
 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE DESARROLLO ECONÓMICO</p>	<p>PROCESO: GESTIÓN DE TIC</p> <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>	<p>Página:</p>	<p>Página 1 de 42</p>	 <p>BAJO ESTÁNDAR MIPG SISTEMA INTEGRADO DE GESTIÓN</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------	----------------	------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------

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

**Secretaría Distrital de Desarrollo Económico
Bogotá D.C.
2023**

TABLA DE CONTENIDO

1.	INTRODUCCIÓN.....	4
2.	OBJETIVO DEL DOCUMENTO	5
3.	ALCANCE DEL DOCUMENTO.....	5
4.	RESPONSABILIDADES.....	5
5.	TÉRMINOS GENERALES.....	6
6.	METODOLOGÍA.....	6
7.	DEFINICIONES.....	7
8.	CRITERIOS BÁSICOS.....	12
8.1	IDENTIFICACION DE RIESGOS INHERENTES.....	12
8.2	CLASIFICACION DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.....	12
8.3	CRITERIOS DE VALORACIÓN DEL ACTIVO.....	13
8.4	CRITERIOS DE EVALUACIÓN DEL RIESGO INHERENTE.....	13
8.5	CRITERIOS DE IMPACTO	15
8.6	CRITERIOS DE ACEPTACIÓN DEL RIESGO.....	18
9.	ANÁLISIS DEL RIESGO.....	20
9.1	IDENTIFICACIÓN DEL RIESGO.....	20
9.2	IDENTIFICACIÓN DE LOS ACTIVOS.....	20
9.3	IDENTIFICACIÓN DE LAS AMENAZAS.....	20
9.4	IDENTIFICACION DE LAS VULNERABILIDADES.....	21
9.5	IDENTIFICACION DE LAS CONSECUENCIAS.....	21
9.6	VALORACION DE LOS RIESGOS INHERENTES.....	22
9.7	IDENTIFICACIÓN Y VALORACIÓN DE LOS CONTROLES EXISTENTES.....	23
9.7.1	Identificación de los Controles.....	23
9.7.2	Tipo de Controles.....	24
9.7.3	Evaluación de los controles.....	24
9.7.4	Estimación del Riesgo Residual.....	29
9.7.5	Tratamiento del riesgo	30

9.8	PRIORIZACIÓN DE RIESGOS A NIVEL DE PROCESOS.....	30
9.9	SEGUIMIENTO, MONITOREO Y REVISIÓN.....	31
9.9.1	Seguimiento y Monitoreo.	31
9.9.2	Revisión.....	31
9.10	COMUNICACIÓN Y CONSULTA.....	31
9.10.1	Publicación en la Intranet y página Web institucional.....	32
9.10.2	Procesos de socialización.....	32
10.	BUENAS PRÁCTICAS PARA LA MITIGACIÓN DE RIESGOS.	33
12.	CRONOGRAMA.....	1
13.	ANEXOS.....	1

1. INTRODUCCIÓN.

El Decreto 1008 de 2018, establece los lineamientos generales de la Política de Gobierno Digital que deberán adoptar las entidades pertenecientes a la administración pública, encaminados hacia la transformación digital y el mejoramiento de las capacidades TIC.

La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, se lleva a cabo a partir de una serie de guías en cada una de las fases, que pone a disposición el Ministerio de las Tecnologías y las Comunicaciones – MINTIC. Su adopción debe ser acorde a las necesidades y objetivos, requisitos de seguridad, procesos misionales, el tamaño y estructura de SDDE, de esto resultan una serie de instrumentos como planes, procedimientos, manuales, formatos y demás que, en conjunto deben ser gestionados desde el contexto de un Sistema de Gestión de Seguridad de la Información - SGSI conducente a la preservación de la confidencialidad, integridad y disponibilidad de la información.

De acuerdo con lo anterior, la relación e interacción entre la gestión de seguridad de la información con el Modelo Nacional de Gestión de Riesgos de Seguridad Digital –MGRSD– se visualiza y se describe de la siguiente manera:

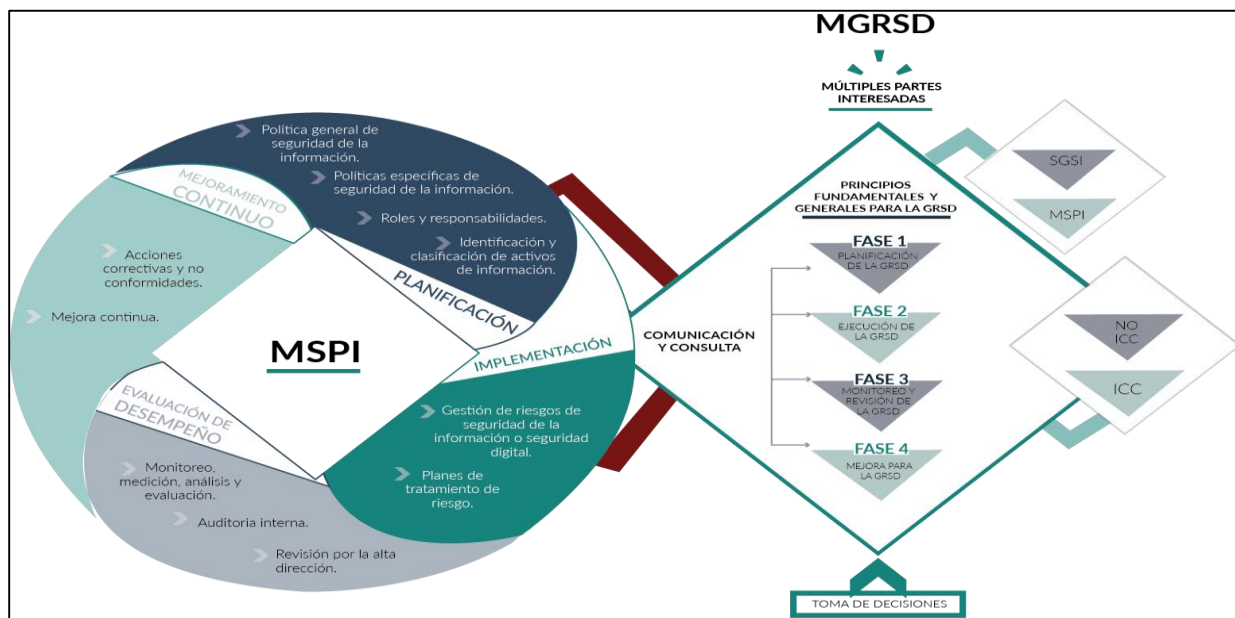




Figura 1. Interacción entre el MSPI y el MGRSD. Fuente: MinTIC.

La estructuración y la puesta en ejecución de esta plan brinda importantes beneficios estratégicos y tácticos para la entidad:

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE DESARROLLO ECONÓMICO</p>	<p>PROCESO: GESTIÓN DE TIC</p> <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>	<p>Página:</p>	<p>Página 5 de 42</p>	 <p>BAJO ESTÁNDAR MIPG SISTEMA INTEGRADO DE GESTIÓN</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------	----------------	------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------

- Apoyar la transformación digital de la entidad por intermedio de un portafolio de proyectos que estén alineados con los objetivos y metas de la alta gerencia, de tal manera que apalanquen y ayuden a la entidad alcanzar las metas de su estrategia en el corto, mediano y largo plazo.
- Fortalecer las capacidades de la Subdirección de Informática y Sistemas para apoyar la estrategia y modelo operativo de la entidad
- Adquirir e implementar buenas prácticas de gestión de TI.
- Adoptar el Modelo de Seguridad y Privacidad de la Información, para resguardar todo tipo de Información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos, puede significar un respaldo para el normal desarrollo de las actividades de la entidad.

2. OBJETIVO DEL DOCUMENTO



Establecer la metodología para la Gestión de Riesgos de Seguridad y Privacidad de la Información en la Secretaría Distrital de Desarrollo Económico, para prevenir o reducir efectos indeseados, lograr la mejora continua, valorar y tratar los riesgos, sus consecuencias potenciales y la probabilidad de ocurrencia.

3. ALCANCE DEL DOCUMENTO.

Aplica para la identificación, clasificación, análisis, evaluación, control y valoración de los riesgos de Seguridad y Privacidad de la Información en la Secretaría Distrital de Desarrollo Económico, este plan complementa el instructivo "*Matriz de Riesgos Seguridad de la Información*" y además está complementado con el *Procedimiento de Gestión de Incidentes de Seguridad de la Información*.

4. RESPONSABILIDADES.

La Oficina Asesora de Planeación como parte de la segunda línea de defensa y siendo la dependencia responsable de liderar el desarrollo e implementación del Sistema de Gestión se encargará de revisar y adecuar la metodología de administración de riesgos propuesta por el

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE DESARROLLO ECONÓMICO</p>	<p>PROCESO: GESTIÓN DE TIC</p> <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>	<p>Página:</p>	<p>Página 6 de 42</p>	 <p>BAJO ENTENDER MIPG SISTEMA INTEGRADO DE GESTIÓN</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------	----------------	------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------

DAFP a las necesidades de la Secretaría Distrital de Desarrollo Económico, también brindará la asesoría y las herramientas a los procesos para su correcta elaboración.

El equipo de la Subdirección de Informática y Sistemas será el encargado de brindar acompañamiento en el desarrollo e implementación del componente de Administración del Riesgo de Seguridad y Privacidad de la Información, este deberá recoger iniciativas, responsabilidades y armonizar los diferentes ejercicios para la implementación de un proceso más efectivo.

El equipo de seguimiento y evaluación está conformado por la Oficina de Control Interno, quienes velarán por la adecuada elaboración e implementación del mapa de riesgos de cada proceso, promoviendo su apropiación, entendimiento y evaluación del mismo.



Es importante revisar el documento PE-M1 POLÍTICA DE ADMINISTRACIÓN DE RIESGOS DE LA SECRETARÍA DISTRITAL DE DESARROLLO ECONÓMICO, que contiene las responsabilidades generales de las tres líneas de defensa en la Gestión de Riesgos Institucional.

5. TÉRMINOS GENERALES.

1. Cumplimiento de la Política de Administración de Riesgos de Seguridad y Privacidad de la Información de la Secretaría Distrital de Desarrollo Económico.
2. Utilizar la metodología propuesta por el Departamento Administrativo de la Función Pública - Guía para la administración del riesgo y el diseño de controles en entidades públicas v5.
3. Implementación de mecanismos para la Administración de Riesgos de Seguridad de la Información en la Secretaría Distrital de Desarrollo Económico.
4. Para reportar materialización de un riesgo de seguridad de la información, utilizar el Procedimiento para Gestión de Incidentes de Seguridad de la Información.
5. Cumplimiento de la Política de Administración del Riesgo de la SDDE.

6. METODOLOGÍA.

La metodología para la administración de los riesgos de seguridad de la información o seguridad digital, es la establecida por la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - Versión 5 - Diciembre de 2020 del Departamento Administrativo de la Función Pública.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE DESARROLLO ECONÓMICO</p>	<p>PROCESO: GESTIÓN DE TIC</p> <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>	<p>Página:</p>	<p>Página 7 de 42</p>	 <p>BAJO ESTÁNDAR MIPG SISTEMA INTEGRADO DE GESTIÓN</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------	----------------	------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------

7. DEFINICIONES.

Activo: Cualquier cosa que pueda ser de valor para la entidad. Algunos tipos de activos incluyen, pero no se limitan a:

- Información.
- Software.
- Recursos físicos.
- Servicios.
- Personas y sus cualificaciones, habilidades y experiencias.
- Elementos intangibles como la reputación y la imagen.

