Gobierno del Estado Plurinacional de
BOLIVIA
Ministerio de
Justicia y Transparencia
Institucional

RESOLUCIÓN MINISTERIAL Nro. 100/2020
La Paz, 5 de noviembre de 2020

CONSIDERANDO:

Que el Parágrafo I del Artículo 175 de la Constitución Política del Estado, dispone que las Ministras y los Ministros de Estado tienen entre otras atribuciones, el proponer y dirigir las políticas gubernamentales en su sector; la gestión de la Administración Pública en el ramo correspondiente, y dictar normas administrativas en el ámbito de su competencia.

Que el Parágrafo I del Artículo 20 del Texto Constitucional, determina que toda persona tiene derecho al acceso universal y equitativo a los servicios básicos de agua potable, alcantarillado, electricidad, gas domiciliario, postal y telecomunicaciones.

Que el Parágrafo II del Artículo 103 de la Norma Fundamental, estipula que el Estado asumirá como política la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de la información y comunicación.

Que el Decreto Supremo Nro. 29894 de 7 de febrero de 2009, de Estructura Organizativa del Órgano Ejecutivo del Estado, establece las atribuciones de la Presidenta o Presidente, Vicepresidenta o Vicepresidente y de las Ministras y Ministros, así como define los principios y valores que deben conducir a las Servidoras y a los Servidores Públicos, de conformidad a lo establecido en la Constitución Política del Estado.

Que el Decreto Supremo Nro. 3058 de 22 de enero de 2017, modifica el Decreto Supremo Nro. 29894 de 7 de febrero de 2009 de Estructura Organizativa del Órgano Ejecutivo del Estado Plurinacional, para crear el Ministerio de Energías, estableciendo su estructura, atribuciones y competencias; fusionar el Ministerio de Autonomías al Ministerio de la Presidencia; y el Ministerio de Transparencia Institucional y Lucha Contra la Corrupción al Ministerio de Justicia; complementado por el Decreto Supremo Nro. 3070 de 01 de febrero de 2017.

Que el Artículo 1 del Decreto Supremo Nro. 2514 de 9 de septiembre de 2015, establece: "El presente Decreto Supremo tiene por objeto: a) Crear la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC; b) Crear los Comités Interinstitucionales de Simplificación de Trámites".

Que el Artículo 9 del citado Decreto Supremo, prevé: "I. Se crea el Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia – CTIC - EPB, como instancia de coordinación para la implementación de Gobierno Electrónico y para el uso y desarrollo de Tecnologías de Información y Comunicación".

Que la Disposición Transitoria Segunda, del precitado Decreto Supremo, dispone: "Las entidades del nivel central del Estado deberán presentar a la AGETIC, en un plazo no mayor a un (1) año, desde la aprobación de las políticas de seguridad de la información por la AGETIC, su Plan Institucional de Seguridad de la Información".

Que el Artículo 1 del Decreto Supremo Nro. 3251 de 12 de julio de 2017, determina: "El presente Decreto Supremo tiene por objeto: a) Aprobar el Plan de Implementación de Gobierno Electrónico que en Anexo forma parte integrante del presente Decreto Supremo; (...)".

Que la Resolución Administrativa AGETIC/RA/0051/2017 de 19 de septiembre de 2017, emitida por la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC, dispone: "Aprobar el documento "Lineamientos para la Elaboración de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público" y sus tres Anexos, con la finalidad que las entidades públicas señaladas en el Decreto Supremo Nro. 2514 de 9 de septiembre de 2015 cumplan a lo dispuesto en el inciso f) del Artículo 7 y disposición transitoria segunda del referido Decreto".

Que los "Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público", aprobado mediante Resolución Administrativa AGETIC/RA/0051/2017 de 19 de septiembre de 2017, modificado por la Resolución Administrativa AGETIC/RA/0059/2018 de 01 de agosto de 2018, emitidos por la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC, establecen: "5. Términos y

definiciones. (...) Plan Institucional de Seguridad de la Información (PISI). Documento que establece las actividades relativas a la organización y gestión de la seguridad de la información en la entidad o institución pública (...)", "6.1.3. Conformación y funciones del Comité de Seguridad de la Información (CSI) Mediante resolución expresa, la Máxima Autoridad Ejecutiva designará al personal que conformará el Comité de Seguridad de la Información (CSI), de acuerdo al tamaño de la estructura organizativa de su entidad, volumen y complejidad de sus operaciones. El CSI estará conformado por: a) La Máxima Autoridad Ejecutiva en calidad de presidente del CSI, con la posibilidad de delegar sus funciones. b) Personal de nivel jerárquico, de acuerdo a la estructura organizativa de la entidad o institución pública. c) El Responsable de Seguridad de la Información (RSI); (...) El CSI establecerá su organización interna y asumirá como mínimo las siguientes funciones: a) Revisar el Plan Institucional de Seguridad de la Información (PISI). b) Promover la aprobación del PISI a través de la MAE. (...)".

Que mediante Decreto Presidencial Nro. 4141 de 28 de enero de 2020, se designa al Ciudadano Álvaro Eduardo Coímbra Cornejo, Ministro de Justicia y Transparencia Institucional.

Que la Resolución Ministerial Nro. 098/2018 de 15 de agosto de 2018, el Ministro de Justicia y Transparencia Institucional, dispone: "PRIMERO. - Designar al personal que conformará el Comité de Seguridad de la Información - CSI del Ministerio de Justicia y Transparencia Institucional, presidido por mi Autoridad en calidad de Presidente del Comité de Seguridad de la Información – CSI (...)"

Que la Resolución Ministerial Nro. 122/2018 de 17 de septiembre de 2018, resuelve: "PRIMERO.- Aprobar el Plan Institucional de Seguridad de la Información – PISI, del Ministerio de Justicia y Transparencia Institucional y sus Anexos: A "Listado de Activos de Información del Ministerio de Justicia y Transparencia Institucional"; B "Análisis de Riesgo del Ministerio de Justicia y Transparencia Institucional"; C "Controles de Seguridad de la Información del Ministerio de Justicia y Transparencia Institucional"; D "Política de Seguridad de la Información del Ministerio de Justicia y Transparencia Institucional"; los mismos que forman parte integrante e indivisible de la presente Resolución Ministerial".

