
El futuro digital
es de todos
MinTIC

Noticias Falsas

https://coronaviruscolombia.gov.co/Covid19/noticias-falsas.html

Trabajo Remoto Seguro

#TrabajoRemotoSeguro

- Mantener actualizado el sistema operativo (iOS, Android. Windows, Linux)
- Utilizar múltiple factor de autenticación al realizar transacciones financieras
- Activar la conexión a la red empresarial a través de SSL/VPN. (Principio de Mínimo Privilegio)
- Instalar y mantener actualizado el software antivirus (reconocido), para evitar infecciones con virus o software malicioso
- Implementar cifrado en los equipos, servidores y herramientas transaccionales con el fin de mantener la protección de la información
- No instalar aplicaciones que exijan permisos que pongan en riesgo la información (acceso a la agenda, geolocalización, etc.).
- Garantizar y cumplir con las exigencias de seguridad de la Entidad y la Ley de protección de datos personales.
- Realizar backup en las plataformas dispuestas por la Entidad
- No enviar información de la Entidad, por medios no oficiales como whatsapp, Dropbox, WeTransfer, correos de dominio gratuito, etc.
- Cambiar las claves el acceso a wifi de la casa y evitar conectarse a redes inalámbricas abiertas

Modelo de Seguridad y Privacidad de la Información (MSPI)

Grupo interno de seguridad y privacidad de la información.

Política de Gobierno Digital

Decreto 1008 de 2018

Establece los lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea y se entiende como:

El uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

DECRETO Nº 1008 DE
14 JUN 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"

EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA

En ejercicio de sus facultades constitucionales y legales, en especial las que le confieren los artículos 189 numeral 11 de la Constitución Política, 14 de la Ley 790 del 2002, 1 numeral 4 de la Ley 962 de 2005, 64 de la Ley 1437 de 2011, 45 de la Ley 1753 de 2015, y,

CONSIDERANDO

Que la Constitución Política en su artículo 113 señala que los diferentes órganos del Estado tienen funciones separadas, pero colaboran armónicamente para la realización de sus funciones.

Que el numeral 8 del artículo 2 de la Ley 1341 de 2009 establece que el Gobierno Nacional fijará los mecanismos y condiciones para garantizar la masificación del Gobierno en Línea, con el fin de lograr la prestación de servicios eficientes a los ciudadanos, así mismo, la citada Ley determino que es función del Estado intervenir en el sector de las TIC, con el fin de promover condiciones de seguridad del servicio al usuario final, incentivar acciones preventivas y de seguridad informática y de redes para el desarrollo de dicho sector; así como reglamentar las condiciones en que se garantizará el acceso a la información en línea, de manera abierta, ininterrumpida y actualizada.

Que el documento CONPES 3650 del 15 de marzo de 2010 declara la importancia estratégica de la implementación de la Estrategia de Gobierno en línea en Colombia y exhorta al Ministerio de Tecnologías de la Información y las Comunicaciones, con el apoyo del Departamento Nacional de Planeación, a formular los lineamientos de política que contribuyan a la sostenibilidad de la Estrategia de Gobierno en Línea.

Modelo de Seguridad y Privacidad de la Información (MSPI)

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), a través de la Dirección de Estándares y Arquitectura de TI, dando cumplimiento a sus funciones, publica **El Modelo de Seguridad y Privacidad de la Información (MSPI)**, el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI.

El MSPI para estar acorde con las buenas prácticas de seguridad **será actualizado periódicamente**; reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información

Elementos Esenciales

- **Identificación de riesgos** de seguridad digital
- **Combinación de amenazas y vulnerabilidades** en el entorno digital.

- **Activo**
- **Servicios** esenciales, humanos y tecnológicos, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Propiedades de Seguridad de la información

Integridad

Disponibilidad

Confidencialidad

Objetivo del MSPI

Modelo de Seguridad y Privacidad de la Información

Promover el uso de **mejores prácticas en seguridad de la información**, como base de aplicación del concepto de Seguridad Digital, en las entidades públicas del Estado colombiano.