Activo de Información: Conocimiento o datos que son de valor para la entidad. Ver modelo estándar de control interno para el Estado Colombiano, MECI 1000:2005, Numeral 2.2 Componente Información

Amenaza: Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema o la entidad.

Causas: (Amenaza o Vulnerabilidad): Aquello que se considera como fundamento u origen de algo.



CCOC: Comando Conjunto Cibernético, Unidad Militar Conjunta (Ejército, Armada y Fuerza Aérea), que tiene como función principal prevenir, detectar, orientar, contener, decidir, responder y recuperar ante amenazas cibernéticas que afecten la sociedad, la soberanía nacional, independencia, integridad territorial, el orden constitucional y los intereses nacionales, todo esto, soportado en un marco jurídico y/o la Constitución Nacional.

Ciberataque: Es cualquier tipo de maniobra ofensiva hecha por individuos u organizaciones que ataquen a sistemas de información como lo son infraestructuras, redes computacionales, o bases de datos que están albergadas en servidores remotos. Estas maniobras son realizadas por medio de actos maliciosos usualmente originados de fuentes anónimas y direcciones que no pueden ser rastreadas.

Ciberincidente: Cualquier acto malicioso o evento sospechoso que: comprometa, o intente comprometer la Seguridad del perímetro electrónico, la Seguridad del primero físico o un activo crítico.

Ciberseguridad: Es el proceso de proteger activos de información por medio del tratamiento de amenazas para información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.

Código malicioso: Conjunto de instrucciones o códigos informáticos que se inserta en los programas de computador, tiene la capacidad de auto replicarse y usualmente porta una carga

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE DESARROLLO ECONÓMICO</p>	<p>PROCESO: GESTIÓN DE TIC</p> <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>	<p>Página:</p>	<p>Página 8 de 42</p>	 <p>BAJO ENTENDIMIENTO MIPG SISTEMA INTEGRADO DE GESTIÓN</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------	----------------	------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------

útil que afecta el funcionamiento del computador, destruye datos, altera y pone en riesgo la información.

COLCERT: Por las siglas en inglés de Computer Emergency Response Team, es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, y tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual estará enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de Ciberseguridad que atenten o comprometan la seguridad y defensa nacional.

Confidencialidad: Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados

Contención de un incidente: Son todas aquellas actividades encaminadas a reducir el impacto inmediato de un incidente de seguridad.

Consecuencia: resultado, efecto o impacto de un riesgo o un evento.

Control correctivo: Es el control que se realiza para eliminar la (s) causa (s) de una no conformidad detectada u otra situación indeseable.

Control preventivo: Es el control que se realiza para eliminar la (s) causa (s) de una no conformidad potencial u otra situación potencialmente indeseable.



CSIRT: Por las siglas en inglés de Computer Security Incident Response Team, es el equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL, creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones

Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales, tales como nombre, apellido, cedula, edad, color de ojos, estatura, fotografía o video de la persona, entre otros. Estos datos se pueden clasificar como dato público, sensible y semiprivado.

Dato Público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al nombre, estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Dato Semiprivado: Datos que son de carácter privado, este tipo de datos sólo le interesan al titular y a un grupo determinado de personas. (Ej. Datos financieros, crediticios).

Datos Sensibles: Son aquellos 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, así como los datos

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE DESARROLLO ECONÓMICO</p>	<p>PROCESO: GESTIÓN DE TIC</p> <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>	<p>Página:</p>	<p>Página 9 de 42</p>	 <p>BAJO ESTÁNDAR MIPG SISTEMA INTEGRADO DE GESTIÓN</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------	----------------	------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------

relativos a la salud, a la vida sexual, videos, fotografías, datos biométricos (huella dactilar, iris del ojo, pulsaciones cardiacas entre otros).

Denegación del servicio: Conjunto de actividades desarrolladas por atacantes informáticos para degradar o interrumpir el normal funcionamiento de un sistema o servicio informático.

Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de un individuo, entidad o proceso autorizado.

Evento de seguridad de la información: Ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha en el cumplimiento de la política de seguridad de la información, falla de un control de seguridad de la información o una condición no identificada con anterioridad que puede ser relevante para la seguridad de la información.

Evaluación del Riesgo: Proceso utilizado para determinar las prioridades de la administración del riesgo, comparando el nivel de un determinado riesgo con respecto a un estándar determinado, es decir, calificar el riesgo de acuerdo a su impacto con respecto a la probabilidad.

Frecuencia: es el número de veces que se repite un evento o un hecho en el tiempo.

Identificación del Riesgo: Proceso para determinar las causas internas y/o externas (debido a...), evento (lo que puede suceder...riesgo) y la consecuencia (lo que podría ocasionar que...).

Impacto: Efecto positivo o negativo producido por un acontecimiento, evento o riesgo.

Incidente de seguridad informática: Una violación o inminente amenaza de violación de las políticas de seguridad informática, políticas de uso aceptable o prácticas del estándar seguridad. En el contexto de este procedimiento, una inminente amenaza es definida como una situación en la cual la organización tiene evidencias para creer que un incidente de seguridad va a ocurrir.



Incidente de seguridad de la información: Es un acceso, intento de acceso, uso, divulgación, modificación o destrucción de información no autorizada; además de un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información que atente contra la misionalidad de la entidad.

