ADR
Agencia de Desarrollo Rural

Plan de Tratamiento de Riesgos de Seguridad Digital -ADR 2021

OFICINA DE TECNOLOGÍAS DE INFORMACIÓN

El campo es de todos

Minagricultura

REVISORES Y APROBACIONES

Titulo	Plan de Tratamiento de Riesgos de Seguridad Digital -ADR 2021
Revisor	Víctor Manuel Mondragón Maca
Fecha	Enero de 2021
Cargo	Jefe de la Oficina TIC - CIO

Aprobación	Plan Estratégico de Tecnologías de Información de la Agencia de Desarrollo Rural – ADR 2019-2022
Aprobación	Comité Institucional de Gestión y Desempeño
Fecha	Enero de 2021

TABLA DE CONTENIDO

1. INTRODUCCIÓN 6
2. OBJETIVO 7
OBJETIVOS ESPECÍFICOS 7
3. ALCANCE DEL DOCUMENTO 7
4. TERMINOS Y DEFINICIONES 7
5. CONTEXTO NORMATIVO 8
6. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO ADR 10
7. ESTABLECIMIENTO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN 10
8. METODOLOGÍA DE IMPLEMENTACIÓN DEL PLAN 10
8.1 Identificación de los activos de seguridad de la información 11
8.2 Identificación del riesgo de seguridad Digital 13
8.3 Valoración de riesgo de seguridad Digital 15
8.4 Controles asociados a la seguridad de la información 17
9. MAPA DE RUTA 20
10. INDICADOR 20
11. BIBLIOGRAFÍA 21

LISTA DE TABLAS

Tabla 1 Conceptos y definiciones 8
Tabla 2 Activos 11
Tabla 3. Ejemplo identificación activos del proceso 12
Tabla 4. Tabla de amenazas y vulnerabilidades de acuerdo con el tipo de activo 13
Tabla 5. Controles para riesgos de seguridad de la información 18
Tabla 6. Mapa de Ruta Plan Riesgos de seguridad Digital ADR 2021 20
Tabla 7. Indicador de Plan Riesgos de seguridad Digital ADR 2021 21

LISTA DE ILUSTRACIONES

Ilustración 1. Metodología para la administración de Riesgo 11
Ilustración 2. Pasos para la identificación y valoración de activos 12
Ilustración 3. Formato de descripción del riesgo de seguridad de la información .. 14
Ilustración 4. Valoración del riesgo en seguridad de la información 17
Ilustración 5. Formato mapa riesgos seguridad de la información 19

1. INTRODUCCIÓN

La Agencia de Desarrollo Rural -ADR, presenta a los grupos de interés, y a la ciudadanía el Plan de Tratamiento de Riesgos de Seguridad Digital para la vigencia 2021, que permita la protección de los recursos, alcanzar mejores resultados y mejorar la prestación de servicios con aspectos fundamentales frente a la generación de valor público, eje fundamental en el que hacer de todas las organizaciones públicas. Es importante resaltar que el Departamento Administrativo de la Función Pública, como entidad técnica, estratégica y transversal del Gobierno nacional, pone a disposición de las entidades del estado la a actualización de la metodología para la administración del riesgo, por medio de la "Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 del 2020", en la cual se actualizaron y precisaron algunos elementos metodológicos para mejorar el ejercicio de identificación y valoración del riesgo, si afectar la estructura general de las primeras versiones. Así las cosas se incluye dentro de la actualización el ítem 5 .Lineamientos riesgos de seguridad de la información de la guía, así como una matriz propuesta para la construcción del mapa de riesgos y se actualiza el Anexo 4 : Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas del Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC) y se mantiene el protocolo para la identificación de riesgos de corrupción, asociados a la prestación de trámites y servicios, en el marco de la política de racionalización de trámites, liderado por la dirección de participación, transparencia y servicio al ciudadano de Función Pública.