El Modelo está enfocado a **preservar la confidencialidad, integridad y disponibilidad** de la información.

Componentes del MSPI

Pasos

PASO 3
Gestión de los Riesgos de Seguridad Digital

- Identificación de amenazas y vulnerabilidades
- Análisis/Valoración del Riesgo
- Tratamiento del Riesgo

PASO 2
Identificación Y Gestión de Activos

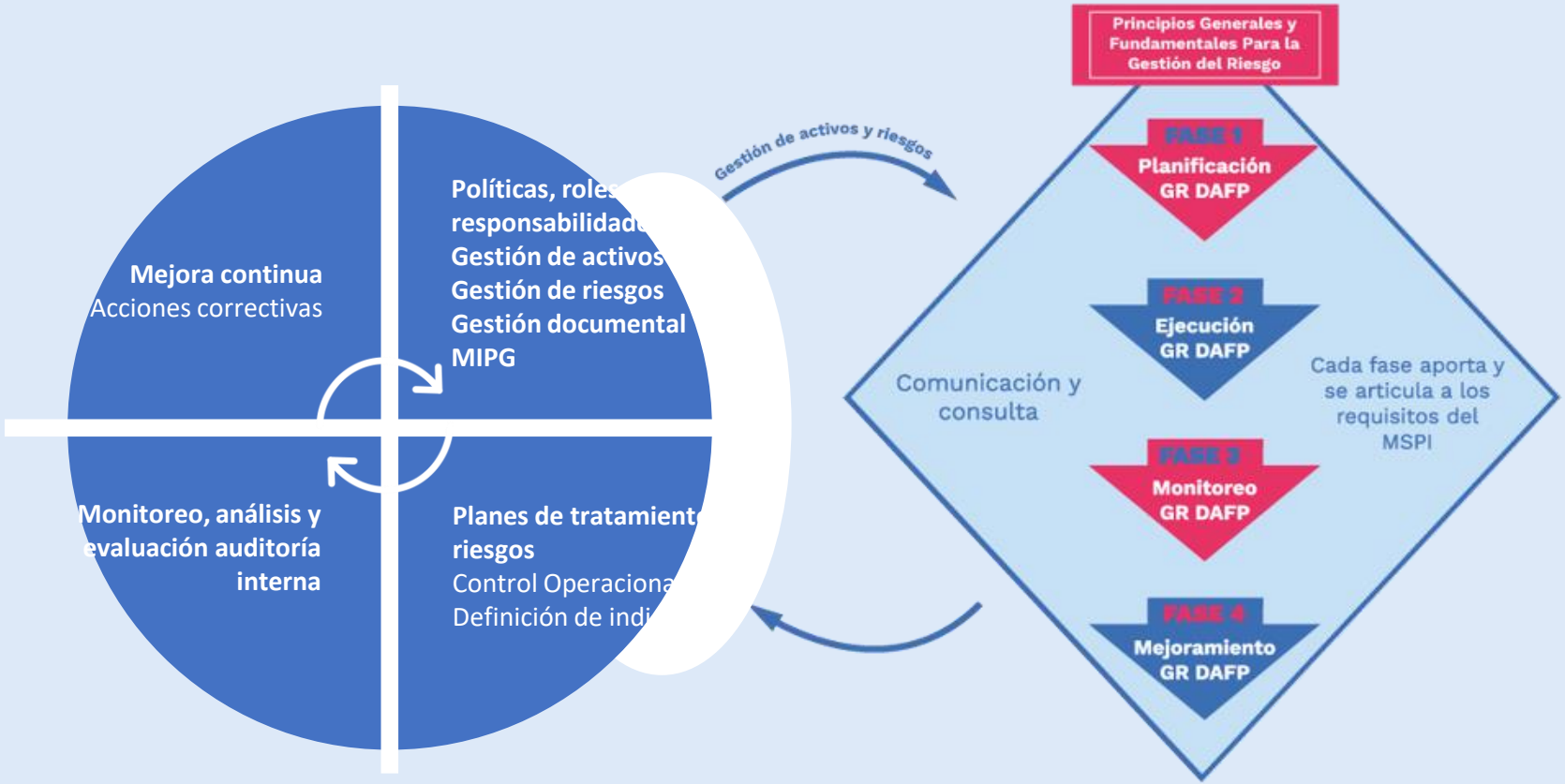
- Valoración de Activos
- Priorización de Activos

PASO 1
Política de seguridad de la información

- Formulación de una política alineada con el plan estratégico de T.I.