Incidente digital: Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos. (CONPES 3854, pág. 87)

Infraestructura Crítica (IC): Son las infraestructuras estratégicas cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. Adaptación Ley 8/2011-Gobierno de España.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Monitorear: Comprobar, supervisar, observar o registrar la forma que se lleva a cabo una actividad con el fin de identificar posibles cambios.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE DESARROLLO ECONÓMICO</p>	<p>PROCESO: GESTIÓN DE TIC</p> <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>	<p>Página:</p>	<p>Página 10 de 42</p>	 <p>BAJO ENTENDIMIENTOS MIPG SISTEMA INTEGRADO DE GESTIÓN</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------	----------------	-------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------

NITS: Es el proceso de proteger información a través de la prevención, detección y respuesta hacia ataques.

Oficial de Seguridad de la Información: Designación dada a una persona para cumplir con los temas relacionados frente a la seguridad de la información.

Phishing: Es un método que los ciberdelincuentes utilizan para engañar y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito, de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos dirigiéndole a un sitio web falso.

Probabilidad: Cualidad de probable, que puede suceder.

Plan de continuidad de la operación (BCP. Business Continuity Plan): Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.

Ransomware: Piezas de código desarrolladas por atacantes informáticos para secuestrar información de los equipos infectados a través de técnicas criptográficas y posteriormente solicitar el pago de rescate para la recuperación de información.

Riesgo Residual: Riesgo remanente después de la implementación del tratamiento del riesgo.

RNBD: Registro Nacional de Bases de Datos.

Seguridad Digital: Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante:

la gestión del riesgo de seguridad digital;

la implementación efectiva de medidas de ciberseguridad;



y el uso efectivo de las capacidades de ciberdefensa que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

Servicio Esencial: El servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la educación, la seguridad, el bienestar social y económico de una comunidad, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas. Adaptación Ley 8/2011-Gobierno de España.

Suplantación de identidad: Todas aquellas actividades realizadas por la que una persona se hace pasar por otra para llevar a cabo actividades de carácter ilegal.

Valoración del Riesgo: Es el producto de confrontar los resultados de la evaluación del riesgo con los controles identificados en el elemento de control.

Tipos de Riesgos:

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE DESARROLLO ECONÓMICO</p>	<p>PROCESO: GESTIÓN DE TIC</p> <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>	<p>Página:</p>	<p>Página 11 de 42</p>	 <p>BAJO ENTENDER MIPG SISTEMA INTEGRADO DE GESTIÓN</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------	----------------	-------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------

- **Riesgo Estratégico:** Se asocia con la forma en que se administra la entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
- **Riesgos Operativos:** Comprende los riesgos relacionados tanto con la parte operativa como con la técnica de la entidad, incluye riesgos provenientes de deficiencias en los sistemas de información, en la definición de los procesos y la ejecución de los procedimientos en la estructura de la entidad, la desarticulación entre dependencias, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.
- **Riesgos Financieros:** Se relacionan con el manejo de los recursos de la entidad, que incluye la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes de cada entidad. De la eficiencia y transparencia en el manejo de los recursos, así como de su interacción con las demás áreas, dependerá en gran parte el éxito o fracaso de toda entidad.
- **Riesgos de Cumplimiento:** Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
- **Riesgos de Conocimiento:** son aquellos que se relacionan con el daño generado por la pérdida de conocimiento e información vital para el desarrollo de las actividades de la entidad y organismo distrital. En esta clasificación se encuentran los riesgos en los activos y la seguridad de la información.
- **Riesgos Normativos:** son aquellos que se relacionan tanto con los daños generados por la violación de una prescripción u obligación legal, incumplimientos a políticas internas, como con la volatilidad normativa. Dentro de este tipo se pueden agrupar los incumplimientos a obligaciones tributarias, a tiempos en la presentación de estados financieros a solicitudes de información y demás incumplimientos legales aplicables.
- **Riesgos de Tecnología:** Se asocian con la capacidad de la entidad para que la tecnología disponible satisfaga sus necesidades actuales, futuras y soporte el cumplimiento de la misión.

Vulnerabilidad: Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (CONPES 3854, pág. 87)

8. CRITERIOS BÁSICOS.

8.1 IDENTIFICACION DE RIESGOS INHERENTES.

Se pueden 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.

La variación son las amenazas y vulnerabilidades que pueden causar que dichos riesgos se materialicen.

8.2 CLASIFICACION DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

Se puede clasificar el riesgo de seguridad de la información según la siguiente tabla:

Clasificación	Descripción
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

8.3 CRITERIOS DE VALORACIÓN DEL ACTIVO.

El valor del activo se calcula como la suma de los valores de confidencialidad, integridad y disponibilidad usando las siguientes tablas:

Tabla1. Valoración de la Confidencialidad del activo

Valor del activo	Descripción
1	Activos con información considerada como de DOMINIO PÚBLICO.
2	Activos con información clasificada como de APOYO.
3	Activos con información clasificada como de ACCESO CONTROLADO.
4	Activos con información clasificada como de CARÁCTER RESERVADO.

Tabla 2. Valoración de la Integridad del activo.

Valor del activo	Descripción
1	Activos con información que aún no es oficial y aún están en proceso de elaboración.
5	Activos con información oficial que no se pueden alterar bajo ninguna condición.

Tabla 3. Valoración de la Disponibilidad del activo.

Valor del activo	Descripción
1	El uso del activo puede esperar un tiempo que puede modificar el usuario
2	El uso del activo puede esperar un tiempo que define el usuario y no se puede modificar ese tiempo de espera.
3	El activo debe estar siempre disponible en el momento en que se necesite.

Resultado valor del activo = Suma de Confidencialidad + Integridad + Disponibilidad.

8.4 CRITERIOS DE EVALUACIÓN DEL RIESGO INHERENTE.

Como referente, a continuación, se muestra una tabla 4 de actividades típicas relacionadas con la gestión de una entidad pública, bajo las cuales se definen las escalas de probabilidad:

Tabla 4. Actividades relacionadas con la gestión en entidades públicas.

