INSTITUTO MUNICIPAL DE DEPORTE Y LA RECREACIÓN DE YUMBO
IMDERTY

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

YAMILET MURCIA ROJAS

GERENTE

YUMBO – VALLE DEL CAUCA

2020 – 2023

TABLA DE CONTENIDO

1. INTRODUCCCION

El Instituto Municipal del Deporte y Recreación Municipal de Yumbo - IMDERTY, en cumplimiento al mantenimiento y mejora del modelo de seguridad de la información a través de la definición de un Sistema de Gestión de Seguridad de la Información (SGSI), tiene el compromiso de generar y actualizar la identificación, clasificación y valoración de los activos que son manejados en los procesos del Instituto.

La valoración de los activos es una actividad estratégica para el IMDERTY, puesto que determina la criticidad de los activos y finalmente como estos deben ser utilizados en los procesos del Instituto, define los roles y las responsabilidades que tiene el personal sobre los mismos y reconoce sus niveles de Confidencialidad, Integridad y Disponibilidad.

Los activos pueden ser de varios tipos: información, hardware, software, servicios, recursos humanos y tienen un ciclo de vida que cuenta con diferentes etapas, a saber: creación, procesamiento, uso, almacenamiento, transmisión y destrucción; independiente de su tipo y de la etapa en que se encuentra, los activos deben ser protegidos adecuadamente, de acuerdo con su nivel de clasificación.

Es importante destacar que el primer paso en la evaluación de riesgos es la identificación, clasificación y valoración de los activos de información, como se observa en la Imagen 1:

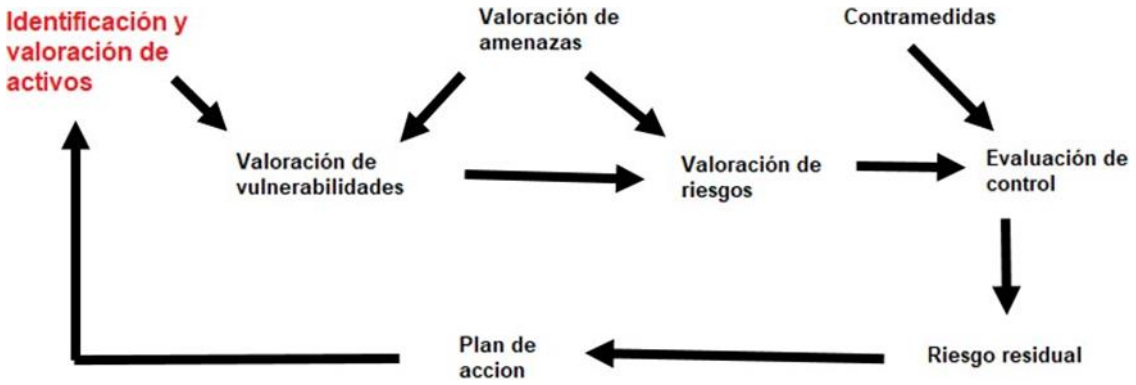


Imagen 1. Marco de referencia de Análisis de Riesgo Fuente. ISACA, IT Governance Implementation Guide

La gestión de riesgos de seguridad digital establece procesos, procedimientos y actividades encaminados a lograr un equilibrio entre la prestación de servicios y los riesgos asociados a los activos de información que dan apoyo y soporte en el desarrollo de la misión de la entidad. En tal sentido, se debe considerar e

implementar medidas que implican tiempo, esfuerzos y recursos necesarios para dar un adecuado tratamiento a los riesgos, generando una estrategia de seguridad digital efectiva que controle y administre la materialización de eventos o incidentes y mitigue los impactos adversos o considerables al interior de la entidad.

Para el Modelo de Seguridad y Privacidad de la Información (MSPI) la identificación, clasificación y valoración de activos hace parte de la fase de PLANIFICACIÓN que a su vez tiene una interacción directa con el Modelo de Gestión de Riesgos de Seguridad Digital (MGRS), como se observa en la Imagen 2:

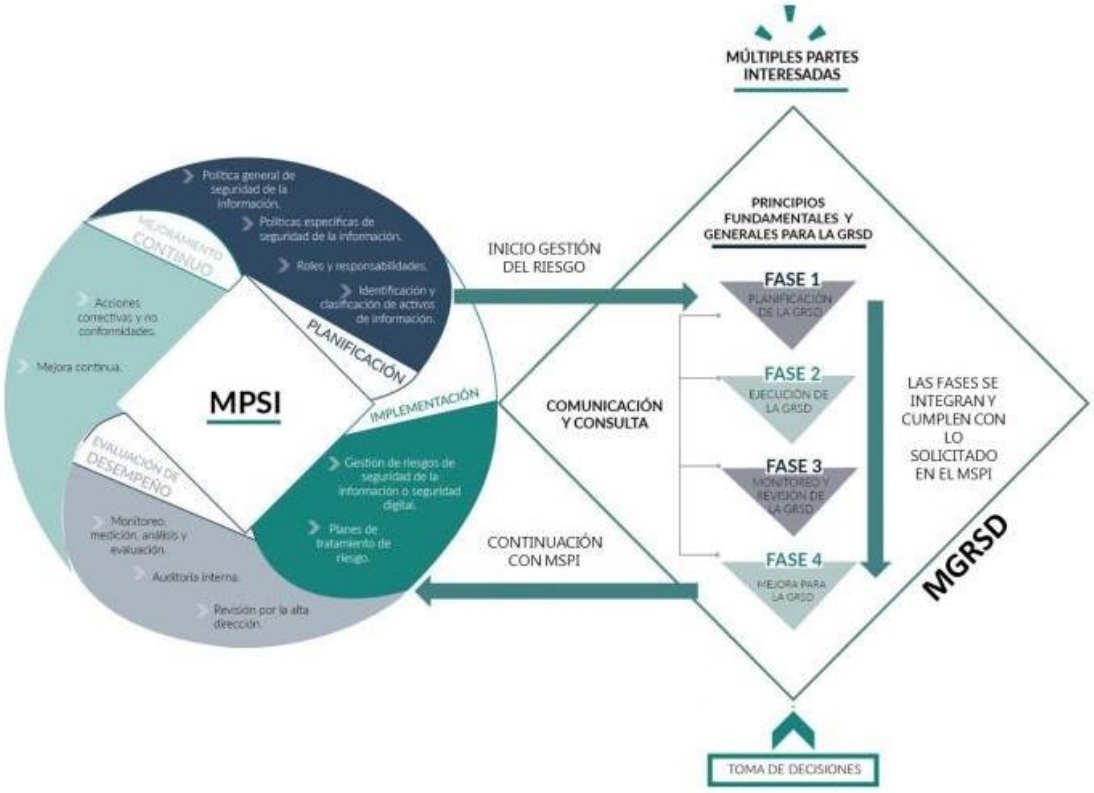


Imagen 2. Interacción entre el MSPI y el MGRSD
Fuente. Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas del DAFP

2. DEFINICIONES

Para la adecuada gestión de riesgos de Seguridad Digital se utilizan los siguientes términos:

- **Activo**: Bienes, recursos o derechos que tenga valor para una organización.
- [Según ISO 27000]: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. Toda la información que se maneja, y con la que cuenta una organización para un correcto funcionamiento.
- **Amenaza**: [Según ISO 27000]: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. Cualquier evento, persona, situación o fenómeno que pueda causar daño.
- **Análisis de brechas**: es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado.
- **Análisis del riesgo:** [NTC ISO 31000:2011]: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo. Método empleado para evaluar los riesgos informáticos y obtener respuesta de peligro.
- **Apetito de riesgo**: Es el nivel máximo de riesgo que la entidad está dispuesta a asumir.
- **Consecuencia**: [NTC ISO 31000:2011]: Resultado o impacto de un evento que afecta a los objetivos.
- **Controles**: [Según ISO 27000]: Las políticas, los procedimientos y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo, o conjunto de mecanismos que regulan el funcionamiento de un sistema.
- **Criterios del riesgo**: [Según NTC ISO 31000:2011]: Términos de referencia frente a los cuales se evalúa la importancia de un riesgo.
- **Dato sensible**. Son aquellos datos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como

los datos relativos a la salud, a la vida sexual y los datos biométricos. (Tomado de la ley 1581 de 2012 llamada ley de protección de datos personales).

- **Documento en construcción**. No será considerada información pública **aquella** información preliminar y no definitiva, propia del proceso deliberatorio de un sujeto obligado en su calidad de tal. (Tomado de la ley 1712 de 2014 llamada ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional).
- **Dato abierto.** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos. (Tomado de la ley 1712 de 2014 llamada ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional).
- **Dato personal**: Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos personales pueden ser públicos, semiprivados o privados. (Tomado de la ley 1266 de 2008 llamada ley habeas data)
- **Dato público**. Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas. (Tomado de la ley 1581 de 2012 llamada ley de protección de datos personales).
- **Evaluación del riesgo**: [Según NTC ISO 31000:2011]: Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- **Evento**: Acción que puedo haber causado daño, pero fue controlado.
- **Gestión del Riesgo Informáticos**: Actividades empleadas para mitigar los riesgos informáticos.
- **Identificación del riesgo:** [Según NTC ISO 31000:2011]: Proceso para encontrar, reconocer y describir el riesgo.
- **Impacto**: [Según ISO 27000]: El costo para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc. Impacto: Daño que provoca la materialización de una amenaza.

- **Incidente de seguridad informática**: daño que puede comprometer las operaciones de la entidad.
- **Información**: Conjunto de datos que tienen un significado.
- **Información interna**. Es aquella información que puede ser conocida y accedida al interior del instituto, tanto como funcionarios o contratistas debido a que es de interés de los mismos. Ejemplo: Intranet, Documentos dispuestos en el Sistema de Gestión Integrado – SGI.
- **Inventario de activos**: [Según ISO 27000.ES]. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos.
- **Información pública clasificada (Dato privado o semiprivado). Es aquella** información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que en su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados, tales como:

  1. El derecho a toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado.

  2. El derecho a toda persona a la vida, la salud o la seguridad.

  3. Los secretos comerciales, industriales y profesionales, así como los estipulados en el parágrafo del artículo 77 de la ley 1474 de 2011.

  Estas excepciones tienen una duración ilimitada y no deberán aplicarse cuando la persona natural o jurídica ha consentido en la revelación de sus datos personales o privados o bien cuando es claro que la información fue entregada como parte de aquella información que debe estar bajo el régimen de publicidad aplicable. (Tomado de la Ley 1712 de 2014 llamada Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional)

- **Información pública reservada**. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos, tales como:

  1. La defensa y seguridad nacional.

  2. La seguridad pública.

  3. Las relaciones internacionales.

4. La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso.

5. El debido proceso y la igualdad de las partes en los procesos judiciales.

6. La administración efectiva de la justicia.

7. Los derechos de la infancia y la adolescencia.

8. La estabilidad macroeconómica y financiera del país.

9. La salud pública. (Tomado de la Ley 1712 de 2014 llamada Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional).

- **ISO**: Organización Internacional de Normalización es una organización para la creación de estándares internacionales.
- **MSPI**: Modelo de seguridad y privacidad de la información
- **Nivel de riesgo**: [Según NTC ISO 31000:2011]: Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad.
- **Perfil del riesgo**: [Según NTC ISO 31000:2011]: Descripción de cualquier conjunto de riesgos.
- **PHVA**: Planear, hacer, verificar, actuar.
- **Política**: [Según ISO/IEC 27000:2016]: Intenciones y dirección de una organización como las expresa formalmente su alta dirección. **Probabilidad**: Posibilidad de que una amenaza se materialice
- **Reducción del riesgo**: [Según NTC ISO 31000:2011]: Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo.
- **Riesgo**: [Según ISO 27000]: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Riesgo Residual**: [Según ISO 27000]: El riesgo que permanece tras el tratamiento del riesgo.
- **Seguridad informática:** Se ocupa de la implementación técnica y de la operación para la protección de la información.
- **Seguridad de la información**: Se Ocupa de evaluar el riesgo y las amenazas, traza el plan de acción y esquemas normativos. Es la línea estratégica de las Seguridad.

- **SGSI**: Sistema de Gestión de seguridad de la Información
- **Vulnerabilidad**: [Según ISO 27000]: Debilidad de un activo o control que puede ser explotada por una o más amenazas. Falla o debilidad en un sistema que puede ser explotada por quien la conozca.

3. NORMATIVA APLICADA

Se tendrán como línea base para la clasificación de activos de información las normas y Leyes vigentes, las cuales se listan a continuación:

- Ley 1755 de 2015
- Ley 1712 de 2014
- Ley 1581 de 2012
- Ley 1266 de 2008
- Decreto 103 de 2015, Decreto 1377 de 2013
- Resolución 3564 de MinTIC
- Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, emitida en agosto de 2018.

4. MARCO TEORICO

a. NORMA ISO 27001

La norma ISO 27001 es un estándar internacional que describe cómo implementar el Sistema de gestión de seguridad de la información de una empresa. Investiga como salvaguardar la información mediante una serie de estándares, lineamientos y procesos que facilitan la identificación de los riesgos.

b. NORMA ISO 27005

La norma ISO 27005 es un soporte a la norma (ISO 27001), que proporciona directrices para la gestión de riesgos de seguridad de la información, es aplicable a todos los tipos de organización y no proporciona ni recomienda una metodología específica.

c. MODELO PHVA PARA EL SGSI

Un SGSI establece una serie de procesos y lineamientos que se deben seguir mediante la estandarización de la norma ISO 27001 para asegurar los activos de información como Bases de datos, oficios, actas etc. de una organización. El objetivo es mantener siempre la confidencialidad, integridad y disponibilidad de la información

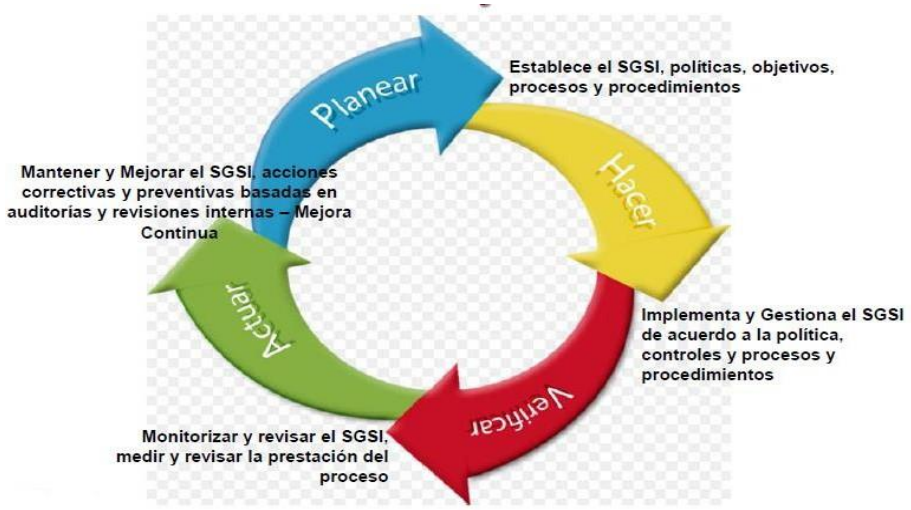
d. SEGURIDAD INFORMÁTICA

La seguridad Informática y la seguridad de la información son métodos y técnicas físicas y documentales empleadas para mantener siempre la confidencialidad, integridad y disponibilidad de la información.

Pilares de la seguridad informática.

e. METODOLOGÍA MAGERIT

Es una metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Se basa en análisis del impacto que puede tener una organización al ser vulnerada, buscando identificar las amenazas que pueden llegar a afectar el funcionamiento de la compañía



Ciclo PHVA de SGSI

Esta metodología, guía paso a paso cómo llevar a cabo el análisis de riesgos. Está dividida en tres partes:

La primera parte hace referencia al Método, donde se describe la estructura que debe tener el modelo de gestión de riesgos de acuerdo a la norma ISO 27001.

La segunda parte es el inventario activo de información que puede utilizar la empresa para enfocar el análisis de riesgo, las características que deben tenerse en cuenta para valorar los activos identificados y además un listado con las amenazas y controles que deben tenerse en cuenta.

La tercera parte, son las técnicas que contiene ejemplos de análisis con tablas, algoritmos, árboles de ataque, análisis de costo beneficio, técnicas gráficas y buenas prácticas para llevar adelante sesiones de trabajo para el análisis de los riesgos.