Que la Resolución Ministerial Nro. 071/2019 de 2 de agosto de 2019, dispone: "PRIMERO. - Designar al personal que conformará el Comité de Seguridad de la Información - CSI del Ministerio de Justicia y Transparencia Institucional, presidido por mi Autoridad en calidad de Presidente del Comité de Seguridad de la Información – CSI, en el siguiente detalle: Despacho Ministerial: Jefe (a) de Gabinete. Viceministerio de Transparencia Institucional y Lucha Contra la Corrupción: Director (a) de Lucha Contra la Corrupción. Viceministerio de Defensa de Derechos del Usuario y del Consumidor: Director (a) General de Defensa de los Derechos del Usuario y del Consumidor. Viceministerio de Igualdad de Oportunidades: Director (a) General de Niñez y Personas Adultas Mayores. Viceministerio de Justicia Indígena Originario Campesina: Director (a) General de Justicia Indígena Originario Campesina. Viceministerio de Justicia y Derechos Fundamentales: Director (a) General de Justicia y Derechos Fundamentales. Dirección General de Asuntos Jurídicos: Director (a) General de Asuntos Jurídicos. Dirección General de Planificación: Director (a) General de Planificación. Dirección General de Asuntos Administrativos: Director (a) General de Asuntos Administrativos. Unidad de Comunicación Social: Jefe (a) de Unidad de Comunicación Social. Área de Tecnologías de Información y Comunicación: Encargado (a) de Infraestructura y Recursos Tecnológicos. Responsable de Seguridad de la Información (RSI): Responsable (a) de Tecnologías de Información y Comunicación. (...)".

Que la Resolución Ministerial Nro. 147/2019 de 13 de diciembre de 2019, dispone: "PRIMERO Ratificar la conformación del Comité de Seguridad de la Información – CSI del Ministerio de Justicia y Transparencia Institucional, designado mediante Resolución Ministerial Nro. 071/2019 de 2 de agosto de 2019".

Que el Área de Tecnologías de Información y Comunicación, dependiente de la Dirección General de Asuntos Administrativos, mediante Informe MJTI-DGAAATIC-349/2020 de 3 noviembre de 2020, concluye: "En fecha 3 de noviembre de la gestión 2020, el Comité de Seguridad de la Información del Ministerio de Justicia y Transparencia Institucional sostuvo su primera reunión de la gestión, en la cual se revisó los ajustes al Anexo C "Controles de Seguridad de la Información del Ministerio de Justicia y Transparencia Institucional" del Plan Institucional de Seguridad de la Informacion. En virtud a la revisión y ajustes del mencionado documento, los miembros del Comité de Seguridad de la Información en el marco de las funciones establecidas en los "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las

RESOLUCIÓN MINISTERIAL Nro. 100/2020
La Paz, 5 de noviembre de 2020

entidades del sector público" numeral 6.1.3 incisos c) e h) solicitaron que se modifique el cronograma detallado en el mencionado Anexo C del PISI. La solicitud de modificacion al cronograma corresponde a que la mayoría de los miembros del CSI fueron incorporados gestión 2020 y requieren tomar conocimiento de todos los documentos emergentes de los Controles de Seguridad de la Información a objeto su análisis y validación conjuntamente con el personal de sus respectivos Viceministerios, Direcciones y Unidades, para posteriormente recién recomendar la aprobación de los mismos por parte de la Máxima Autoridad Ejecutiva. En el marco de esta solicitud se requiere ajustar el cronograma del Anexo C "Controles de Seguridad de la Información del Ministerio de Justicia y Transparencia Institucional" del Plan Institucional de Seguridad de la Información del Ministerio de Justicia y Transparencia Institucional aprobado mediante Resolución Ministerial Nro 122/2018 de 17 de septiembre de 2018, debido a que en este documento se encuentran plasmadas las tareas y plazos para la implementación de los Controles de Seguridad. Al modificarse los plazos para la implementación de los controles de Seguridad de la Información es necesario que se ajuste el cronograma debido a que las tareas subsecuentes como la aprobación formal e implementación de los mismos también recorrerá. En virtud a esta necesidad se remite adjunto al presente informe el Acta de Reunión y el Anexo C del PISI con los plazos de los Controles de Seguridad de la Información ajustados según el requerimiento consensuado de los miembros del Comité de Seguridad de la Información para su aprobación mediante Resolución Ministerial en el marco de las conclusiones de la primera reunión de la gestión 2020 del Comité de Seguridad de la Información".

Que el Informe Legal CITE: MJTI – DGAJ – UAJ - INF. Nro. 354/2020 de 5 de noviembre de 2020, emitido por la Dirección General de Asuntos Jurídicos de esta Entidad Ministerial, recomienda: "(...) suscribir la Resolución Ministerial que aprueba el ajuste al anexo C "Controles de Seguridad de la Información del Ministerio de Justicia y Transparencia Institucional"; del Plan Institucional de Seguridad de la Información - PISI del Ministerio de Justicia y Transparencia Institucional (...)".

POR TANTO:

El Ministro de Justicia y Transparencia Institucional, en ejercicio de las atribuciones establecidas en los numerales 3 y 4 del parágrafo I del Artículo 175 de la Constitución Política del Estado, numeral 22 del parágrafo I del Artículo 14 del Decreto Supremo Nro. 29894 de 7 de febrero de 2009.

RESUELVE:

PRIMERO. –Aprobar el nuevo Anexo C "Controles de Seguridad de la Información del Ministerio de Justicia y Transparencia Institucional", del Plan Institucional de Seguridad de la Información – PISI del Ministerio de Justicia y Transparencia Institucional aprobado mediante la Resolución Ministerial Nro. 122/2018 de 17 de septiembre de 2018, el mismo que forma parte integrante e indivisible de la presente Resolución Ministerial.

SEGUNDO.- Se aprueban los Informes CITE: MJTI-DGAA-ATIC-349/2020 de 3 de noviembre de 2020, y CITE: MJTI – DGAJ – UAJ - INF. Nro. 354/2020 de 5 de noviembre de 2020, elaborados por las áreas respectivas de esta Entidad Ministerial, que sustentan técnica y legalmente la presente Resolución Ministerial.

TERCERO.- La Dirección General de Asuntos Administrativos, a través de su unidad organizacional pertinente, queda encargada del cumplimiento y ejecución de la presente Resolución Ministerial.

REGÍSTRESE, COMUNÍQUESE, CÚMPLASE Y ARCHÍVESE.