Actividad	Frecuencia	Probabilidad frente al riesgo
Planeación estratégica	1 vez al año	Baja
Actividades de talento humano, jurídica, administrativa	Mensual	Moderada
Contabilidad, cartera	Semanal	Mayor
Tecnología* (incluye disponibilidad de aplicativos), tesorería *Nota: En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez. Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia, su frecuencia se calcularía 60 días * 24 horas= 1440 horas.	Diaria	Alta

Determinar la probabilidad del riesgo, se entiende como la posibilidad de ocurrencia del riesgo, para efectos de este análisis, la **exposición al riesgo** estará asociada al proceso o actividad que se esté analizando, es decir, al **número de veces que se pasa por el punto de riesgo en el periodo de 1 año**, en la siguiente tablase establecen los criterios para definir el nivel de probabilidad:

Tabla 5. Criterios para definir el nivel de probabilidad.

Puntaje	Frecuencia de la actividad	Descripción	Probabilidad
1	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	La eventualidad de ocurrencia es muy baja o casi nula	Muy baja - 20%
2	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	El evento puede ocurrir solo en circunstancias excepcionales.	Baja - 40%
3	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	El evento podrá ocurrir en algún momento.	Moderada - 60%
4	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	Es viable que el evento ocurra en la mayoría de las circunstancias.	Mayor - 80%
5	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	Se espera que el evento ocurra en la mayoría de las circunstancias	Alta - 100%

8.5 CRITERIOS DE IMPACTO

Para medir el impacto de los riesgos de seguridad de la información en la Secretaría Distrital de Desarrollo Económico, se puede evaluar con una de las siguientes tres maneras:

Opción 1. Valorar el impacto teniendo en cuenta principalmente variables de impactos económicos y reputacionales, como en la siguiente tabla:

Valor	Impacto	Afectación Económica	Descripción reputacional
1	Leve - 20%	Afectación menor a 10 SMLV	El riesgo afecta la imagen de algún área de la organización.

2	Menor - 40%	Entre 10 y 50 SMLV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
3	Moderado - 60%	Entre 50 y 100 SMLV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
4	Mayor - 80%	Entre 100 y 500 SMLV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.
5	Catastrófico - 100%	Mayor a 500 SMLV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Opción 2. Valorar el impacto teniendo en cuenta el valor del activo, como se muestra en la siguiente tabla:

Valor	Concepto	Descripción
1	Muy bajo	Cuando el valor del activo afectado se encuentra entre 3 y 4
2	Bajo	Cuando el valor del activo afectado se encuentra entre 5 y 6
3	Moderado	Cuando el valor del activo afectado se encuentra entre 7 y 8
4	Mayor	Cuando el valor del activo afectado se encuentra entre 9 y 10
5	Catastrófico	Cuando el valor del activo afectado se encuentra entre 11 y 12

Opción 3. Valorar el impacto teniendo en cuenta los riesgos inherentes de la seguridad de la información:

NIVELES PARA CALIFICAR EL IMPACTO	Muy bajo	Bajo	Moderado	Mayor	Catastrófico
VALOR	1	2	3	4	5
Integridad	La pérdida de exactitud y completitud afecta a la persona que ejecuta la actividad y no conlleva afectación significativa.	La pérdida de exactitud y completitud afecta al personal de todo el proceso o proyecto y no conlleva afectación significativa.	La pérdida de exactitud y completitud afecta hasta tres (3) proyectos de la entidad y conlleva a la afectación significativa de índole legal o económica, retrasa funciones o genera pérdida de imagen de funcionarios de la institución.	La pérdida de exactitud y completitud afecta una línea de investigación con la que interactúa la SDDE y conlleva a la afectación significativa de índole legal o económica, retrasa funciones o genera pérdida de imagen severa de la institución.	La pérdida de exactitud y completitud afecta más de una entidad con la que interactúa la SDDE y conlleva afectación, así como a un impacto negativo de índole legal o económica, retrasa funciones o genera pérdida de imagen severa de la institución, además no puede repararse.
Disponibilidad	Afecta solo a la persona que ejecuta la actividad o afecta la disponibilidad por hasta 1 hora de la jornada laboral.	Afecta un grupo de trabajo o afecta la disponibilidad por más de una hora y hasta una semana.	Afecta hasta tres (3) grupos de trabajo o afecta la disponibilidad más de una (1) semana.	Afecta una entidad con la que interactúa la SDDE o afecta la disponibilidad más de una (1) semana, hasta dos (2) semanas.	Afecta más de una entidad con la que interactúa la SDDE o afecta la disponibilidad más de dos (2) semanas.

Confidencialidad	Afecta la información de uso interno de la persona que ejecuta el proceso.	Afecta la información pública del área que lidera el proceso.	Afecta la información pública de hasta tres (3) grupos de trabajo.	Afecta la información reservada y clasificada de un grupo o línea de investigación de la SDDE.	Afecta información clasificada y reservada de entidades o personas con las que interactúa la SDDE.
-------------------------	----------------------------------------------------------------------------	---------------------------------------------------------------	--------------------------------------------------------------------	------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------

8.6 CRITERIOS DE ACEPTACIÓN DEL RIESGO.

De acuerdo a la valoración de los riesgos, teniendo en cuenta la ubicación final en la Matriz de calificación, evaluación y respuesta a los riesgos, se establecen las medidas de respuesta, a través de la identificación de las opciones de manejo para el tratamiento de los riesgos.

Las opciones de manejo a tomar son las siguientes y se pueden considerar cada una de manera independiente o en conjunto:



- Evitar el Riesgo: Se toman medidas encaminadas a evitar la materialización del riesgo.
- Reducir el Riesgo (Mitigar): Incluye medidas orientadas a disminuir tanto la probabilidad (medidas de prevención) como el impacto (medidas de detección).
- Transferir el Riesgo: Reducen los efectos de los riesgos, a través del traspaso de las pérdidas a otras organizaciones.
- Asumir el Riesgo: En este caso, no se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.