La metodología tiene como objetivos:

- Concientizar a los funcionarios y responsables de la información, los riesgos que enfrentan y como mitigarlos.
- Establecer el tratamiento de los riesgos para evitar que los mismos se materialicen.
- Proyectar a las organizaciones para la auditoria y certificación de la Norma ISO 27001.

5. PLAN DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

a. OBJETIVO

Establecer un marco de gestión de Riesgos Seguridad Digital, mediante el cual se mitiguen las vulnerabilidades y amenazas asociados a los activos de información del Instituto Municipal del Deporte y Recreación Municipal de Yumbo - IMDERTY, con el fin de lograr niveles de aceptación razonable en relación con los atributos de disponibilidad, integridad y confidencialidad de la información de la entidad.

b. OBJETIVOS ESPECÍFICOS

- Evaluar y analizar los Riesgos de Seguridad Digital asociadas a los procesos relacionados con los activos de información del Instituto Municipal del Deporte y Recreación Municipal de Yumbo - IMDERTY.
- Identificar e implementar controles que atiendan la gestión de riesgos y facilite la toma de decisiones sobre el riesgo residual.
- Definir el plan de tratamiento del riesgo residual de la entidad.

c. ALCANCE

El alcance del plan de gestión de Riesgos de Seguridad Digital inicia con la definición del contexto estratégico de los riesgos de Seguridad Digital a los que está expuesta la entidad dando cubrimiento a los procesos estratégicos, misionales, de apoyo y de evaluación y mejora que indiquen los criterios diferenciales del Modelo de Seguridad y Privacidad de la Información; y termina con el Plan de acción mediante el cual se realizará el tratamiento, monitoreo y revisión de los riesgos de Seguridad Digital identificados.

En concordancia con los lineamientos trazados en la Ley de transparencia 1712 de 2014, la Política de Gobierno Digital, se deben definir actividades que de manera articulada permitan implementar medidas de control que coadyuven a la prevención, contención y mitigación de amenazas a las que se encuentran expuestos los activos de información de la entidad por medio de una metodología descrita a continuación:

d. FASE DE PLANIFICACIÓN

i. METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

El Instituto Municipal del Deporte y Recreación Municipal de Yumbo - IMDERTY adoptará la metodología contenida en la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital del Departamento Administrativo de la Función Pública, complementando con buenas prácticas del estándar ISO-27005.

ii. POLÍTICA DE GESTIÓN RIESGOS

La Política de gestión de riesgos de Seguridad Digital GRSD definida para la entidad, se encuentra integrada en el documento titulado “Política de Integrada de Riesgos”.

iii. ROLES Y RESPONSABILIDADES

La gestión de Riesgos de Seguridad Digital es una responsabilidad que se debe apropiar por las dependencias, funcionarios y/o contratistas al interior del IMDERTY, establecidas en el documento de roles y responsabilidades.

El responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información, pertenece a la Subgerencia Administrativa y Financiera y hace parte de la Alta Dirección o Línea Estratégica y las responsabilidades, cuyas responsabilidades respecto a la gestión del riesgo de Seguridad Digital son las siguientes:

- ✓ Aplicar el procedimiento para la Identificación y Valoración de Activos.
- ✓ Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).

- ✓ Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
- ✓ Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
- ✓ Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

iv. DEFINICIÓN DE RECURSOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL.

Los recursos destinados para la gestión de riesgos de seguridad digital del IMDERTY provienen del rubro de funcionamiento. Donde parte de estos recursos son destinados a la adquisición de software e infraestructura tecnológica que coadyuve a la reducción de riesgos de seguridad digital y finalmente, contratación de personal con formación y conocimiento en gestión de seguridad de la información.

v. IDENTIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DIGITAL.

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital son activos elementos tales como aplicaciones de la entidad pública, servicios Web, redes, información física o digital, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-) que utiliza la organización para su funcionamiento.[1]

El IMDERTY posee un inventario y clasificación de los activos de información valorados con su nivel de criticidad de acuerdo a los atributos de integridad, disponibilidad y confidencialidad, los cuales ayudan a determinar los controles y medidas que protejan y salvaguardan los activos de información, que son los más importantes y críticos dentro de los procesos y procedimientos de la entidad.

De esta manera se busca proteger para garantizar tanto su funcionamiento interno (BackOffice), como su funcionamiento de cara al ciudadano (FrontOffice), aumentando así su confianza en el uso del entorno digital para interactuar con el Estado.

[1] ANEXO 4. LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

La identificación y valoración de activos se realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad digital, siendo debidamente orientados por el responsable de Seguridad Digital o de Seguridad de la información, ejecutando los siguientes pasos:

Paso 1. Listar los activos por cada proceso: En cada proceso, deberán listarse los activos de información indicando el tipo de proceso, proceso y descripción breve de cada uno.

Paso 2. Identificar el dueño de los activos: Cada uno de los activos identificados deberá tener un dueño asignado, si un activo no posee dueño, nadie se hará responsable ni lo protegerá debidamente.

Paso 3: Clasificar los activos: Se especifica la tipología del activo según su naturaleza, como, por ejemplo: Información, Software, Hardware, entre otros.

Paso 4: Clasificar la información: Realizar la clasificación de la información conforme los indican las Leyes, decretos y normas que apliquen.

Paso 5. Determinar la criticidad del activo: Evaluar el valor (Alta, Media, Baja) para cada una de las propiedades de confidencialidad, integridad y confidencialidad, con la finalidad de que sea un insumo para el análisis de riesgos y generar la protección, dependiendo del activo de información.