UNIDAD DE ANÁLISIS JURÍDICO
Vo Bo
MINISTERIO DE JUSTICIA Y TRANSPARENCIA INSTITUCIONAL

Abg. Bertha Cecilia Guzmán Collao
DIRECTORA GENERAL DE ASUNTOS JURÍDICOS
MINISTERIO DE JUSTICIA Y TRANSPARENCIA INSTITUCIONAL

Abg. Álvaro Eduardo Coimbra Cornejo
MINISTRO DE JUSTICIA Y
TRANSPARENCIA INSTITUCIONAL

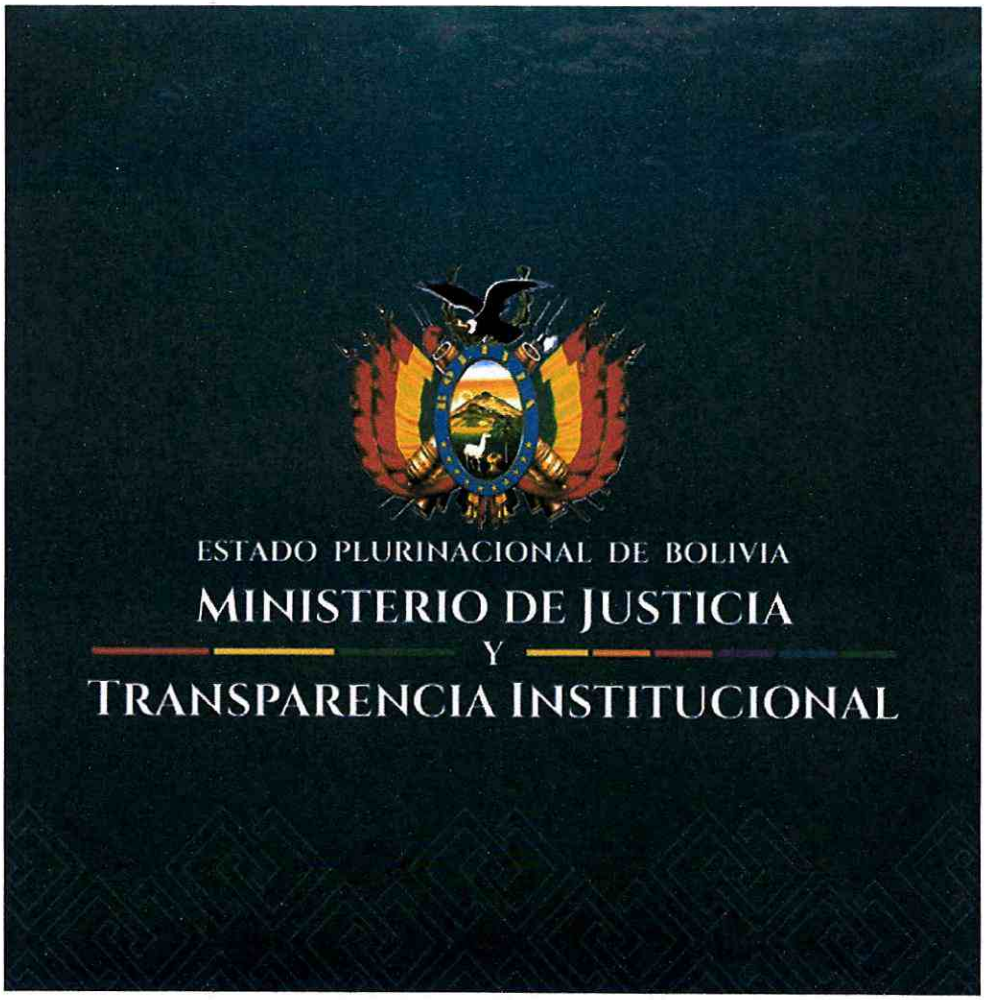
M.J.T.I.
VºBº
O.C.C.S.
ANÁLISIS JURÍDICO

ESTADO PLURINACIONAL DE BOLIVIA
MINISTERIO DE JUSTICIA
Y
TRANSPARENCIA INSTITUCIONAL

ANEXO C

Plan Institucional de Seguridad de la Información

Controles de Seguridad de la Información del Ministerio de Justicia y Transparencia Institucional



Versión 2018

Decreto Supremo N° 2514

Índice

Contenido

1) Controles por Implementar e Implementados

Como primer punto del inciso de controles de seguridad se presenta a continuación la tabla de Controles de Seguridad de la Información Implementados y por Implementar, obteniendo los controles requeridos del Anexo B "Análisis de Riesgo del Ministerio de Justicia y Transparencia Institucional" del Plan Institucional de Seguridad de la Información versión 2018 del Ministerio de Justicia y Transparencia Institucional.

Controles implementados y por implementar						
N	Control de Seguridad de la Información	Inclusión del Control	Control Existente	Justificación de Inclusión	Justificación de la Exclusión	Documentación
1	1.1.1.Seguridad en recursos humanos – Acuerdo de confidencialidad	SI	NO	El Reglamento Interno de Personal establece la confidencialidad de la información, sin embargo es necesario que todo personal vinculado a la entidad tenga conocimiento de la confidencialidad de la información y se tenga una constancia de este hecho.		
2	1.2.1.Seguridad en recursos humanos – Capacitación y formación	SI	NO	Es de vital importancia capacitar al personal institucional sobre la seguridad de la información para fortalecer la implementación de las políticas de seguridad al interior del Ministerio de Justicia y Transparencia institucional		
3	1.4. Seguridad en recursos humanos – Desvinculación de personal o cambio de cargo	SI	SI	Se cuenta con un formulario para la desvinculación del personal, sin embargo se necesita realizar una verificación y actualización del formulario de desvinculación del personal de la institución para garantizar la preservación de la información y la devolución de los activos de información		Formularios de desvinculación
4	2.1.2. Gestión de activos de información – Responsabilidad y custodia de los activos de información	SI	NO	Se deberá implementar un procedimiento que establezca quienes son responsables de archivos físicos de información confidencial o sensible y el cuidado que deberá tener el responsable con los mismos.		
5	2.2.1. Gestión de activos de información –Clasificación de la información	SI	NO	Se deberán identificar aquellos archivos físicos considerados confidenciales y sensibles en el marco del alcance del PISI		
6	2 Gestión de activos de información - Gestión de la configuración	SI	NO	Se deberá generar un formato para la documentación de la configuración de los servidores y soluciones de almacenamiento instalados en los Data Centers		
7	3.1.1. Control de accesos – Normativa de control de acceso	SI	NO	Se deberá elaborar un reglamento de control de acceso general a todas las instalaciones del MJTI estableciendo requisitos mínimos de ingreso, ambientes reservados y mecanismos de control de acceso		