El presente documento contiene el Plan de Tratamiento de Riesgos de Seguridad Digital - ADR 2021, para el análisis, valoración y tratamiento de riesgos de Seguridad, alineados con las políticas de seguridad y privacidad de la información, con objetivos, generalidades, contexto, contexto normativo, definiciones, metodología de implementación y mapa de ruta con las actividades a ejecutar con fechas y responsables, con el fin de ser desarrolladas por la Entidad y de esta manera se logre mejorar la gestión de Riesgos de Seguridad Digital, a fin de incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información de la Entidad..

2. OBJETIVO

El presente documento tiene como objetivo definir los lineamientos y metodología a seguir para el análisis, valoración y tratamiento de riesgos de Seguridad Digital, alineados con las políticas de seguridad y privacidad de la información, con el fin de mantener la integridad, confidencialidad y disponibilidad de la información a través de la gestión del riesgo asociado a la información de la Agencia de Desarrollo Rural – ADR

OBJETIVOS ESPECÍFICOS

Validar la metodología de riesgos de la Agencia de Desarrollo Rural -ADR, para la vigencia 2021 en lo relacionado a aquellos que puedan afectar la integridad, confidencialidad y disponibilidad de la información.

Identificar durante el 2021 los riesgos en los procesos de la ADR, que puedan afectar la integridad, confidencialidad y disponibilidad de la información.

Hacer seguimiento en el 2021 a los riesgos en los procesos del Instituto, que puedan afectar la integridad, confidencialidad y disponibilidad de la información.

3. ALCANCE DEL DOCUMENTO

El Plan de Tratamiento de Riesgos de Seguridad Digital -ADR, se aplica para todos los procesos del ADR, en el cumplimiento de la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI)[1], el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital[2]: seguridad de la información, arquitectura, servicios ciudadanos digitales.

debido al cumplimiento que las entidades públicas cumplen de mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”, siempre y cuando se ajusten al análisis de riesgos

4. TERMINOS Y DEFINICIONES

A continuación, se relacionan una serie de conceptos, necesarios para la comprensión basados en la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 del 2020.

[1] https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

2 Entiéndase por habilitadores transversales de la Política de Gobierno Digital: Arquitectura, Seguridad y privacidad y Servicios Ciudadanos Digitales, como elementos de base que permiten el desarrollo de los componentes de la política.

Tabla 1 Conceptos y definiciones

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.	**Riesgo de Seguridad de la Información:** 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. (ISO/IEC 27000).	**Riesgo de Corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado	**Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Est ará asociad a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo	**Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.	**Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.	**Riesgo Inherente**: Nivel de riesgo propio de la actividad. El resultado de combina la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad
Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.	**Control:** Medida que permite reducir o mitigar un riesgo.	**Causa Inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.	**Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
Factores de Riesgo: Son las fuentes generadoras de riesgos.	**Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados	**Integridad:** Propiedad de exactitud y completitud.	**Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.

Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020 .

5. CONTEXTO NORMATIVO

El Plan de Tratamiento de Riesgos de Seguridad Digital para la Agencia de Desarrollo Rural (ADR), se define teniendo en cuenta las principales normas relacionadas con el accionar misional de la Entidad, el Sector Agropecuario y Pesquero, el Sector de las Tecnologías de la Información y las Comunicaciones asociada a los temas de la Política de Gobierno Digital, Arquitectura de Información, el Modelo de Gestión Estratégica de TI y el Modelo integrado de Planeación y Gestión (MIPG) (Departamento Administrativo de la Función Pública de Colombia, 2017).

Ley 527 de 1999 (Comercio Electrónico) Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Se tratan conceptos como: mensaje de datos (artículos 2º y 5º), el principio de equivalencia funcional (artículos 6º, 8º, 7º, 28º, 12º y 13º), la autenticación electrónica (artículo 17º), la firma

electrónica simple (artículo 7º), la firma digital (artículo 28º), y la firma electrónica certificada (artículo 30º, modificado por el artículo 161 del Decreto Ley 019 de 2012)

Ley Estatutaria 1581 de 2012 "Régimen General de Protección de Datos Personales", y el artículo 2.2.2.25.3.1. del Decreto 1074 de 2015 "Decreto Único Reglamentario del Sector Comercio Industria y Turismo", consagraron la necesidad de garantizar de forma integral la protección y el ejercicio del derecho fundamental de Habeas Data y estableció dentro de los deberes de los responsables del tratamiento de datos personales, desarrollar políticas para este derecho.