Paso 6. Identificar si existen infraestructuras críticas cibernética: Se considera como infraestructura crítica cibernética a todo activo que sea afectado por uno o más de los siguientes tres tipos de impacto:

- Impacto social, (0,5%) correspondiente a 250.000 personas de la Población Nacional
- Impacto económico, PIB de un día o 0,123% del PIB Anual.
- Impacto ambiental, de 3 años o más en recuperación.

Imagen 3. Etapas de la metodología de inventario y clasificación de activos de información Fuente. https://bit.ly/2IrNSGA

	SISTEMA INTEGRADO DE GESTIÓN INVENTARIO Y CLASIFICACIÓN DE ACTIVOS INSTRUCTIVO	Código:	FO:SIG.
		Versión:	01
		Fecha aprobación:	10/01/2020
		Páginas:	9

INFORMACIÓN BÁSICA											PROPIEDAD		ACCESO	FECHA		DATOS PERSONALES
						Criterios										
Identificador	Proceso/Área	Nombre del Activo	Descripción/Observaciones	Tipo de Activo	Ubicación	Confidencialidad	Integridad	Disponibilidad	Criticidad	Justificación	Propietario	Custodio	Usuarios	Fecha ingreso	Fecha salida	Personal S/N
ICI001	Gerencia	Acuerdo 003 de 1995. Creación IMDERTY	Contiene información relacionada con la creación del Instituo	Información	Despacho de la Gerencia, Archivo General				Sin Clasificar	Determina el marco de competencias legales del IMDERTY.	Proceso de Gestión Documental. Sub. AF	Técnico administrativo (Archivo)	Todos los procesos	15/12/2019		NO
ICI002	Gerencia	Acuerdo de Junta Directiva No. Xx Estructura organizacional							Sin Clasificar							
ICI003	Gerencia	Resolución Mapa de Procesos del IMDERTY							Sin Clasificar							
ICI004	Gerencia	Plan Estratégico Institucional							Sin Clasificar							
ICI005	Gerencia	Plan Estratégico Institucional							Sin Clasificar							

A continuación, se describe la tipología de activos con el fin de hacer la clasificación mencionada:

- **Información**: Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior se puede distinguir como información: contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos de nóminas, estados financieros, entre otros.

- **Software**: Activo informático lógico como programa, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades.

- **Hardware**: Equipos físicos de cómputo y de comunicaciones como: servidores, biométricos, etc. que por su criticidad son considerados activos de información.

- **Personas**: aquellas personas que, por su conocimiento, habilidades, experiencia y criticidad para el proceso, son consideradas activos de información.

- **Servicios**: Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como servicios de computación y comunicaciones, Internet, CRM, ERP, correo electrónico, páginas de consulta, directorios compartidos e Intranet, entre otros.

- **Otros**: activos que no corresponden a ninguno de los tipos descritos anteriormente.

Se debe especificar si el activo de información contiene datos personales y si hace parte de los siguientes tipos de información, datos o documentos:

- Información pública clasificada (Dato privado o semiprivado)
- Información pública reservada
- Documento privado
- Dato sensible
- Información interna
- Documento en construcción
- Dato abierto
- Dato público

Recordar que la Ley 1581 de 2012 llamada Ley de Protección de Datos Personales, reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.

Las siguientes figuras son de apoyo, buscando facilitar los conceptos de los diferentes tipos de información y datos:

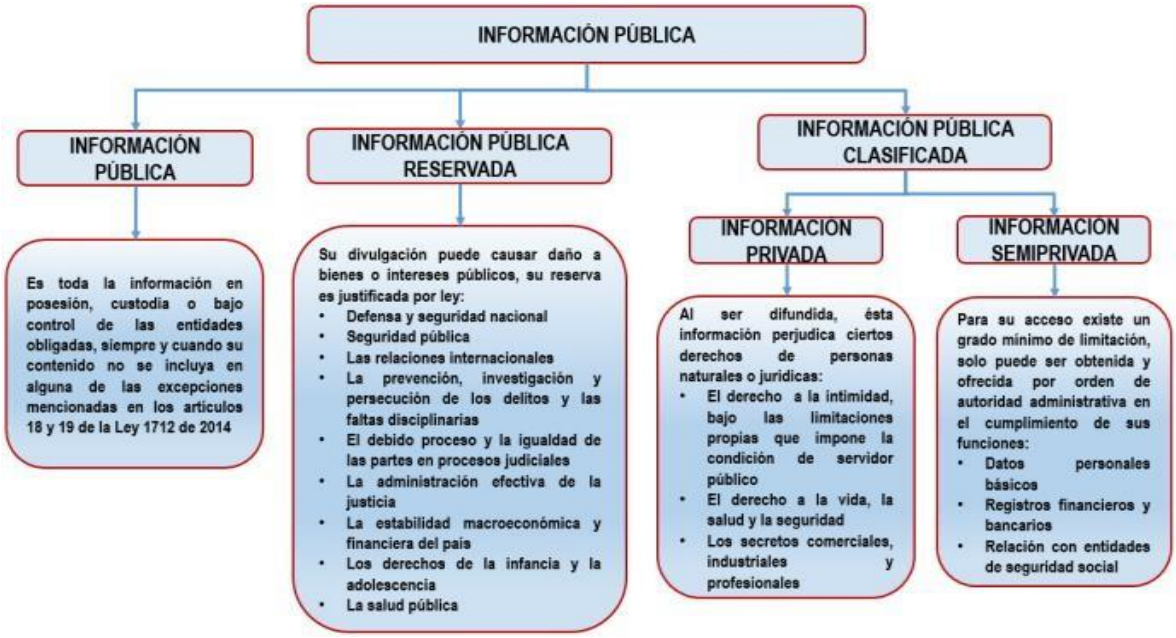


Figura 1. Clasificación de datos apoyo 1.
Fuente. http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/G-GD-02-calificacion-informacion.pdf

Figura 2. Clasificación de datos apoyo 2
Fuente.https://www.ecopetrol.com.co/Presentacion-charla-seguridad-informacion(29-09-16).pdf

La clasificación de activos de información tiene como objetivo asegurar que los activos reciben los niveles de protección adecuados, ya que con base en su valor y de acuerdo a otras características particulares requiere un tipo de manejo especial.