Controles implementados y por implementar						
N	**Control de Seguridad de la Información**	**Inclusión del Control**	**Control Existente**	**Justificación de Inclusión**	**Justificación de la Exclusión**	**Documentación**
8	3.2.1 Control de accesos – Administración de accesos, cancelación y privilegios de usuarios	SI	NO	Se deben elaborar procedimientos para la habilitación y baja de usuarios en los diferentes servicios y sistemas institucionales		
9	3.2.1. Control de accesos – Responsabilidades de los usuarios para la autenticación	SI	NO	Se debe generar un documento para conocimiento de los usuarios de los sistemas de información que establezcan las responsabilidades de los mismos respecto a la autenticación		
10	5.1.1 Seguridad física y ambiental – Seguridad física en áreas e instalaciones	SI	NO	Se deberán identificar los ambientes en los cuales se requiere contar con un control estricto de ingreso y procedimientos para control de ingreso a los mismos		
11	4.1.1 Criptografía – Uso de Criptografía	NO	Si	Se cuenta con criptografía en la transmisión de información entre oficinas de Transparencia mediante VPNs encriptadas, asimismo, se cuenta con encriptación en la remisión de algunos datos para el SIRIEFI		
12	5.3.1. Seguridad física y ambiental – Condiciones operativas del CPD	SI	NO	Se debe establecer la periodicidad del mantenimiento de los componentes del CPD, así como el procedimiento para la realización de los mantenimiento		
13	6.2.1. Seguridad de la Operaciones – Respaldos de información	SI	NO	Se debe acordar la periodicidad de copias de respaldo a ser realizada para los diferentes sistemas de información almacenados en los Data Centers		
14	7.1.1 Seguridad de las comunicaciones – Gestión de red	SI	NO	Se deberá generar un formato para la documentación de la configuración de los switchs y Firewalls instalados en los ambientes de alcance del PISI		
15	8.1.1. Desarrollo, mantenimiento y adquisición de sistemas – Elaboración de la normativa de desarrollo	SI	NO	Se deberá elaborar un reglamento para el desarrollo de software al interior del Ministerio de Justicia y Transparencia Institucional		
16	8.1.4. Desarrollo, mantenimiento y adquisición de sistemas – Interoperabilidad de sistemas	SI	NO	Se deben generar formatos para documentar los servicios de interoperabilidad utilizados por los diferentes sistemas.		
17	11.2.1. Cumplimiento – Auditoría al Plan Institucional de Seguridad de la Información	SI	NO	Anualmente se deberá realizar una auditoría al Plan institucional de Seguridad de la Información para verificar su cumplimiento		

2) Directrices de los Controles de Seguridad

A continuación se describen las Directrices para la elaboración de cada control, así como los indicadores y las métricas a ser utilizadas y las fechas individuales de implementación de cada control

I. 1.1.1. Seguridad en recursos humanos – Acuerdo de confidencialidad

a) Justificación

El Reglamento Interno de Personal establece la confidencialidad de la información, sin embargo es necesario que todo personal vinculado a la entidad tenga conocimiento de la confidencialidad de la información y se tenga una constancia de este hecho.

b) Trabajo a ser realizado

- Dirección General de Asuntos Jurídicos establecerá el mecanismo adecuado para que se incluya un cláusula de confidencialidad de la información y propiedad del trabajo realizado en la documentación firmada por: Personal de Planta, Personal Eventual, Consultores por Producto, Consultores de Línea, Pasantes, Proyectistas de Grado
- Para cada caso la Dirección General de Asuntos Jurídicos elaborará las clausulas respectivas según las características de relación laboral con el Ministerio
- Las Cláusulas de confidencialidad y propiedad del trabajo finales serán puestas a conocimiento de todo el Ministerio para su inmediata incorporación mediante una Minuta de Instrucción emitida por Despacho Ministerial
- El personal de Contrataciones y Recursos Humanos verificará su adecuada implementación

c) Métricas a ser utilizadas

Para medir la eficacia del control se seleccionará un periodo de tiempo y se contrastará la incorporación de personal con la cantidad de Clausulas Incorporadas en los documentos de vinculación con el Ministerio de Justicia y Transparencia Institucional

Cumplimiento = Cantidad de documentos con cláusula / Cantidad de personal Vinculado

d) Cronograma

Control	2020		2021											
	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
1.1.1. Seguridad en recursos humanos – Acuerdo de confidencialidad	Una													

1.2.1. Seguridad en recursos humanos – Capacitación y formación

a) Justificación

Es de vital importancia capacitar al personal institucional sobre la seguridad de la información, para fortalecer el conocimiento en seguridad de la información al interior del Ministerio de Justicia y Transparencia institucional.

b) Trabajo a ser realizado

- El Responsable de Seguridad de la Información en coordinación con el Comité de Seguridad de la Información determinará un temario para las capacitaciones
- Con apoyo de la Dirección General de Asuntos Administrativos se elaborará un cronograma de capacitación y se lo comunicará a nivel del Ministerio
- Se capacitará al personal institucional enmarcado en el alcance del PISI

c) Métricas a ser utilizadas

Para medir la eficacia del control se dividirá la cantidad de personas que asistieron a las capacitaciones entre la cantidad de personal de planta que trabaja en los ambientes que se enmarcan en el alcance del PISI. Este análisis debe contemplar las capacitaciones de una sola gestión cada vez que se audite o evalúe el PISI.

Cumplimiento = Cantidad de asistentes / Cantidad de personal de planta en los tres edificios principales

d) Cronograma

Control	2020		2021											
	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
1.2.1. Seguridad en recursos humanos – Capacitación y formación	Ajustes a Controles		Revisión miembros CSI				Aprobación	Capacitaciones						

II. 1.4. Seguridad en recursos humanos – Desvinculación de personal o cambio de cargo

a) Justificación

Se cuenta con un formulario para la desvinculación del personal, sin embargo se necesita realizar una verificación y actualización del formulario de desvinculación del personal de la institución para garantizar la preservación de la información y la devolución de los activos de información.

b) Trabajo a ser realizado

- La Dirección General de Asuntos Administrativos en coordinación con el Responsable de Seguridad de la Información elaborarán una propuesta de nuevo formulario de desvinculación de personal
- El formulario de desvinculación del personal es presentado al Comité de Seguridad de la Información y consensuado por el mismo
- El Responsable de Seguridad de la Información capacitará al personal de la Unidad de Recursos Humanos en el uso del nuevo formulario
- La Unidad de Recursos Humanos utilizará el nuevo formulario para procesos de desvinculación de personal

c) Métricas a ser utilizadas

Para medir la eficacia de la implementación se deberá elegir un periodo de tiempo posterior a la implementación del formulario actualizado y dividir la cantidad de formularios de desvinculación existentes entre la cantidad de personal desvinculado