GOBERNANZA + PLANEACIÓN + ASEGURAMIENTO

Integración entre modelos



Componentes del **MSPI**

Instrumento para la identificación de la línea base de Seguridad de la información

El futuro digital es de todos — MinTIC

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD
HOJA PORTADA

Más Seguridad Digital Mejor Región — Gobierno Digital en las regiones

ENTIDAD EVALUADA	Nombre de la Entidad
FECHAS DE EVALUACIÓN	fecha de entrega
CONTACTO	contacto de la entidad
ELABORADO POR	Personal de la Entidad

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles — DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	0	100	INEXISTENTE
A.8	GESTIÓN DE ACTIVOS	0	100	INEXISTENTE
A.9	CONTROL DE ACCESO	0	100	INEXISTENTE
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	0	100	INEXISTENTE
A.12	SEGURIDAD DE LAS OPERACIONES	0	100	INEXISTENTE
A.13	SEGURIDAD DE LAS COMUNICACIONES	0	100	INEXISTENTE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0	100	INEXISTENTE
A.15	RELACIONES CON LOS PROVEEDORES	0	100	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	100	INEXISTENTE
A.18	CUMPLIMIENTO	0	100	INEXISTENTE
PROMEDIO EVALUACIÓN DE CONTROLES		0	100	INEXISTENTE

1. Política de Seguridad de la Información

Documentos de Referencia

Decreto 612 de 2018

- PETI
- PTRSPI
- PSPI

MSPI

- Gobernanza
- Activos
- Riesgos
- Mejora Continua

Manual de Gobierno Digital

Implementación de la política de Seguridad de la Información

Decreto 2106 de 2019

- Las autoridades que realicen trámites, procesos y procedimientos por medios digitales deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones

Documentos de Referencia

Manual operativo MIPG

- **Planes:** Objetivos, Estrategias, Proyectos, Metas, Acciones, Productos, Responsables, Cronogramas, Planes de compras, Distribución presupuestal de los proyectos de inversión, Indicadores , Mapas de riesgos.
- el **Comité Institucional de Gestión y Desempeño** debe asegurar la implementación de la política de seguridad
- designar un responsable de Seguridad de la Información el cual debe pertenecer a un área que haga parte de la Alta Dirección. Para las entidades cabeza de sector, el Responsable de Seguridad Digital será el enlace sectorial de seguridad digital.

Guía para la administración del riesgo

Anexo 4. Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas

2. Activos de información

Gestión de Activos

¿Qué son los activos?

Información | Software | Hardware | Redes | Personas | Instalaciones

¿Cómo identificar los activos?

Ejemplo

ACTIVO	TIPO DE ACTIVO	CRITICIDAD CON RESPECTO A SU CONFIDENCIALIDAD	CRITICIDAD CON RESPECTO A SU INTEGRIDAD	CRITICIDAD CON RESPECTO A SU DISPONIBILIDAD	NIVEL DE CRITICIDAD
BASES DE DATOS DE NÓMINA	Información	Alta	Alta	Alta	Alta
APLICATIVO DE FINANCIERO	Software	Alta	Media	Media	Media
SERVIDOR INTERNO	Hardware	Baja	Baja	Baja	Baja

¿Cómo identificar los activos?