El sistema de gestión de la información definido en el IMDERTY se basa en las características particulares de los activos, el cual contempla su valor, requisitos legales, sensibilidad y la importancia para el Instituto.

Cada nivel de clasificación establece requerimientos específicos de tratamiento durante el ciclo de vida del activo; cada activo, a su vez, debe estar clasificado en un único nivel de Confidencialidad, Integridad y Disponibilidad, ya sea Alta, Media, Baja o Sin Clasificar de acuerdo a su criticidad.

vi. CLASIFICACIÓN DE ACUERDO CON LA CONFIDENCIALIDAD

El sistema de clasificación se basa en la confidencialidad como principio rector en la selección e incluye el tratamiento de la información en cuanto a la Confidencialidad, la Integridad y la Disponibilidad de cada activo. Asimismo, contempla el impacto que causaría la pérdida de alguna de estas propiedades.

En cada propiedad de los activos se establecen criterios específicos y lineamientos para su tratamiento. Se definen tres niveles que permiten determinar el valor general del activo (es importante aclarar que los niveles pueden ser definidos a criterio de la entidad): Alta, Media y Baja, con el fin identificar qué activos deben ser tratados de manera prioritaria (ver Tabla: Niveles de evaluación)[2].

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla 1 Criterios de Clasificación

[2] Guía No. 5 para la Gestión y Clasificación de Activos de Información. MINTIC.

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Tabla 2 Niveles de Clasificación

De acuerdo con las características de los activos que se manejan en IMDERTY, se definió el siguiente esquema de clasificación de cuatro (4) niveles, como muestra la tabla 3:

VALOR	CONFIDENCIALIDAD
ALTA	Activo disponible sólo para un grupo de personas dentro o fuera de IMDERTY (definido por el propietario del activo) y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole operativa, de pérdida de imagen o económica en IMDERTY o sus clientes finales. Por lo tanto, la Información pública clasificada, Información pública reservada, Datos sensibles serán catalogados como "Alta".
MEDIA	Corresponde a la Información interna del instituto que puede ser conocida y accedida por los funcionarios y contratistas, adicionalmente la información en construcción será catalogada como "Media"
BAJA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera del Instituto, sin que esto implique daños a terceros ni a las actividades y procesos del IMDERTY, los tipos de datos que hacen parte de esta categoría son datos públicos y datos abiertos.
NO CLASIFICADA	No tiene ningún impacto negativo para el proceso o el Instituto, o no aplica para el activo valorado. Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

Tabla 3. Esquema de clasificación por confidencialidad

La gestión de activos debe estar alineada con el Dominio 8 Gestión de Activos del anexo A de la norma ISO 27001:2013, y la guía de controles del modelo de seguridad y privacidad de la información, para garantizar el cumplimiento de los puntos descritos a continuación:

Inventario de activos: Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.

Propiedad de los activos: Los activos mantenidos en el inventario deberían tener un propietario.

Uso aceptable de los activos: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.

Devolución de activos: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

Clasificación de la información: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

Etiquetado de la información: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.

Manejo de activos: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización[3].

vii. CLASIFICACIÓN DE ACUERDO CON LA INTEGRIDAD

La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción. En esta guía se recomienda el siguiente esquema de clasificación de tres (3) niveles:

A **(ALTA)**	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
M **(MEDIA)**	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.

[3] Guía No. 5 para la Gestión y Clasificación de Activos de Información. MINTIC.

B **(BAJA)**	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

Tabla 4 Esquema de clasificación por integridad

viii. CLASIFICACIÓN DE ACUERDO CON LA DISPONIBILIDAD

La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso.

En esta guía se recomienda el siguiente esquema de clasificación de tres (3) niveles:

1 **(ALTA)**	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
2 **(MEDIA)**	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
3 **(BAJA)**	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

Tabla Esquema de clasificación por integridad

ix. IDENTIFICAR LOS RIESGOS INHERENTES DE SEGURIDAD DIGITAL

En esta fase[4] se utilizará la “Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas” del DAFP y la política integral de Riesgos del IMDERTY.

[4] MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL (MGRSD). MINTIC. 2018

En este caso, se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad digital:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles **amenazas** y **vulnerabilidades** que podrían causar su materialización. A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados:

Identificación de Amenazas:

Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan las siguientes amenazas:

- Deliberadas (D), Fortuito (F) o Ambientales (A).

Tabla 5. Tabla de amenazas comunes

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua	E
	Fallas en el suministro de aire acondicionado	F, D, A
Perturbación debida a la radiación	Radiación electromagnética	F, D, A
	Radiación térmica	F, D, A
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida	D
	Espionaje remoto	D
Fallas técnicas	Fallas del equipo	D, F
	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F
Acciones no autorizadas	Uso no autorizado del equipo	D, F

Tipo	Amenaza	Origen
	Copia fraudulenta del software	D, F
Compromiso de las funciones	Error en el uso o abuso de derechos	D, F
	Falsificación de derechos	D

Fuente: ISO/IEC 27005:2009

- Amenazas dirigidas por el hombre: empleados con o sin intención, proveedores y piratas informáticos, entre otros.

