y la probabilidad de que estos se materialicen y deben quedar registrados en la matriz de riesgos del sistema de información, esta ya fue elaborada por la OATI y será enviada a cada uno de los procesos que estableció la Universidad para que sea evaluada y actualizada según los activos informáticos y criterios de cada uno de ellos; por parte de la oficina de control interno se determinó

- Los 136 riesgos que identificó la OATI son transversales ya que se pueden materializar en cada uno de los procesos establecidos por la Universidad
- La segmentación por tipo de activo es acorde y está alineado al modelo de seguridad y privacidad de la información - MSPI
- La definición del impacto responde correctamente a los 3 principios de seguridad de la información: Disponibilidad, Integridad y Confidencialidad
- la efectividad de cada control impacta directamente en la disminución del riesgo residual, y es exactamente lo que se evidencia en la matriz que presentó la OATI, aunque se evidencian riesgos que no cuentan con controles establecidos
- Es importante realizar esta actividad de identificación de riesgos y controles en cada uno de los 22 procesos de la Universidad para asegurar y avanzar en la implementación general del sistema de seguridad de la información.



## 3. CONCLUSIONES

- Diagnosticar el nivel de implementación de un Sistema de Seguridad de la Información es una tarea compleja ya que contempla muchas variables, entornos y enfoques por lo que el MSPI se plantea como un ciclo, esto lo que permite es abordar temas y/o elementos que son críticos para la organización e ir avanzando en su implantación de tal forma que una vez alcanzada la meta se reinicia el ciclo y se apunta a otros objetivos; con este método se logra establecer prioridades y un

	INFORME DE AUDITORÍA Y SEGUIMIENTO	Código: EC-PR-002-FR-004	
	Macroproceso: Evaluación y Control	Versión: 03	
	Proceso: Gestión de Evaluación y Control	Fecha de Aprobación: 05/12/2022	

avance progresivo en el aseguramiento del sistema garantizando mayor robustez superando el riesgo existente con el menor impacto posible para la Universidad

- El informe de brechas que presento la OATI el 6 de junio de 2024 pertenece a la Fase de Diagnóstico y en él se logra determinar cual es el nivel de madurez del actual Sistema de Seguridad de la Información de la Universidad, y determino cual es la brecha para alcanzar un sistema estable, confiable, eficaz que cumpla con el criterio de aseguramiento que plantea el modelo MSPI.
- La universidad tiene implementadas varias herramientas informáticas desde sus inicios en la era digital que están orientadas a la seguridad tanto a la información como de las mismas plataformas, pero están desarticuladas y trabajando de manera independiente, lo que se quiere alcanzar con la implantación del SSI es generar políticas, estrategias, procedimientos que vinculen y articulen estas herramientas de seguridad en un contexto único de administración compartiendo recursos y unificando conceptos, por lo tanto la evolución del SSI es constante y cambiante ante las nuevas tecnologías
- Es importante darle continuidad a la fase de planificación para lograr el objetivo deseado en los tiempos establecidos; el levantamiento de activos informáticos y el mapa de riesgos son esenciales y prioritarios para establecer estrategias de aseguramiento de información.
- Actualmente la OATI esta liderando el proceso, sin embargo se requiere un Oficial de Seguridad de la Información que se apropie del mismo, determine la necesidad de realizar pruebas técnicas como son hacking ético y/o análisis forenses, que definan y caractericen el proceso de seguridad para toda la entidad, estableciendo e integrando políticas, estrategias, administrando recursos humanos/técnicos y articule el subsistema de seguridad con los objetivos estratégicos y misionales de la universidad.
- La privacidad de la información y la gestión de los datos personales se debe contemplar y clasificar adecuadamente, por lo que es necesario contar con la participación de un oficial de datos personales para gestionar correctamente los requerimientos surgidos en los procesos con los datos personales recolectados no

	INFORME DE AUDITORÍA Y SEGUIMIENTO	Código: EC-PR-002-FR-004	
	Macroproceso: Evaluación y Control	Versión: 03	
	Proceso: Gestión de Evaluación y Control	Fecha de Aprobación: 05/12/2022	



solamente en bases de datos sino también físico (papel) y evitar errores que puedan afectar legalmente a la Universidad.

- La priorización de continuidad de negocio fue acertada y se evidencia un avance real con la definición del procedimientos, formatos, indicadores y guías con el fin de madurar esta necesidad esencial para toda organización, es necesario contemplar elementos como servicios de nube, respaldo de información y de infraestructura tecnológica
- Se hace necesario empezar a realizar auditorías a elementos puntuales del subsistema de seguridad de la información, para determinar si las políticas de gestión son pertinentes, evaluar si los procedimientos establecidos son efectivos y si cuentan con controles adecuados, teniendo en cuenta la constante variación en los sistemas digitales y sus alcances.
- No se cuenta con un sistema de gestión documental que tenga el alcance para digitalizar y clasificar documentos físicos y electrónicos, el cual debe estar acompañado de una política o estrategia de gestión de información, dentro de este módulo ya se habla de retención de la información, clasificación y priorización de la información, gestión y administración de copias de seguridad, servicios de almacenamiento en nube, implementación de puntos de control, etc.
- Se analizó la matriz de riesgos de seguridad de la información por parte de la OCI y se avala como la matriz general ya que los riesgos identificados se pueden materializar en cada proceso de la Universidad, por lo tanto, esta matriz se debe alimentar y consolidar con los riesgos que identifique cada uno de los procesos según sus propios activos tecnológicos

#### 4. RECOMENDACIONES

- Con relación a la elaboración del inventario de activos informáticos propuesto por la OATI se debe realizar una campaña de capacitación y debe proporcionar medios audiovisuales que faciliten a los colaboradores de cada proceso la identificación de los



	INFORME DE AUDITORÍA Y SEGUIMIENTO	Código: EC-PR-002-FR-004	
	Macroproceso: Evaluación y Control	Versión: 03	
	Proceso: Gestión de Evaluación y Control	Fecha de Aprobación: 05/12/2022	

activos, y contemplar la asignación de personal que acompañe y resuelva las inquietudes y/o inconveniente que se puedan presentar durante el ejercicio, orientar y proponer en base a su experiencia y experticia en el área TI que activos se deben incluir en dicho inventario para garantizar de esta forma la efectividad de la actividad.

- Las redes sociales institucionales deben formar parte del inventario de activos informáticos de la Universidad, por lo tanto, deben ser tratadas como elementos esenciales en la comunicación asertiva entre Universidad y Comunidad, en este contexto deben existir políticas de administración y gestión que garanticen el aseguramiento de las mismas a nivel de acceso, publicación y contenido

Atentamente,



**GUILLERMO EDUARDO ALFONSO GUTIÉRREZ**

Jefe Oficina de Control Interno

RepresentanteAlta Dirección	Jefe Oficina de Control Interno	Auditor Responsable
N.A.	Guillermo Eduardo Alfonso Gutiérrez	Jhon Henry Arenas Martinez