Ley 1712 de 2014, sobre transparencia y derecho de acceso a la información pública nacional, adiciona nuevos principios, conceptos y procedimientos para el ejercicio y garantía del referido derecho; junto con lo dispuesto en el Decreto 1080 de 2015, "por medio del cual se expide el Decreto Reglamentario Único del Sector Cultura", el cual establece las directrices para la calificación de información pública, y se establecen los instrumentos de la gestión de información pública (1) Registro de Activos de Información; (2) Índice de Información Clasificada y Reservada; (3) Esquema de Publicación de Información; (4) Programa de Gestión Documental.

Decreto 1078 de 2015 "por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones" modificado mediante el Decreto 1008 de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", en el artículo 2.2.9.1.1.3. incluye la seguridad de la información entre los principios de la Política de Gobierno Digital, de igual manera, en el artículo 2.2.9.1.2.1. se establece que la Política de Gobierno Digital se desarrollará a través de componentes y habilitadores transversales y respecto de estos últimos indica que son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital. (Comunicaciones, 2018)

Decreto 612 de 2018: "Por el cual se fijan las directrices para la integración de los planes institucionales y estratégicos al plan de acción por parte de las entidades del estado".

Resolución No. 0409 de 2019: "Por la cual se adopta la política de seguridad y privacidad de la información de la Agencia de Desarrollo Rural - ADR y se definen lineamientos frente al uso y manejo de la información"

ISO/IEC 27001:2013: Es la evolución certificable del código de buenas prácticas ISO 17799. Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información

· CONPES 3854 de 2020. Política Nacional De Confianza Y Seguridad Digital

· CONPES 3854 de 2016. Política Nacional de Seguridad digital.

· CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

Adicionalmente, la ADR sigue estándares y buenas prácticas utilizados en TI, bajo las Normas ISO 9001, ISO 22301, ISO 31000, OCTAVE allegro, la NTC 5854 para accesibilidad de páginas web, ITIL, TOGAF, COBIT, entre otras.

6. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO ADR

La Agencia de Desarrollo Rural – ADR cuenta con la política de administración del riesgo publicada DE-SIG-002, tomando como referente los lineamientos impartidos en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas", emitida por el Departamento Administrativo de la Función Pública -DAFP. Esta política está articulada con el Sistema Integrado de Planeación y Gestión, y demás normas aplicables a la Entidad.

Así mismos establece lineamientos y parámetros basados en una adecuada gestión del riesgo asociados a los procesos, planes, programas, proyectos y control a los mismos, que le permitan a la Agencia de Desarrollo Rural-ADR asegurar de manera razonable el logro de los objetivos institucionales.