Tabla 6. Tabla de amenazas dirigida por el hombre

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto Ego	Piratería Ingeniería social
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información	Crimen por computador Acto fraudulento
Terrorismo	Chantaje Destrucción	Ataques contra el sistema DDoS Penetración en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa Hurto de información
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ganancia monetaria	Asalto a un empleado Chantaje

Fuente: ISO/IEC 27005:2009

Identificación de vulnerabilidades:

El IMDERTY puede identificar vulnerabilidades (debilidades) en las siguientes áreas:

Tabla 7. Tabla de Vulnerabilidades Comunes

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección

Tipo	Vulnerabilidades
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Fuente: ISO/IEC 27005

NOTA: *La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza* ***puede*** *no requerir la implementación de un control.*

A continuación, se presentan ejemplos de relación entre vulnerabilidades de acuerdo con el tipo de activos y las amenazas.

Tabla 8. Tabla de Amenazas y Vulnerabilidades

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

x. IDENTIFICACIÓN DEL RIESGO INHERENTE DE SEGURIDAD DIGITAL:

Para cada tipo de activo o grupo de activos pueden existir una serie de riesgos, que se deben identificar, valorar y posteriormente tratar si el nivel de dicho riesgo lo amerita.

Adicionalmente, se debe identificar el dueño del riesgo, es decir, "quien tiene que rendir cuentas sobre el riesgo o quien tiene la autoridad para gestionar el riesgo"[5].

xi. IDENTIFICACIÓN Y EVALUACIÓN DE LOS CONTROLES EXISTENTES

Acorde con lo indicado en la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas" del DAFP y la política integral de Riesgos del IMDERTY, y una vez establecidos y valorados los riesgos inherentes se procede a la identificación y evaluación de los controles existentes para evitar trabajo o costos innecesarios.

[5] GTC 137 Gestión del Riesgo. Vocabulario

Nota: Para determinar si existen uno o varios controles asociados a los riesgos inherentes identificados se puede consultar la sección 4. OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA (Tomados del Anexo A de la Norma ISO/IEC 27001:2013) como un insumo base y determinar si ya posee alguno de los controles orientados a seguridad digital que están enunciados en dicho anexo.

xii. TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DIGITAL

Identificado los riesgos, se debe definir el tratamiento para cada uno de los riesgos analizados y evaluados, conforme a los criterios y al **apetito de riesgo** definidos previamente en la Política Integral de Administración de Riesgos del IMDERTY.

El tratamiento de los riesgos es un proceso cíclico, el cual involucra una selección de opciones para modificarlos, por lo tanto, que tiene en cuenta lo establecido en la política institucional.

Nota Importante: Si la entidad pública decide mitigar o tratar el riesgo mediante la selección de controles que permitan disminuir la probabilidad o el impacto del riesgo, deberá tener en cuenta la Sección 4. OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA, basados en la norma ISO/IEC 27001:2013 en su Anexo A, como un insumo base para mitigar los riesgos de seguridad digital, sin embargo, la entidad pública puede implementar nuevos controles de seguridad que no estén incluidos dentro del Anexo, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo.

xiii. PLANES DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL E INDICADORES PARA LA GESTIÓN DEL RIESGO

Los planes de tratamiento de riesgos y los indicadores para medir la eficacia o la efectividad se generan teniendo en cuenta la “Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas” emitida por el DAFP y la Política Integral de Riesgos del IMDERTY.

e. FASE DE EJECUCIÓN

Se implementan los planes de tratamiento de riesgos definidos en la fase anterior, siguiendo la ruta crítica definida, llevando a cabo lo definido en la FASE 1.

La ejecución se realiza teniendo en cuenta la asignación de Roles y Responsabilidades, definidos en la Política Integral de Riesgos del IMDERTY.

f. FASE DE MONITOREO Y REVISIÓN

El IMDERTY a través de las tres Líneas de defensa de la matriz de Roles y Responsabilidades, definidos en la Política Integral de Riesgos, realizara un seguimiento a los planes de tratamiento para determinar su efectividad, teniendo en cuenta lo siguiente:

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.
- Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.
- Realizar monitoreo de los riesgos y controles tecnológicos.
- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

En esta fase se evalúan periódicamente los riesgos residuales para determinar la efectividad de los planes de tratamiento y de los controles propuestos, de acuerdo con lo definido en la Política Integral de Riesgos del IMDERTY. Así mismo, también tendrán en cuenta los incidentes de seguridad digital que hayan afectado a la entidad y también las métricas o indicadores definidos para hacer seguimiento a las medidas de seguridad implementadas. Lo anterior contribuye a la toma de decisiones en el proceso de revisión de riesgo por parte de la línea estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y las partes interesadas.

i. REGISTRO Y REPORTE DE INCIDENTES DE SEGURIDAD DIGITAL

Se realizará el registro de los incidentes de seguridad digital que se hayan materializado, con el fin de analizar las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar.

El propósito fundamental del registro de incidentes es garantizar que se tomen las acciones adecuadas para evitar o disminuir su ocurrencia, retroalimentar y fortalecer la identificación y gestión de dichos riesgos y enriquecer las

estadísticas sobre amenazas y vulnerabilidades y, con esta información, adoptar nuevos controles.

ii. REPORTE DE LA GESTIÓN DEL RIESGO DE SEGURIDAD DIGITAL AL INTERIOR DE LA ENTIDAD PÚBLICA

El responsable de seguridad digital asignado, reporta periódicamente a la Línea Estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y a las partes interesadas la siguiente información:

1. Matriz de Riesgos identificados
2. Listados de Activos críticos
3. Reporte de Criticidad/Impacto del IMDERTY
4. Plan de tratamientos de Riesgos
5. Reporte de evolución de Riesgos y modificación del apetito de Riesgo
6. Cantidad de Riesgos por fuera de la tolerancia de riesgos identificados de acuerdo con la periodicidad de evaluación realizada.
7. Impacto económico que podría presentarse frente a la materialización del riesgo.