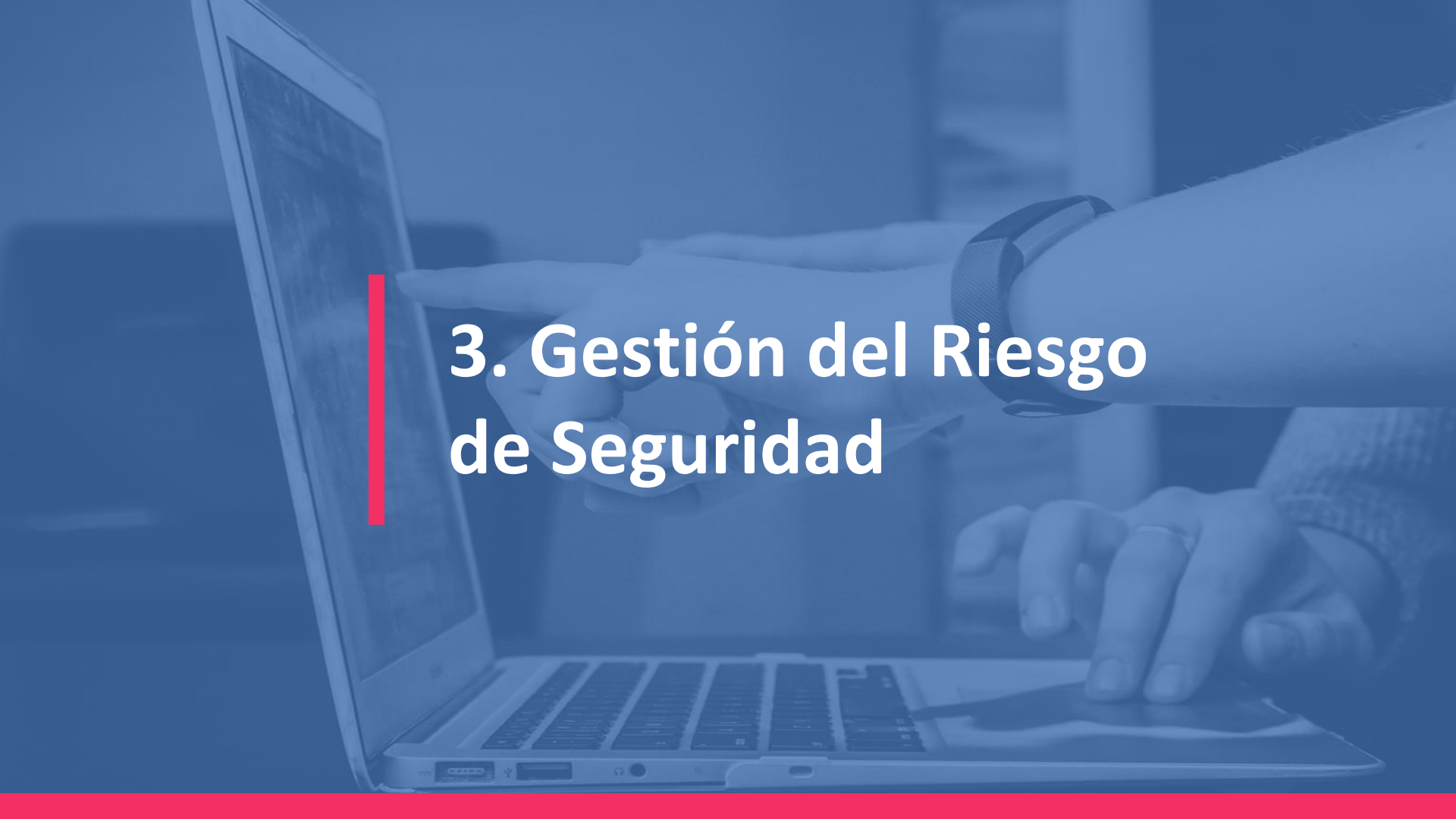
Infraestructura crítica cibernética

Criterios de identificación de ICC

IMPACTO SOCIAL	IMPACTO ECONÓMICO	IMPACTO AMBIENTAL
(0,5%) de Población Nacional	PIB de un Día o 0,123% del PIB Anual	
250.000 personas	$464.619.736	3 años en recuperación

Si la entidad pública determina que tiene ICC, es importante que **se identifiquen los componentes que conforman dicha infraestructura**. Por ejemplo, dicha ICC puede tener componentes de TI (como servidores) o de TO (como sistemas de control industrial o sensores).