7. ESTABLECIMIENTO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

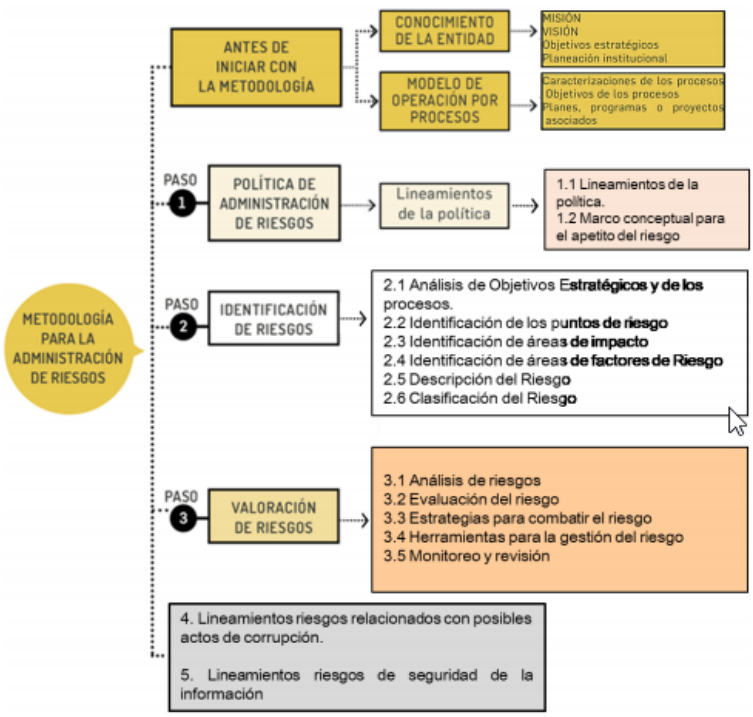
El comité institucional de gestión y desempeño – MIPG, mediante la resolución 1602 de 2017 "Por la cual crea el Comité Institucional de Desarrollo Administrativo de la Agencia de Desarrollo Rural, como instancia orientadora del Modelo Integrado de Planeación y Gestión y se establece su reglamentación" y en su lugar se integra el Comité Institucional de Gestión y Desempeño de la Agencia de Desarrollo Rural.

8. METODOLOGÍA DE IMPLEMENTACIÓN DEL PLAN

Con el fin de efectuar el proceso de implementación del presente Plan, se hará uso de la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 del 2020[3]. En los Lineamientos riesgos de seguridad de la información, en el cual se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales

[3] https://www.funcionpublica.gov.co/documents/28587410/34298398/2020-12-16_Guia_administracion_riesgos_dise%C3%B1o_controles_final.pdf/fa179c5e-45bb-dffd-027c-043d4733c834?t=1609857497641

Ilustración 1. Metodología para la administración de Riesgo



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

8.1 Identificación de los activos de seguridad de la información

Como primer paso para la identificación de riesgos de seguridad digital para la ADR, es necesario identificar los activos de información del proceso.

Tabla 2 Activos

¿Qué son los activos?	¿Por qué identificar los activos?
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 organización -Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	Permite determinar **qué es lo más importante que cada entidad y sus procesos poseen** (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios). La entidad puede saber **qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano** , aumentando así su confianza en el uso del entorno digital

Fuente: Actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública y Ministerio TIC, 2020

Realizar la identificación de los activos de seguridad digital con los pasos de identificación de activos

Ilustración 2. Pasos para la identificación y valoración de activos

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

para realizar la identificación de activos deberá remitirse a la sección 3.1.6 del anexo 4 "Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas" que hace parte de los anexos de la presente guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 del 2020.

Tabla 3. Ejemplo identificación activos del proceso

Proceso	Activo	Descripción	Dueño del activo	Tipo del activo	Ley 1712 de 2014	Ley 1581 de 2012	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Gestión financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe de oficina financiera	Información	Información reservada	No contiene datos personales	ALTA	ALTA	ALTA	ALTA
Gestión financiera	Aplicativo de nómina	Servidor web que contiene el *front office* de la entidad	Jefe de oficina financiera	Software	N/A	N/A	BAJA	MEDIA	BAJA	MEDIA
Gestión financiera	Cuentas de cobro	Formatos de cobro diligenciados	Jefe de oficina financiera	Información	Información pública	No contiene datos personales	BAJA	BAJA	BAJA	BAJA

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones Min TIC 2018

8.2 Identificación del riesgo de seguridad Digital

se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

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. Para este efecto, es necesario consultar el Anexo 4 Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas donde se encuentran las siguientes tablas necesarias para este análisis:

Tabla de amenazas comunes
Tabla de amenazas dirigida por el hombre
Tabla de vulnerabilidades comunes

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.