Periodicidad

Cuando ocurra un cambio organizacional o de los procesos que genere un impacto en la operación o que pueda afectarlos riesgos ya identificados. En este caso debe efectuarse una nueva evaluación de riesgos y reportar los resultados a las partes interesadas.

iii. AUDITORÍAS INTERNAS Y EXTERNAS

Se realizará la evaluación (aseguramiento) sobre la gestión del riesgo de seguridad digital, conforme al Plan Anual de Auditoría aprobado por el Comité Institucional de Coordinación de Control Interno de la entidad.

iv. MEDICIÓN DEL DESEMPEÑO

El IMDERTY realizara la medición del desempeño con base en los indicadores para la gestión de los riesgos de seguridad digital, las cuales deben reflejar el cumplimiento de los objetivos propuestos.

g. FASE DE MEJORAMIENTO CONTINUO DE LA GESTIÓN DEL RIESGO DE SEGURIDAD DIGITAL

Se establece que cuando existan hallazgos, falencias o incidentes de seguridad digital se mitiga el impacto de su existencia y se toman acciones para controlarlos y prevenirlos. Adicionalmente, se establecen acciones por las consecuencias propias de la no conformidad que llegó a materializarse.

Se definen las siguientes acciones para mejorar continuamente la gestión de riesgos de seguridad digital:

- Revisión y evaluación de los hallazgos encontrados en las auditorías internas, otras auditorías e informes de los entes de control realizadas.
- Definir las posibles causas y consecuencias del hallazgo.
- Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.
- Emprender acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la entidad pública o de los servicios que presta al ciudadano.

ANEXO 1: PLAN DE TRABAJO MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

FASE	OBJETIVO	ACTIVIDAD	2020				2021				2022				2023			
			TRIMESTRE1	TRIMESTRE2	TRIMESTRE3	TRIMESTRE4	TRIMESTRE1	TRIMESTRE2	TRIMESTRE3	TRIMESTRE4	TRIMESTRE1	TRIMESTRE2	TRIMESTRE3	TRIMESTRE4	TRIMESTRE1	TRIMESTRE2	TRIMESTRE3	TRIMESTRE4
PLANIFICACIÓN	Establecer las actividades y procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información establecidos en el MSPI	Establecer Política de Seguridad de la Información																
		Establecer manual de gestión de Seguridad de la Información																
		Actualizar el manual de seguridad de la información																
		Actualizar la política de seguridad de la información																
		Validar seguridad en aplicaciones de la Entidad																
		Establecer roles y responsabilidades al interior del IMDERTY																
		Definir guía e instrumento para el levantamiento y clasificación de activos de información																
		Realizar levantamiento y clasificación de activos de información																
		Establecer contexto de los riesgos de seguridad de la información																
		Identificar riesgos de seguridad de la información																
		Realizar análisis de riesgos de seguridad de la información																
		Realizar evaluación de los riesgos de seguridad de la información																

ANEXO 1: PLAN DE TRABAJO MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

FASE	OBJETIVO	ACTIVIDAD	2020				2021				2022				2023			
			TRIMESTRE1	TRIMESTRE2	TRIMESTRE3	TRIMESTRE4	TRIMESTRE1	TRIMESTRE2	TRIMESTRE3	TRIMESTRE4	TRIMESTRE1	TRIMESTRE2	TRIMESTRE3	TRIMESTRE4	TRIMESTRE1	TRIMESTRE2	TRIMESTRE3	TRIMESTRE4
		Establecer declaración de aplicabilidad																
		Diseñar el plan de sensibilización y capacitación de sensibilización y capacitación en seguridad de la información																
		Implementar el programa de sensibilización y capacitación en seguridad de la información																
		Establecer y documentar procedimientos de seguridad de la información																
IMPLEMENTACIÓN	Ejecutar actividades, controles y medidas de protección que permitan la mitigación de riesgos de seguridad de la información	Implementar plan de tratamiento de riesgos de seguridad de la información																
		Establecer el plan de contingencias de los sistemas de información y servicios de TI																
		Definir componentes para la continuidad del negocio																
		Realizar análisis de impacto del negocio																
EVALUACIÓN DE DESEMPEÑO	Hacer seguimiento y medición a la implementación del MSPI.	Realizar plan de seguimiento y revisión de la efectividad de la implementación del MSPI.																
		Ejecución de auditorías																
		Medir la efectividad de los controles y políticas definidas																
		Revisar los niveles de riesgos.																

ANEXO 1: PLAN DE TRABAJO MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN																			
FASE	**OBJETIVO**	**ACTIVIDAD**	**2020**				**2021**				**2022**				**2023**				
			TRIMESTRE1	**TRIMESTRE2**	**TRIMESTRE3**	**TRIMESTRE4**	**TRIMESTRE1**	**TRIMESTRE2**	**TRIMESTRE3**	**TRIMESTRE4**	**TRIMESTRE1**	**TRIMESTRE2**	**TRIMESTRE3**	**TRIMESTRE4**	**TRIMESTRE1**	**TRIMESTRE2**	**TRIMESTRE3**	**TRIMESTRE4**	
		Actualizar los planes entorno a la seguridad de la información																	
MEJORA CONTINUA	Determinar los factores y/o aspectos a mejorar que hacen parte del MSPI	Desarrollar plan de mejora continua																	