El tratamiento del riesgo implica la preferencia para la modificación de los riesgos y la aplicación del mismo, dependiendo la zona en la que estos se encuentren ubicados se define una opción de tratamiento de acuerdo con lo establecido en la siguiente tabla:

Opción de Aceptación	Evaluación Residual del Riesgo	
✓ Asumir el Riesgo.	BAJA	
✓ Reducir el Riesgo.	MEDIA	
✓ Reducir el Riesgo (Mitigar). ✓ Transferir el Riesgo.	ALTA	

✓ Evitar el Riesgo.		
✓ Reducir el Riesgo (Mitigar). ✓ Transferir el Riesgo. ✓ Evitar el Riesgo.	EXTREMA	

Una vez empleado el tratamiento, se otorgan controles o se modifican, es importante incluir las opciones de análisis, evaluación, desarrollo e implementación que se deben tener en cuenta para el tratamiento del riesgo.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE DESARROLLO ECONÓMICO</p>	<p>PROCESO: GESTIÓN DE TIC</p> <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>	<p>Página:</p>	<p>Página 20 de 42</p>	 <p>BAJO ESTÁNDAR MIPG SISTEMA INTEGRADO DE GESTIÓN</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------	----------------	-------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------

9. ANÁLISIS DEL RIESGO.

9.1 IDENTIFICACIÓN DEL RIESGO.

La evaluación de riesgos de seguridad y privacidad de la información debe iniciar con la identificación y selección de los procesos a evaluar, es necesario contar con la mayor cantidad posible de información de los procesos a evaluar como: descripción del proceso, procedimientos que lo componen, instructivos y cualquier documentación que ayude a entender el alcance y características del proceso.

- Los procesos seleccionados para evaluación se documentan en el campo respectivo de la “Matriz Mapa de Riesgos”.
- Colocar el objetivo del Proceso en el campo indicado de la “Matriz Mapa de Riesgos”.

9.2 IDENTIFICACIÓN DE LOS ACTIVOS.

Se considera como activo cualquier cosa que tiene valor para la entidad, se debe tener en cuenta que los procesos se apoyan en sistemas de información que además de software y hardware también están compuestos por documentos (registros, instrucciones de trabajo, procedimientos), personas (responsables de actividades en el proceso o administradores de componentes de tecnología) y directrices que guían el proceso en sí mismo.



Del proceso de identificación de activos resulta un inventario de activos de información con un responsable identificado del activo.

Nota: Los activos de información se pueden usar para identificar los riesgos de seguridad de la información.

9.3 IDENTIFICACIÓN DE LAS AMENAZAS.

Se considera como amenaza (causa) cualquier agente externo al activo que puede aprovechar una vulnerabilidad del mismo para causar daño y que afectará la seguridad de la información. La identificación de amenazas se realiza mediante la evaluación de fuentes de información como:

- Experiencia de los dueños de los activos que se están evaluando.
- Experiencia de especialistas externos.
- Bases de datos públicas sobre amenazas de seguridad de la información.
- Reportes de listas de interés en seguridad de la información.
- Recomendaciones de las normas ISO 27001:2013.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE DESARROLLO ECONÓMICO</p>	<p>PROCESO: GESTIÓN DE TIC</p> <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>	<p>Página:</p>	<p>Página 21 de 42</p>	 <p>BAJO ENTENDAR MIPG SISTEMA INTEGRADO DE GESTIÓN</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------	----------------	-------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------

- Experiencia de los administradores del SGSI mediante el tratamiento de incidentes de seguridad.

Nota: Las amenazas se consideran como causas externas.

En el Anexo 1 de este documento encuentra una lista de posibles amenazas que pueden afectar a los activos de información de la Secretaría Distrital de Desarrollo Económico.

9.4 IDENTIFICACION DE LAS VULNERABILIDADES.

Se considera como vulnerabilidad una debilidad en un activo o un control que puede ser explotada (aprovechada) por una amenaza. La identificación de vulnerabilidades sobre los activos se realiza con pruebas técnicas o auditorias (pruebas con herramientas de software, pruebas de ingeniería social o herramientas de auditoría como la inspección y la observación) de cumplimiento de la fortaleza del activo o el control. Las fuentes de información en donde se pueden detectar vulnerabilidades que pueden afectar a los sistemas de información incluyen:

- Documentación de los procesos y procedimientos.
- Rutinas de administración de activos.
- Personal responsable de la administración de los activos.
- Información de la configuración de equipos y sistemas.
- Evaluación del entorno físico y lógico del activo.

Para la evaluación de la existencia de vulnerabilidades se debe considerar la existencia o no de controles en el activo y la calidad de los controles implementados.

La existencia de una vulnerabilidad no implica automáticamente la existencia de un riesgo, es necesario que exista una amenaza que esté en capacidad de aprovechar la vulnerabilidad. Las vulnerabilidades también se deben considerar como causas de riesgos. Las vulnerabilidades se registran como amenazas internas

En el Anexo 2 de este documento encuentra una lista de posibles vulnerabilidades que pueden afectar a los activos de información de la Secretaría Distrital de Desarrollo Económico.

9.5 IDENTIFICACION DE LAS CONSECUENCIAS.

Las consecuencias son los hechos que se derivan del evento identificado. A nivel de los riesgos de la seguridad de la información, las consecuencias se describen en términos de los tres componentes de la seguridad de la información:

- Pérdida de Disponibilidad.

- Pérdida de Integridad.
- Pérdida de Confidencialidad.

9.6 VALORACION DE LOS RIESGOS INHERENTES.

Consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE), para la realización de esta valoración debe tenerse en cuenta:

1. Calcular el impacto.

El cálculo del impacto se realiza usando la tabla registrada en los Criterios Básicos de este plan.