Fuente: Tomado de Comando Conjunto Cibernético (CCOC), Comando General Fuerzas Militares de Colombia. Guía para la Identificación de Infraestructura Crítica Cibernética (ICC) de Colombia Primera



3. Gestión del Riesgo de Seguridad

Riesgos inherentes de Seguridad Digital a identificar:

Pérdida de la confidencialidad

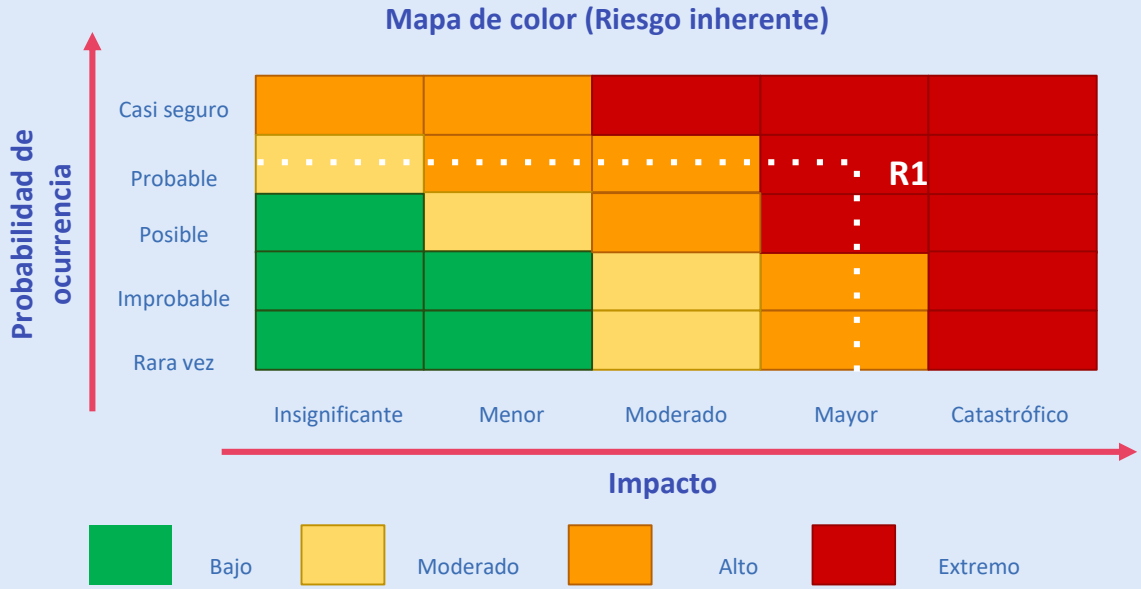
Pérdida de la integridad

Pérdida de la disponibilidad

Seleccionar las vulnerabilidades asociadas a la amenaza identificada

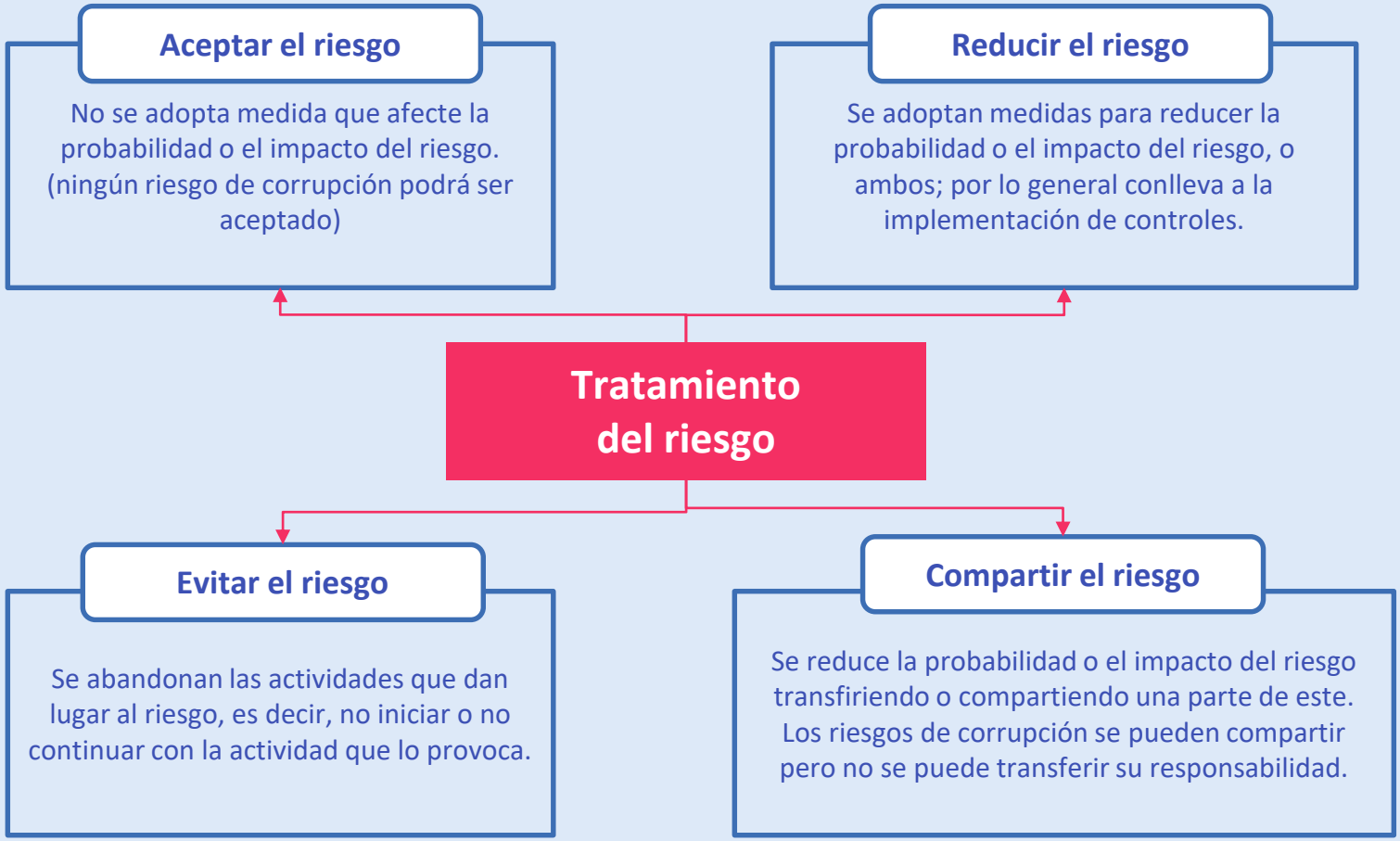
Activo	Riesgo	Descripción del riesgo	Amenaza	Tipo	Causa/ Vulnerabilidades	Consecuencias
Bases de datos de nómina	Pérdida de la integridad	Pérdida de datos por modificación, alteración y eliminación de información de la base de datos de nómina de entidad.	Falsificación de permisos	Información	**1.**Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario **2.**Gestión deficiente de las contraseñas **3.**Tablas de contraseñas sin protección	Pérdida de Dinero, Retraso en el pago de nómina, Demandas por incumpliendo de salarios, Plan tortuga funcionarios, Generación de desconfianza a los ciudadanos.
Servidor de base de datos	Pérdida de confidencialidad	Acceso no autorizado al servidor	Error de uso	Hardware	Ausencia de un eficiente control de cambios en la configuración	Ausencia de un eficiente control de cambios en la configuración Explotación de vulnerabilidades por falta de actualizaciones se seguridad y hardening
Servidor aplicación de impuestos	Pérdida de confidencialidad	Acceso no autorizado al servidor, donde se encuentran los datos de los contribuyentes para el pago de impuestos.	**Uso no autorizado del equipo** **Falsificación de derechos**	Hardware	**1.** Conexiones de red pública sin protección **2.** Arquitectura insegura de la red **3.** Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	**1.** Desconfianza ciudadanos, robo de información, cifrado de información (Ramsonware) **2.** Robo de información, activación de malware, escalamiento de privilegios, modificación y eliminación de datos.
Servidor Portal Web	Pérdida de disponibilidad	Servidor fuera de servicio, impidiendo que los usuarios autorizados no tengan acceso para descargar el recibo de pago de impuestos.	Saturación del sistema de información	Hardware	**1.** Arquitectura insegura de la red **2.** Ausencia de mecanismos de monitoreo	Impedir la descarga de los formatos de pago de impuestos