Tabla 4. Tabla de amenazas y vulnerabilidades de acuerdo con el tipo de activo

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 Min TIC 2018

En la ilustración número 3, se observa un ejemplo de identificación del riesgo sobre un activo como es la base de datos de nómina

Ilustración 3. Formato de descripción del riesgo de seguridad de la información

Seleccionar las vulnerabilidades asociadas a la amenaza identificada

RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/ VULNERA-BILIDADES	CONSECUENCIAS
Base de datos de nómina	Pérdida de la integridad	La falta de políticas de seguridad digital, ausencia de políti-cas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina.	Modificación no autorizada	Seguridad digital	Falta de políticas de seguridad digital	Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo(legales, económicas, sociales, reputacionales, confianza en el ciudadano). Ej.: posible retraso en el pago de nómina.
					Ausencia de políticas de control de acceso	
					Contraseñas sin protección	
					Autenticación débil	

IMPORTANTE

* Existirían tres (3) tipos de riesgos: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.
* Los catálogos de amenazas y vulnerabilidades comunes se encuentran en la sección 4.1.7. del **anexo "Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas"**, el cual hace parte de la presente guía.
* **NOTA 1:** tener en cuenta que la agrupación de activos debe ser del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.
* **NOTA 2:** las entidades públicas deben incluir como mínimo los procesos y procedimientos establecidos en esta guía. Aquellas entidades que ya estén adelantando procesos relacionados con la gestión de este tipo de riesgo y que incorporen al menos lo dispuesto en estas guías podrán continuar bajo sus procedimientos. Si alguno de los aspectos contenidos en esta guía no está contemplado, deberá ser agregado a los que manejan actualmente.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

8.3 Valoración de riesgo de seguridad Digital

Para esta etapa se asociarán las tablas de probabilidad e impacto definidas en la primera parte de la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 del 2020

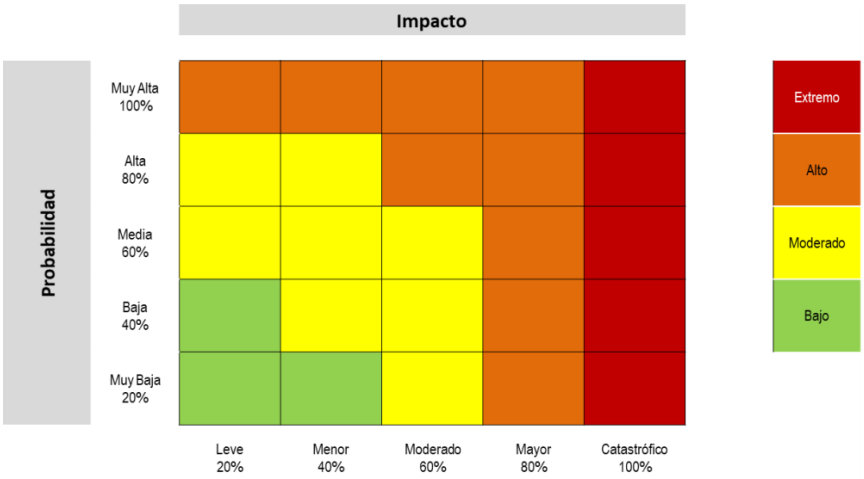
	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

La determinación del impacto se debe llevar a cabo entendiendo que el impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo.

En este sentido, se debe considerar para este análisis la tabla,

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Para el análisis preliminar (riesgo inherente), en esta etapa se define el nivel de severidad para el riesgo de seguridad de la información identificado, para ello, se aplica la matriz de calor:



En la Ilustración 3, se observa un ejemplo aplicando la etapa de valoración del riesgo sobre un activo como es la base de datos de nómina.

IMPORTANTE

Cada entidad deberá adaptar los criterios a su realidad.
El nivel de impacto deberá ser determinado con la presencia de cualquiera de los criterios establecidos, tomando el criterio con mayor nivel de afectación, ya sea cualitativo o cuantitativo.