Cumplimiento = Cantidad de formularios de desvinculación / Cantidad personal desvinculado

d) Cronograma

Control	2020		2021											
	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
1.4. Seguridad en recursos humanos – Desvinculación de personal o cambio de cargo	Ajustes a Controles		Revisión miembros CSI				Aprobación	Implementación				Uso		

III. 2.1.2. Gestión de activos de información – Responsabilidad y custodia de los activos de información

a) Justificación

Se deberá implementar un procedimiento que establezca quienes son responsables de archivos físicos de información confidencial o sensible y el cuidado que deberá tener el responsable con los mismos.

b) Trabajo a ser realizado

- Personal de Biblioteca y Archivo elaborará un procedimiento para la asignación y el tratamiento de archivos de información físicos con información confidencial o sensible
- Personal de Biblioteca y Archivo remitirá el procedimiento para su aprobación
- Las Áreas Organizacionales que cuenta con archivos confidenciales y sensibles identificados por en el control V – "2.2.1. Gestión de activos de información – Clasificación de la información" serán capacitados en el nuevo procedimiento
- Las Áreas y Unidades Organizacionales que correspondan implementarán el procedimiento

c) Métricas a ser utilizadas

Para medir la eficacia del control se deberá dividir la cantidad de archivos en los que se implementa el procedimiento de control entre la cantidad de archivos confidenciales y sensibles identificados en el control V – "2.2.1. Gestión de activos de información – Clasificación de la información"

Cumplimiento = Cantidad de archivos que implementan el procedimiento de control / Cantidad de archivos confidenciales y sensibles identificados

d) Cronograma

Control	2020		2021											
	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
2.1.2. Gestión de activos de información – Responsabilidad y custodia de los activos de	Ajustes a Controles		Revisión miembros CSI				Aprobación	Implementación				Uso		

IV. 2.2.1. Gestión de activos de información –Clasificación de la información

a) Justificación

Se deberán identificar aquellos archivos físicos considerados confidenciales y sensibles en el marco del alcance del PISI.

b) Trabajo a ser realizado

- La Dirección General de Asuntos Administrativos a través del personal de Biblioteca y Archivo requerirá a todas las Áreas Organizacionales enmarcadas en el alcance del PISI que identifiquen y remitan el detalle de archivos físicos bajo su custodia que son considerados confidenciales y/o sensibles
- Las Unidades y Áreas Organizacionales identificarán y remitirán la información requerida con un debido justificativo de su clasificación
- Personal de Biblioteca y Archivo elaborará un listado de Archivos sensibles y/o confidenciales

c) Métricas a ser utilizadas

Para medir la eficacia del control se deberá dividir la cantidad Áreas Organizacionales que respondieron a la solicitud de información y remitieron el detalle o la ausencia de archivos confidenciales y/o sensibles entre la cantidad de Áreas Organizacionales a las que se solicitó esta información.

Cumplimiento = Cantidad de Áreas que remiten detalle de archivos sensibles y/o confidenciales / Cantidad de áreas a las que se solicitó información

d) Cronograma

Control	2020		2021											
	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
2.2.1. Gestión de activos de información –Clasificación de la información											Solicitud	Remisión de información		Generación del listado

V. 2 Gestión de activos de información - Gestión de la configuración

a) Justificación

Se deberá generar un formato para la documentación de la configuración de los servidores y soluciones de almacenamiento instalados en los Data Centers.

b) Trabajo a ser realizado

- El Área de Tecnologías de Información y Comunicación elaborará un formato de documento para el registro de la configuración de servidores y soluciones de almacenamiento
- El documento será presentado al Comité de Seguridad de la Información para su revisión y consenso mediante acta

- El formulario consensuado será remitido a la Dirección General de Asuntos Administrativos para su conocimiento
- Consensuado el formulario el Área de Tecnologías de Información y Comunicación procederá a documentar las configuraciones de los servidores y soluciones de Almacenamiento existentes y actualizarlo

c) Métricas a ser utilizadas

Para medir la eficacia de este control se deberán contrastar la cantidad de servidores y soluciones de almacenamiento con configuración documentada entre la cantidad de servidores y soluciones de almacenamiento implementadas y en funcionamiento en los Data Center o CPD.

Cumplimiento = Cantidad de Servidores y soluciones de almacenamiento documentados / Cantidad de Servidores y soluciones de almacenamiento implementados en los CPD

d) Cronograma

Control	2020		2021											
	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
2 Gestión de activos de información - Gestión de la configuración	Ajustes a Controles		Revisión miembros CSI				Aprobación	Documentación de servidores y soluciones de almacenamiento actuales				Actualización de la documentación		

VI. 3.1.1. Control de accesos – Normativa de control de acceso

a) Justificación

Se deberá elaborar un reglamento de control de acceso general a todas las instalaciones del MJTI estableciendo requisitos mínimos de ingreso, ambientes reservados y mecanismos de control de acceso.

b) Trabajo a ser realizado

- La Dirección General de Asuntos Administrativos solicitará a todas las Áreas Organizacionales enmarcadas en el alcance del PISI que identifiquen los ambientes con información confidencial o sensible
- La Dirección General de Asuntos Administrativos con la información precedente elaborará una propuesta de reglamento para el acceso a todas las instalaciones de los tres edificios principales del MJTI enmarcados en el alcance del PISI
- El Reglamento será presentado para conocimiento, sugerencias y revisión al Comité de Seguridad de la Información
- La Dirección General de Asuntos Administrativos remitirá el reglamento para su aprobación
- Una vez aprobado, se pondrá el reglamento a conocimiento del personal de seguridad y se lo capacitará en su implementación

c) Métricas a ser utilizadas

Para medir la eficacia del control se deberá dividir la cantidad de personal de seguridad capacitado en una gestión entre la cantidad de personal de seguridad que apoya al Ministerio.

Cumplimiento = Cantidad de personal capacitado en una gestión / Cantidad de personal de seguridad

d) Cronograma

Control	2020		2021											
	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
3.1.1. Control de accesos – Normativa de control de acceso	Ajustes a Controles		Revisión miembros CSI				Aprobación	Implementación				Uso		

VII. 3.2.1 Control de accesos – Administración de accesos, cancelación y privilegios de usuarios

a) Justificación

Se deben elaborar procedimientos para la habilitación y baja de usuarios en los diferentes servicios y sistemas institucionales.

b) Trabajo a ser realizado

- El Área de Tecnologías de Información y Comunicación elaborará una propuesta de procedimiento para la habilitación y baja de usuarios al interior del Ministerio de Justicia y Transparencia Institucional
- El Área de Tecnologías de Información y Comunicación remitirá la propuesta de procedimiento para su aprobación
- Aprobado el procedimiento se capacitará a los Administradores de los sistemas de información de cada Área Organizacional encargada de su propio sistema de información

c) Métricas a ser utilizadas

Para medir la eficacia del control se deberá dividir la cantidad de sistemas que implementan el procedimiento entre la cantidad de sistemas utilizados.