2. Valorar la posibilidad de ocurrencia (probabilidad).

El cálculo de la probabilidad de ocurrencia se realiza usando la tabla registrada en los Criterios Básicos de este plan.

Nota: Todos valores deben ser registrados en la Matriz de Riesgos Seguridad de la Información.

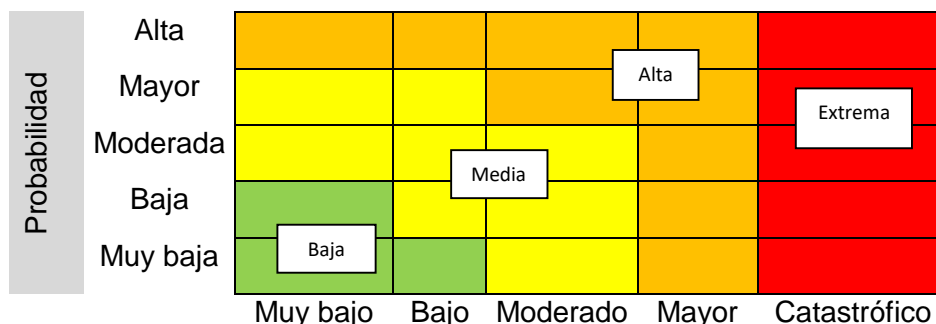
3. Estimar el nivel de riesgo inicial – inherente.

Se logra a través de la determinación de la probabilidad y el impacto que puede causar la materialización del riesgo, teniendo en cuenta la siguiente tabla:

		Impacto				
Probabilidad	Muy Alta	5	10	15	20	25
	Alta	4	8	12	16	20
	Medio	3	6	9	12	15
	Baja	2	4	6	8	10
	Muy baja	1	2	3	4	5
		Muy bajo	Bajo	Moderado	Mayor	Catastrófico

Resultado de la determinación del riesgo inherente, se obtiene la ubicación de riesgo en el mapa de calor:

Impacto



9.7 IDENTIFICACIÓN Y VALORACIÓN DE LOS CONTROLES EXISTENTES.

9.7.1 Identificación de los Controles.

Se considera como control un proceso, política, dispositivo, practica u otra acción existente que actúa para minimizar el riesgo negativo o potenciar oportunidades positivas. La identificación de controles existentes de seguridad de la información considera los controles recomendados por la norma técnica Colombiana NTC ISO /IEC 27001:2013.

Para realizar la valoración de controles existente se pueden seguir las siguientes actividades:

- Revisar la documentación existente que contiene información sobre los controles implementados a nivel de los procesos de la entidad
- Indagar con los responsables de los activos la existencia real y correcto funcionamiento de los controles descritos en la documentación.
- Realizar revisiones detalladas de la existencia de controles de seguridad de la información usando listas de verificación de controles de seguridad de la información como ISO27001:2013 y buenas prácticas de auditoría.
- Revisar los resultados de las evaluaciones de seguridad de la información realizadas.

La norma NTC ISO/IEC 27001:2013 contiene una lista de 114 controles recomendados para la seguridad de la información.

9.7.2 Tipo de Controles.

Tipo	Descripción
Controles Preventivos	Va a las causas del riesgo. Atacan la probabilidad de ocurrencia del riesgo.
Controles Detectivos	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Atacan la probabilidad de ocurrencia del riesgo.
Controles Correctivos	Atacan el impacto frente a la materialización del riesgo.

9.7.3 Evaluación de los controles.

A continuación, se muestra la tabla de valoración de controles, la cual está basada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, Departamento de la función Pública - DAFP.

IMPORTANTE

- * Para cada causa debe existir un control.
- * Las causas se deben trabajar de manera separada (no se deben combinar en una misma columna o renglón).
- * Un control puede ser tan eficiente que me ayude a mitigar varias causas, en estos casos se repite el control, asociado de manera independiente a la causa específica.

El líder del proceso debe determinar por cada vulnerabilidad cuál es el control existente y valorar el diseño de acuerdo a los siguientes criterios cuantitativos y cualitativos:

Criterios Cuantitativos

Características		Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	25%
		Detectivo	15%
		Correctivo	10%
Implementación		Automático	25%
		Manual	15%

El total de valoración del control es la suma de la selección del atributo de implementación y el de eficiencia. La herramienta de manera automáticamente realizará la sumatoria. Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

Criterios informativos:

Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad. (Tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5). Deben tenerse en cuenta los siguientes lineamientos para su registro en la matriz correspondiente:

Criterio de evaluación	Aspecto por evaluar	Definición	Opciones de respuesta	Peso
1.Responsable	¿Existe un responsable asignado en la ejecución del control?	Persona asignada para ejecutar el control.	Asignado	-
			No asignado	-
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Debe tener la autoridad, competencias y conocimientos para ejecutar el control, sus responsabilidades deben ser adecuadamente redistribuidas entre diferentes individuos, para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas.	Adecuado	-
			Inadecuado	0
2.Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la		Oportuna	-

Criterio de evaluación	Aspecto por evaluar	Definición	Opciones de respuesta	Peso
	mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?		Inoportuna	-
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir, detectar o corregir las causas que pueden dar origen al riesgo?	Debe indicar para qué se realiza y que conlleve a prevenir las causas que generan el riesgo o detectar la materialización del riesgo, con el objetivo de llevar a cabo los ajustes y correctivos en el diseño del control o en su ejecución, debemos preguntarnos si es una actividad o un control.	Preventivo	-
			Detectivo	-
			Correctivo	-
			No es un control	-
4. Cómo se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?		Confiable	-
			No confiable	-

Criterio de evaluación	Aspecto por evaluar	Definición	Opciones de respuesta	Peso
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	El responsable de ejecutar el control debe realizar actividades de seguimiento a las observaciones o desviaciones, si la actividad continúa a pesar de indicar esas observaciones o desviaciones, el control tendría problemas en su diseño.	Se investigan y resuelven oportunamente	-
			No se investigan y resuelven oportunamente.	-
6. Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	El control debe dejar evidencia de su ejecución. Esta evidencia ayuda a que se pueda revisar la misma información por parte de un tercero y llegue a la misma conclusión de quien ejecutó el control y se pueda evaluar que el control realmente fue ejecutado de acuerdo con los parámetros establecidos.	Completa	-
			Incompleta	-
			No existe	-

Nota:

En el instrumento Matriz de Riesgos Seguridad de la Información, se permite el registro de los controles existentes.