Las variables confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.

La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados. Los porcentajes en las escalas pueden variar, según la entidad y su contexto.

La variable presupuesto es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.

La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.

Ilustración 4. Valoración del riesgo en seguridad de la información

RIESGO	ACTIVO	AMENAZA	VULNERABILI-DAD	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
Pérdida de la Confiden-cialidad	Base de datos de nómina	Modificación no autorizada	Ausencia de políticas de control de acceso	4-Probable	4- Mayor	Extrema
			Contraseñas sin protección			
			Ausencia de mecanismos de identificación y autenticación de usuarios			
			Ausencia de bloqueo de sesión			

Fuente: Adaptado de Instituto de Auditores Internos. COSO ERM. Agosto 2004.

Extremo
Alto
Moderado
Bajo

IMPORTANTE:
La probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

8.4 Controles asociados a la seguridad de la información

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4[4], "Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas", siempre y cuando se ajusten al análisis de riesgos.
Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

[4] https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b

A continuación, se incluyen algunos ejemplos de controles y los dominios a los que pertenecen, la lista completa se encuentra en del documento maestro del modelo de seguridad y privacidad de la información (MSPI):

Tabla 5. Controles para riesgos de seguridad de la información

Procedimientos operacionales y responsabilidades	**Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información**
Procedimientos de operación documentados	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	Control: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Control: se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos	Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	Objetivo: proteger la información contra la perdida de datos.
Respaldo de información	Control: se deberían hacer copias de respaldo de la información, del *software* y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones Min TIC 2018

Ilustración 5. Formato mapa riesgos seguridad de la información

N.	RIESGO	ACTIVO	TIPO	AMENAZAS	TIPO	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN TRATAMIENTO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
2	**Pérdida de la integridad**	Base de datos de nómina	Seguridad digital	Modificación no autorizada	Ausencia de políticas de control de acceso	**Probable**	**Menor**	**Moderado**	Reducir	A.9.1.1 Política de control de acceso	Política creada y comunicada	Oficina TI	Tercer trimestre de 2018	**EFICACIA:** Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD:** Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)
					Contraseñas sin protección				Reducir	A.9.4.3 Sistema de gestión de contraseñas	Procedimientos para la gestión y protección de contraseñas	Oficina TI	Tercer trimestre de 2018	
					Ausencia de mecanismos de identificación y autenticación de usuarios				Reducir	A 9.4.2 Procedimiento de ingreso seguro	Procedimiento para ingreso seguro	Oficina TI	Tercer trimestre de 2018	
					"Ausencia de bloqueo				Reducir	A.11.2.8 Equipos de usuario desatendidos	Configuraciones para bloqueo automático de sesión	Oficina TI	Tercer trimestre de 2018	

*En este ejemplo el responsable de las actividades de control fue la Oficina de TI, sin embargo existen actividades para el área de personal, recursos físicos o cada oficina en particular. El análisis de riesgos determinará los controles y los responsables en cada caso.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

Los riesgos identificados traen consigo controles que incluyen el monitoreo de los eventos correspondientes, invirtiendo los recursos de acuerdo con la criticidad del riesgo asociado, las responsabilidades del monitoreo comprenden todos los aspectos del proceso para la gestión del riesgo con el
fin de:

Garantizar que los controles son eficaces y eficientes tanto en el diseño como en la operación.
Obtener información adicional para mejorar la valoración del riesgo.
Analizar y aprender lecciones a partir de los eventos.
Detectar cambios en el contexto externo e interno, incluyendo los cambios en los criterios de riesgo y en el riesgo mismo que puedan exigir revisión de los tratamientos del riesgo y las prioridades

9. MAPA DE RUTA

A continuación, se presenta el mapa de ruta de actividades proyectadas en el presente Plan Riesgos de seguridad Digital ADR 2021.