Cumplimiento = Cantidad de sistemas que usan procedimiento / Cantidad de sistemas en uso

d) Cronograma

Control	2020		2021											
	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
3.2.1 Control de accesos – Administración de accesos, cancelación y privilegios de usuarios	Ajustes a Controles		Revisión miembros CSI				Aprobación	Implementación				Uso		

VIII. 3.2.1. Control de accesos – Responsabilidades de los usuarios para la autenticación

a) Justificación

Se debe generar un documento para conocimiento de los usuarios de los sistemas de información que establezcan las responsabilidades de los mismos respecto a la autenticación.

b) Trabajo a ser realizado

- El Área de Tecnologías de Información y Comunicación en coordinación con la Dirección General de Asuntos Jurídicos elaborarán un documento para conocimiento de todo usuario de sistemas de información respecto a su uso
- El documento será puesto a conocimiento del Comité de Seguridad de la Información y se consensuará mediante acta
- El documento consensuado será puesto a conocimiento de todo el personal.

c) Métricas a ser utilizadas

Para medir la eficacia del control se dividirá las Áreas Organizacionales fueron puestas a conocimiento del documento entre las Áreas Organizacionales del Ministerio.

Cumplimiento = Áreas Organizacionales puestas a conocimiento / Áreas Organizacionales existentes

d) Cronograma

Control	2020		2021											
	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
3.2.1. Control de accesos – Responsabilidades de los usuarios para la autenticación	Ajustes a Controles		Revisión miembros CSI				Aprobación	Implementación				Uso		

IX. 5.1.1 Seguridad física y ambiental – Seguridad física en áreas e instalaciones

a) Justificación

Se deberán identificar los ambientes en los cuales se requiere contar con un control estricto de ingreso y procedimientos para control de ingreso a los mismos.

b) Trabajo a ser realizado

- La Dirección General de Asuntos Administrativos solicitará a todas las Áreas Organizacionales el detalle de ambientes utilizados que contienen información confidencial y sensible
- Utilizando la información remitida la Dirección General de Asuntos Administrativos establecerá mecanismos para que se pueda controlar el ingreso a estos ambientes y los incluirá en el Reglamento de control de acceso del Control "3.1.1. Control de accesos – Normativa de control de acceso"

* Este control debe ser trabajo en conjunto al control "VII. 3.1.1. Control de accesos – Normativa de control de acceso".

c) Métricas a ser utilizadas

Para medir la implementación de este control se deberá verificar que existen ambientes sensibles con aspectos propios de ingreso en el Reglamento de Control de Acceso.

Cumplimiento = Existencia de ambientes especiales en Reglamento de Control de Acceso (SI | NO)

d) Cronograma

Control	2020		2021											
	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
5.1.1 Seguridad física y ambiental – Seguridad física en áreas e instalaciones	Ajustes a Controles		Revisión miembros CSI				Aprobación	Implementación				Uso		

X. 5.3.1. Seguridad física y ambiental – Condiciones operativas del CPD

a) Justificación

Se debe establecer la periodicidad del mantenimiento de los componentes del CPD, así como el procedimiento para la realización de los mantenimientos.

b) Trabajo a ser realizado

- El Área de Tecnologías de Información y Comunicación (ATIC) elaborará un documento que establezca la periodicidad de los mantenimientos preventivos de los diferentes componentes del Data Center, así como el procedimiento que debe ser aplicado para este trabajo
- El Procedimiento será presentado al Comité de Seguridad de la información para su revisión y conocimiento de los costos de mantenimiento
- El ATIC remitirá el procedimiento para su aprobación
- Una vez aprobado el procedimiento y la periodicidad, la Dirección General de Asuntos Administrativos asignará recursos de acuerdo a disponibilidad presupuestaria
- Una vez asignado el presupuesto el ATIC procederá a realizar los mantenimientos preventivos

c) Métricas a ser utilizadas

Para medir la eficacia de este control se deberá dividir la cantidad de mantenimientos realizados entre la cantidad de mantenimientos establecidos en el Procedimiento.

Cumplimiento = Mantenimientos realizados / Mantenimientos establecidos en el Procedimiento

d) Cronograma

Control	2020		2021											
	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
5.3.1. Seguridad física y ambiental – Condiciones operativas del CPD	Ajustes a Controles		Revisión miembros CSI				Aprobación	Cumplimiento						

XI. 6.2.1. Seguridad de la Operaciones – Respaldos de información

a) Justificación

Se debe acordar la periodicidad de copias de respaldo a ser realizada para los diferentes sistemas de información almacenados en los Data Centers.

b) Trabajo a ser realizado

- El Área de Tecnologías de Información y Comunicación (ATIC) se reunirá con las áreas organizacionales que utilizan los diferentes sistemas de información y mediante acta se establecerá la periodicidad con la cual se deberá realizar el respaldo de la información
- El Área de Tecnologías de Información y Comunicación procederá a realizar las copias de respaldo con la periodicidad determinada

c) Métricas a ser utilizadas

Para medir la eficacia de este control se deberá dividir la cantidad de sistemas de información que cuentan con acta de determinación de periodicidad de copias de respaldo entre la cantidad de sistemas de información en uso.

Cumplimiento = Sistemas con acta de periodicidad / Sistemas en uso

d) Cronograma

Control	2020		2021											
	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
6.2.1. Seguridad de la Operaciones – Respaldos de información	Implementación													

XII. 7.1.1 Seguridad de las comunicaciones – Gestión de red

a) Justificación

Se deberá generar un formato para la documentación de la configuración de los switchs y Firewalls instalados en los ambientes de alcance del PISI.

b) Trabajo a ser realizado

- El Área de Tecnologías de Información y Comunicación elaborará un formato de documento para el registro de la configuración de switchs y Firewalls
- El documento será presentado al Comité de Seguridad de la Información para su revisión y consenso mediante acta
- El formulario consensuado será remitido a la Dirección General de Asuntos Administrativos para su conocimiento
- Aprobado el formulario el Área de Tecnologías de Información y Comunicación procederá a documentar las configuraciones de los switchs y Firewalls instalados y en uso en los ambientes de los tres edificios principales enmarcados en el alcance del PISI

c) Métricas a ser utilizadas

Para medir la eficacia de este control se deberán contrastar la cantidad de switchs y firewalls con configuración documentada entre la cantidad de switchs y firewalls implementados y en uso en los ambientes de los tres edificios principales enmarcados en el alcance del PISI.