Gestión de riesgo



Mapa de calor

Se toma la calificación de probabilidad (resultante de la tabla Matriz de priorización de probabilidad), en el ejemplo: probable y la calificación de impacto, para nuestro ejemplo: mayor; ubique la calificación de probabilidad en la fila y la de impacto en la columnas correspondientes, establezca el punto de cruce de las dos y este punto corresponderá al nivel de riesgo, que para el ejemplo es nivel extremo – color rojo determinando así el riesgo inherente.


Aceptar el riesgo
No se adopta medida que afecte la probabilidad o el impacto del riesgo. (ningún riesgo de corrupción podrá ser aceptado)
Reducir el riesgo
Se adoptan medidas para reducer la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.
Tratamiento del riesgo
Evitar el riesgo
Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.
Compartir el riesgo
Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir pero no se puede transferir su responsabilidad.

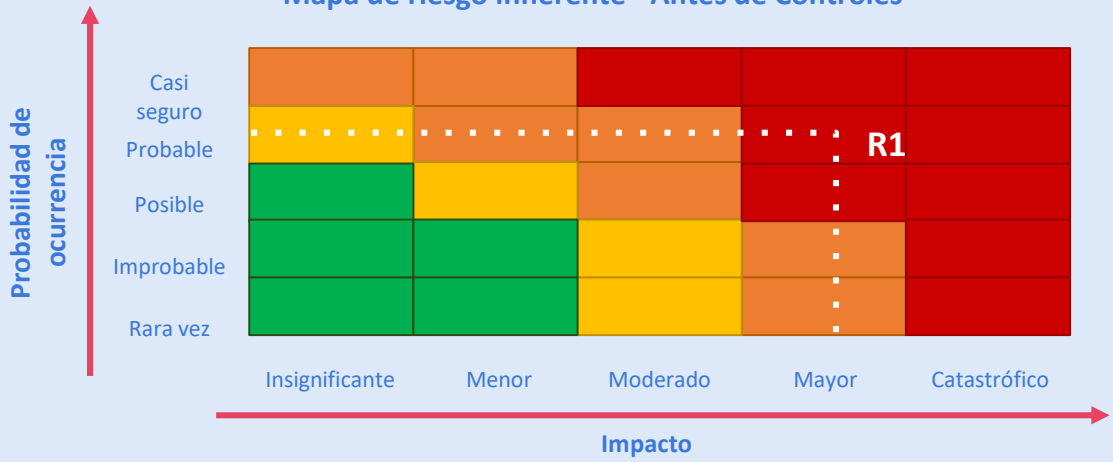
RESULTADOS DEL MAPA DE RIESGO RESIDUAL

Tenemos **el Riesgo 1** - Con una calificación de riesgo inherente de probabilidad e impacto como se muestra en la siguiente gráfica:

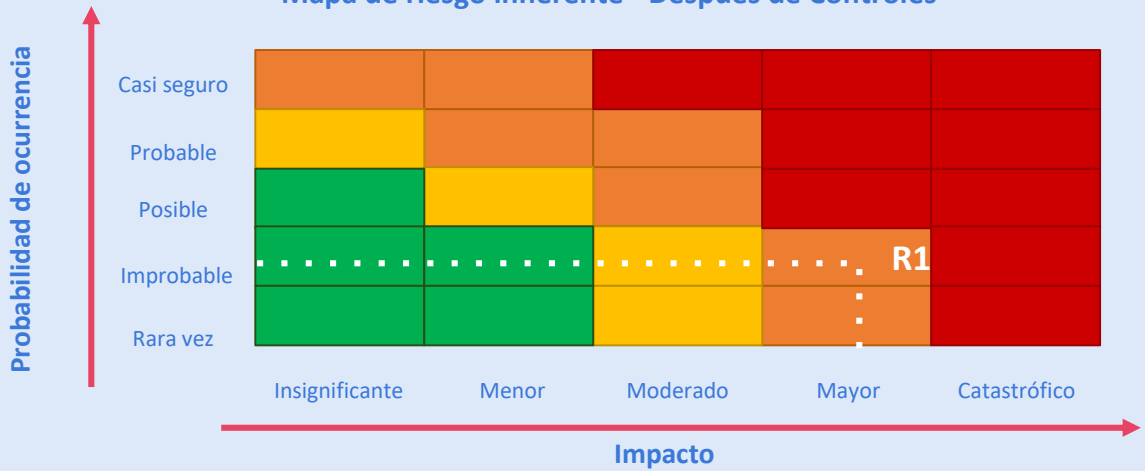
Como podemos observar es probable que el riesgo suceda y tenga un impacto en caso de materializarse para la entidad. Ahora supongamos que existen controles bien diseñados y que siempre se ejecutan, y que estos controles disminuyen de manera directa la probabilidad.

En nuestro ejemplo disminuiría dos cuadrantes de probabilidad, pasa de probable a improbable y un cuadrante de impacto, pasa de mayor a moderado.

Mapa de riesgo inherente - Antes de Controles



Mapa de riesgo inherente - Después de Controles



N.	Riesgo	Activo	Tipo	Amenazas	Vulnerabilidad	Probabilidad	Impacto	Riesgo residual	Opción tratamiento	Actividad de control	Soporte	Responsable	Tiempo	Indicador
2	Perdida 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	**EFICACIA** Índice de cumplimiento actividades= (# de actividades cumplidas/# actividades programadas)*100 **EFECTIVIDAD** Efectividad del plan de manejo de riesgos=(# de modificaciones no autorizadas)
					Contraseñas sin protección				Reducir	A.9.4.3 Sistema de gestion de constraseñas	Procedimientos para la gestion y protección de contraseñas	Oficina TI	Tercer trimestre	
					Ausencia de mecanismos de identificación y autenticación de usuarios				Reducir	A.9.4.2 Procedimiento de ingreso seguro	Procedimiento para inrgeso seguro	Oficina TI	Tercer trimestre	
					Ausencia de bloqueo				Reducir	A.11.2.8 Equipos de usuarios desatentidos	Configuraciones para bloqueo automático de sesión	Oficina TI	Tercer trimestre	

CSIRT Gobierno

CSIRT de Gobierno

CSIRT

Es un **Equipo de Respuesta a Incidentes de Seguridad** en sus siglas en inglés (**Computer Security Incident & Response Team**).

- Integrado por un grupo de personas técnicas especializadas, que implementan y desarrollan acciones tendientes a prevenir y gestionar los incidentes cibernéticos.
- Surge como necesidad de realizar una adecuada gestión y reaccionar ante los incidentes cibernéticos de modo centralizado.
- Especializado para adelantar seguimiento de manera unificada a las principales tipologías de riesgos.

Catálogo de servicios del CSIRT Gobierno

Proactivos

1. Generación de Alertas y Advertencias de seguridad digital
2. Difusión de Información Relacionada con la Seguridad digital
3. Análisis de Vulnerabilidades Web
4. Monitoreo de eventos de seguridad de las Entidades de Gobierno
5. Monitoreo de disponibilidad de portales web de Entidades del Gobierno

Reactivos

6. Gestión de incidentes

Gestión de la seguridad

7. Capacitación y sensibilización en gestión de incidentes de Seguridad digital.

2020

Ministerio de Tecnologías de la Información y las Comunicaciones
Tel:+57(1) 344 34 60
Edif. Murillo Toro Cra. 8a entre calles 12 y 13, Bogotá, Colombia - Código Postal 111711
www.mintic.gov.co

¡Contáctanos!

CSIRT

csirtgob@mintic.gov.co

018000910742 Opción: 4

Gobierno Digital

acompanamiento@mintic.gov.co

(571) 390 79 51 Opción 2
01 8000 910 742 Línea gratuita nacional

El futuro digital es de todos

MinTIC