Tabla 6. Mapa de Ruta Plan Riesgos de seguridad Digital ADR 2021

ID	ACTIVIDAD	FECHA INICIO	FECHA FINAL	RESPONSABLE	PRODUCTO O RESULTADO ESPERADO
1	Actualización metodología de Riesgos de Seguridad Digital	MARZO	ABRIL	Oficina de Tecnologias de la Información -OTI	Documento Matriz de riesgos
2	Información sobre la evaluación de riesgos de seguridad	MAYO	MAYO	Oficina de Tecnologias de la Información -OTI	Comunicaciones internas / Correo electrónico
3	Identificación y Análisis de Riesgos Seguridad Digital	ABRIL	JULIO	Todas las áreas y acompañamiento de Equipo OTI	Matriz de riesgos diligenciado
4	Publicación de riesgos de seguridad de información	AGOSTO	AGOSTO	Oficina de Tecnologias de la Información -OTI	Enlace en trasparencia del portal WEB
5	Tratamiento de Riesgos Seguridad de la Información	SEPTIEMBRE	SEPTIEMBRE	Todas las áreas y acompañamiento de Equipo OTI	Actas de reunión / correos electrónicos
6	Información de seguridad Seguimiento de Riesgos y Revisión Informe	NOVIEMBRE	DICIEMBRE	Todas las áreas y acompañamiento de Equipo OTI- Control Interno	Informe de riesgos

Fuente: OTI

10. INDICADOR

A continuación, se presenta el indicador proyectado para la evaluación del siguiente plan.

Tabla 7. Indicador de Plan Riesgos de seguridad Digital ADR 2021

Nombre del indicador	Gestión de riesgos
Propósito del indicador	Medir el nivel de implementación y ejecución de la metodología para la gestión de riesgos de seguridad digital
Objetivo de control o controles asociados	4.1 requerimientos generales.
	4.2.1 establecer el MSPI
	4.2.2 Implementar y Operar el MSPI
	8.3 Acción preventiva
	A.6.2.1. Identificación de riesgos de terceras partes
Destinatario	Todas las áreas y acompañamiento de Equipo OTI
Formula	Número de actividades realizadas en el Plan Riesgos de seguridad Digital/Número de actividades programadas en el Plan Riesgos de seguridad Digital *100%
Escala	Porcentaje
Nivel para el cumplimiento	85%
Frecuencia de medición	Anual
Nivel de cumplimiento	Medición corte a Diciembre

11. BIBLIOGRAFÍA

Comunicaciones, M. d. (1 de agosto de 2018). *Manual de Gobierno Digital.* (L. C. 4.0), Ed.) Obtenido de Implementación de la Política de Gobierno Digital Decreto 1078 de 2015 libro 2, parte 2, título 9. Cap. 1: http://estrategia.gobiernoenlinea.gov.co/623/articles-7929_recurso_1.pdf

Congreso de la Republica de Colombia. (29 de Julio de 2016). *Código Nacional de Policía y Convivencia*. (Policía Nacional de Colombia) Obtenido de https://www.policia.gov.co/sites/default/files/ley-1801-codigo-nacional-policia-convivencia.pdf

Departamento Administrativo de la Función Pública de Colombia. (2017). *Modelo Integrado de Planeación y Gestión -MIPG.* Función Pública. Bogotá D.C: F. Recuperado el 1 de 12 de 2017, de http://www.funcionpublica.gov.co/eva/mipg/index.html

Departamento de la Función Pública. (07 de marzo de 2016). *Decreto 415 de 07 de marzo de 2016.* Recuperado el 02 de 05 de 2018, de http://www.mintic.gov.co/portal/604/articles-61527_documento.pdf

Departamento de Planeación Nacional. (17 de abril de 2018). *CONPES 3920.* Recuperado el 1 de septiembre de 2018, de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3920.pdf

Ministerio de las Tecnologías de la Información y las Comunicaciones. (14 de junio de 2018). *Decreto 1008 de 2018 - política de Gobierno Digital* . Obtenido de https://www.mintic.gov.co/portal/604/w3-article-74903.html