Cumplimiento = Cantidad de Switchs y Firewalls con configuración documentada / Cantidad de Switchs y Firewalls en edificios principales en uso

d) Cronograma

Control	2020		2021											
	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
7.1.1 Seguridad de las comunicaciones – Gestión de red	Ajustes a Controles		Revisión miembros CSI				Aprobación	Documentación de Switches y Firewalls				Actualización de la documentación		

XIII. 8.1.1. Desarrollo, mantenimiento y adquisición de sistemas – Elaboración de la normativa de desarrollo

a) Justificación

Se deberá elaborar un reglamento para el desarrollo de software al interior del Ministerio de Justicia y Transparencia Institucional.

b) Trabajo a ser realizado

- El Área de Tecnologías de Información y Comunicación elaborará el reglamento de desarrollo de Software
- El reglamento será presentado al Comité de Seguridad de la Información para su revisión y sugerencias
- El Área de Tecnologías de Información y Comunicación remitirá el reglamento de desarrollo de Software para su aprobación
- Una vez aprobado el Reglamento el mismo será puesto a conocimiento de todo el personal mediante un Comunicado de la Dirección General de Asuntos Administrativos

c) Métricas a ser utilizadas

Para medir la eficacia de este control se deberá dividir la cantidad de sistemas de información desarrollados posteriores a la probación que hayan cumplido con el Reglamento entre la cantidad de sistemas de información desarrollados posteriores a la aprobación del Reglamento.

Cumplimiento = Cantidad de Sistemas desarrollados que cumplen con el Reglamento / Cantidad de Sistemas desarrollados

d) Cronograma

Control	2020		2021											
	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
8.1.1. Desarrollo, mantenimiento y adquisición de sistemas – Elaboración de la normativa de desarrollo	Ajustes a Controles		Revisión miembros CSI				Aprobación	Uso						

XIV. 8.1.4. Desarrollo, mantenimiento y adquisición de sistemas - Interoperabilidad de sistemas

a) Justificación

Se deben generar formatos para documentar los servicios de interoperabilidad utilizados por los diferentes sistemas.

b) Trabajo a ser realizado

- El Área de Tecnologías de Información y Comunicación elaborará un formato de documento para el registro de información de servicios de interoperabilidad utilizados en los diferentes sistemas
- El documento será presentado al Comité de Seguridad de la Información para su revisión y consenso mediante acta
- El formato consensuado será remitido a la Dirección General de Asuntos Administrativos para su conocimiento
- Consensuado el formato el Área de Tecnologías de Información y Comunicación procederá a documentar la información de los servicios de interoperabilidad en uso

c) Métricas a ser utilizadas

Para medir la eficacia de este control se deberá dividir la cantidad servicios de interoperabilidad documentados entre la cantidad de servicios de interoperabilidad usados.

Cumplimiento = Cantidad de servicios de interoperabilidad / Cantidad de servicios de Interoperabilidad documentados

d) Cronograma

Control	2020		2021											
	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
8.1.4. Desarrollo, mantenimiento y adquisición de sistemas - Interoperabilidad de sistemas	Ajustes a Controles		Revisión miembros CSI				Aprobación	Implementación						

XV. 11.2.1. Cumplimiento – Auditoría al Plan Institucional de Seguridad de la Información

a) Justificación

Anualmente se deberá realizar una auditoría al Plan institucional de Seguridad de la Información para verificar su cumplimiento.

b) Trabajo a ser realizado

- La Unidad de Auditoría Interna anualmente realizará una Auditoría al cumplimiento de los Controles de Seguridad del Plan Institucional de Seguridad de la Información

c) Métricas a ser utilizadas

Se deberá verificar si se realizó o no la auditoría al Plan Institucional de Seguridad de la Información.

Cumplimiento = Se realizó la auditoría al PISI (SI | NO)

d) Cronograma

Control	2020		2021											
	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
11.2.1. Cumplimiento – Auditoría al Plan Institucional de Seguridad de la Información														Auditoria

3) Cronograma General de Implementación de Controles de Seguridad

A continuación se detalla el cronograma integrado de implementación de todos los controles establecidos en el presente anexo.

Control	2020		2021											
	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
1.1.1. Seguridad en recursos humanos – Acuerdo de confidencialidad	Uso													
1.2.1. Seguridad en recursos humanos – Capacitación y formación	Ajustes a Controles		Revisión miembros CSI				Aprobación	Capacitaciones						
1.4. Seguridad en recursos humanos – Desvinculación de personal o cambio de cargo	Ajustes a Controles		Revisión miembros CSI				Aprobación	Implementación				Uso		
2.1.2. Gestión de activos de información – Responsabilidad y custodia de los activos de información	Ajustes a Controles		Revisión miembros CSI				Aprobación	Implementación				Uso		
2.2.1. Gestión de activos de información –Clasificación de la información											Solicitud	Remisión de información		Generación del listado
2 Gestión de activos de información - Gestión de la configuración	Ajustes a Controles		Revisión miembros CSI				Aprobación	Documentación de servidores y soluciones de almacenamiento actuales				Actualización de la documentación		
3.1.1. Control de accesos – Normativa de control de acceso	Ajustes a Controles		Revisión miembros CSI				Aprobación	Implementación				Uso		
3.2.1 Control de accesos – Administración de accesos, cancelación y privilegios de usuarios	Ajustes a Controles		Revisión miembros CSI				Aprobación	Implementación				Uso		
3.2.1. Control de accesos – Responsabilidades de los usuarios para la autenticación	Ajustes a Controles		Revisión miembros CSI				Aprobación	Implementación				Uso		

5.1.1 Seguridad física y ambiental – Seguridad física en áreas e instalaciones	Ajustes a Controles	Revisión miembros CSI	Aprobación	Implementación	Uso
5.3.1. Seguridad física y ambiental – Condiciones operativas del CPD	Ajustes a Controles	Revisión miembros CSI	Aprobación	Cumplimiento	
6.2.1. Seguridad de la Operaciones – Respaldos de información	Implementación				
7.1.1 Seguridad de las comunicaciones – Gestión de red	Ajustes a Controles	Revisión miembros CSI	Aprobación	Documentación de Switches y Firewalls	Actualización de la documentación
8.1.1. Desarrollo, mantenimiento y adquisición de sistemas – Elaboración de la normativa de desarrollo	Ajustes a Controles	Revisión miembros CSI	Aprobación	Uso	
8.1.4. Desarrollo, mantenimiento y adquisición de sistemas - Interoperabilidad de sistemas	Ajustes a Controles	Revisión miembros CSI	Aprobación	Implementación	
11.2.1. Cumplimiento – Auditoría al Plan Institucional de Seguridad de la Información					Auditoría

4) Tabla general de indicadores

A continuación se presenta la tabla general de indicadores para cada Control

Control	Descripción métrica	Métrica
I. 1.1.1. Seguridad en recursos humanos – Acuerdo de confidencialidad	Para medir la eficacia del control se seleccionará un periodo de tiempo y se contrastará la incorporación de personal con la cantidad de Clausulas Incorporadas en los documentos de vinculación con el Ministerio de Justicia y Transparencia Institucional	Cantidad de documentos con cláusula / Cantidad de personal Vinculado
1.2.1. Seguridad en recursos humanos – Capacitación y formación	Para medir la eficacia del control se dividirá la cantidad de personas que asistieron a las capacitaciones entre la cantidad de personal de planta que trabaja en los ambientes que se enmarcan en el alcance del PISI. Este análisis debe contemplar las capacitaciones de una sola gestión cada vez que se audite o evalúe el PISI.	Cantidad de asistentes / Cantidad de personal de planta en los tres edificios principales
1.4. Seguridad en recursos humanos – Desvinculación de personal o cambio de cargo	Para medir la eficacia de la implementación se deberá elegir un periodo de tiempo posterior a la implementación del formulario actualizado y dividir la cantidad de formularios de desvinculación existentes entre la cantidad de personal desvinculado	Cantidad de formularios de desvinculación / Cantidad personal desvinculado
IV. 2.1.2. Gestión de activos de información – Responsabilidad y custodia de los activos de información	Para medir la eficacia del control se deberá dividir la cantidad de archivos en los que se implementa el procedimiento de control entre la cantidad de archivos confidenciales y sensibles identificados en el control V – "2.2.1. Gestión de activos de información – Clasificación de la información"	Cantidad de archivos que implementan el procedimiento de control / Cantidad de archivos confidenciales y sensibles identificados
2.2.1. Gestión de activos de información – Clasificación de la información	Para medir la eficacia del control se deberá dividir la cantidad Áreas Organizacionales que respondieron a la solicitud de información y remitieron el detalle o la ausencia de archivos confidenciales y/o sensibles entre la cantidad de Áreas Organizacionales a las que se solicitó esta información	Cantidad de Áreas que remiten detalle de archivos sensibles y/o confidenciales / Cantidad de áreas a las que se solicitó información
2 Gestión de activos de información - Gestión de la configuración	Para medir la eficacia de este control se deberán contrastar la cantidad de servidores y soluciones de almacenamiento con configuración documentada entre la cantidad de servidores y soluciones de almacenamiento implementadas y en funcionamiento en los Data Center o CPD.	Cantidad de Servidores y soluciones de almacenamiento documentados / Cantidad de Servidores y soluciones de almacenamiento implementados en los CPD
3.1.1. Control de accesos – Normativa de control de acceso	Para medir la eficacia del control se deberá dividir la cantidad de personal de seguridad capacitado en una gestión entre la cantidad de personal de seguridad que apoya al Ministerio.	Cantidad de personal capacitado en una gestión / Cantidad de personal de seguridad
3.2.1 Control de accesos – Administración de accesos, cancelación y privilegios de usuarios	Para medir la eficacia del control se deberá dividir la cantidad de sistemas que implementan el procedimiento entre la cantidad de sistemas utilizados.	Cantidad de sistemas que usan procedimiento / Cantidad de sistemas en uso
3.2.1. Control de accesos – Responsabilidades de los usuarios para la autenticación	Para medir la eficacia del control se dividirá las Áreas Organizacionales fueron puestas a conocimiento del documento entre las Áreas Organizacionales del Ministerio.	Áreas Organizacionales puestas a conocimiento / Áreas Organizacionales existentes
5.1.1 Seguridad física y ambiental – Seguridad física en áreas e instalaciones	Para medir la implementación de este control se deberá verificar que existen ambientes sensibles con aspectos propios de ingreso en el Reglamento de Control de Acceso.	Existencia de ambientes especiales en Reglamento de Control de Acceso (SI | NO)

5.3.1. Seguridad física y ambiental – Condiciones operativas del CPD	Para medir la eficacia de este control se deberá dividir la cantidad de mantenimientos realizados entre la cantidad de mantenimientos establecidos en el Procedimiento.	Mantenimientos realizados / Mantenimientos establecidos en el Procedimiento
6.2.1. Seguridad de la Operaciones – Respaldos de información	Para medir la eficacia de este control se deberá dividir la cantidad de sistemas de información que cuentan con acta de determinación de periodicidad de copias de respaldo entre la cantidad de sistemas de información en uso.	Sistemas con acta de periodicidad / Sistemas en uso
7.1.1 Seguridad de las comunicaciones – Gestión de red	Para medir la eficacia de este control se deberán contrastar la cantidad de switchs y firewalls con configuración documentada entre la cantidad de switchs y firewalls implementados y en uso en los ambientes de los tres edificios principales enmarcados en el alcance del PISI.	Cantidad de Switchs y Firewalls con configuración documentada / Cantidad de Switchs y Firewalls en edificios principales en uso
8.1.1. Desarrollo, mantenimiento y adquisición de sistemas – Elaboración de la normativa de desarrollo	Para medir la eficacia de este control se deberá dividir la cantidad de sistemas de información desarrollados posteriores a la probación que hayan cumplido con el Reglamento entre la cantidad de sistemas de información desarrollados posteriores a la aprobación del Reglamento.	Cantidad de Sistemas desarrollados que cumplen con el Reglamento / Cantidad de Sistemas desarrollados
8.1.4. Desarrollo, mantenimiento y adquisición de sistemas - Interoperabilidad de sistemas	Para medir la eficacia de este control se deberá dividir la cantidad servicios de interoperabilidad documentados entre la cantidad de servicios de interoperabilidad usados.	Cantidad de servicios de interoperabilidad documentados / Cantidad de servicios de Interoperabilidad
11.2.1. Cumplimiento – Auditoría al Plan Institucional de Seguridad de la Información	Se deberá verificar si se realizó o no la auditoría al Plan Institucional de Seguridad de la Información	Se realizó la auditoría al PISI (SI | NO)