Para diligenciar los "controles existentes", la información debe ser diligenciada, teniendo en cuenta las siguientes observaciones:

- a) Los riesgos se deben diligenciar en el mismo orden que aparecen en la hoja "Mapa de riesgo" existan o no controles para estos.
- b) Diligenciar el control existente.
- c) Si existen controles indicar si es correctivo, preventivo o los dos.
- d) Si se diligencian controles, es necesario llenar todos los campos de la columna valoración, es decir, si se aplica el control, si es efectivo, si está documentado y si este disminuye el impacto, la probabilidad o ambos; en caso contrario dejar la columna en blanco.

9.7.4 Estimación del Riesgo Residual.

Una vez valorados los controles y aplicados a la Zona de Riesgo Inherente, se determina los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor.

Es IMPORTANTE tener en cuenta la valoración asignada a los atributos de los controles:

*Solidez del control.

Probabilidad.

Es la multiplicación de la Probabilidad inherente (%) y la calificación del control (%); posteriormente se resta a la Probabilidad inherente el resultado de la multiplicación anterior.

1. Probabilidad = Probabilidad inherente (%) * Calificación (%)
2. Probabilidad Residual = Probabilidad inherente (%) - Resultado P (%)

Impacto.

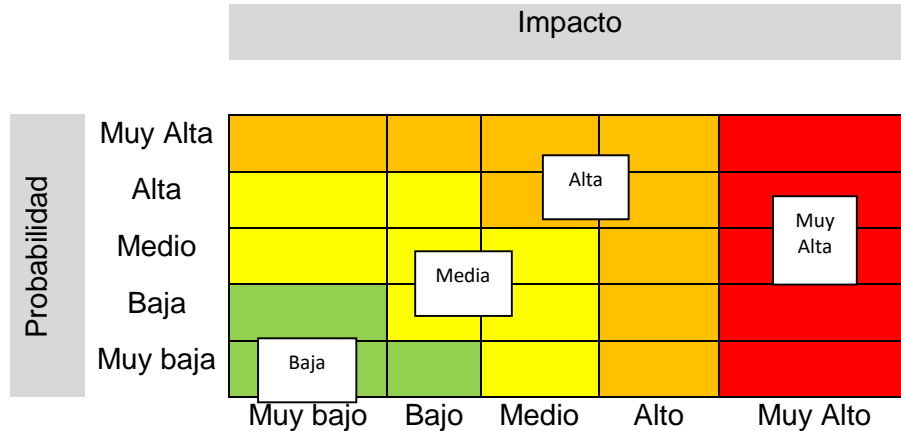
Es la multiplicación del Impacto inherente (%) y la calificación del control CORRECTIVO (%); posteriormente se resta al impacto inherente el resultado de la multiplicación anterior.

1. Impacto = Impacto inherente (%) * Calificación (%)
2. Impacto Residual = Impacto inherente (%) - Resultado I (%)

Nota: En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.

**Cuando se asigna un control de TIPO Correctivo este es el único que permite modificar el impacto.

Cruzando los datos de probabilidad e impacto definidos se obtiene la zona del riesgo residual.



9.7.5 Tratamiento del riesgo

El tratamiento del riesgo implica la preferencia para la modificación de los riesgos y la aplicación del mismo, una vez empleado el tratamiento otorga controles o los modifica, es importante incluir las opciones de análisis, evaluación, desarrollo e implementación que se deben tener en cuenta para el tratamiento del riesgo. Después de definir qué opción (es) de manejo se le va (n) a dar a los riesgos, se deben establecer las actividades de control, responsables, tiempo, indicadores que midan la efectividad de las acciones de control y acciones de contingencia de acuerdo al siguiente cuadro:

Tratamiento	
Plan de acción	
Control Anexo A. NTC-ISO-IEC 27001:2013	
Responsable	
Fecha de implementación	
Fecha de seguimiento	
Indicador	
Estado de plan de acción	

9.8 PRIORIZACIÓN DE RIESGOS A NIVEL DE PROCESOS.

Una vez estimados los niveles de riesgo, se ordenan y se seleccionan aquellos que presentan el nivel más alto para ser consolidados en la herramienta “Matriz de Gestión de Riesgos”, y que deben ser supervisados por el Sistema de Gestión de la Secretaría Distrital de Desarrollo Económico.

Los riesgos que presenten niveles bajos son administrados internamente por los responsables de los procesos.

9.9 SEGUIMIENTO, MONITOREO Y REVISIÓN

Es necesario para la gestión del riesgo realizar un continuo monitoreo, seguimiento y control de cada uno de los planes de tratamiento del riesgo donde se determinen cuáles serán los controles que permitirán mitigar los riesgos y solucionarlos por medio de mantenerlos, de reducir su nivel, eliminarlos o transferirlos.

La revisión de las actividades que se ejecutan se verificará por medio de los planes de tratamiento, identificando la gestión, avances y resultados con relación a los efectos de los cambios de nivel de riesgo que puede perjudicar en las consecuencias y el riesgo se pueda materializar, de tal manera es necesario la revisión continua para adquirir información para la valoración del riesgo e identificar los riesgos emergentes.

9.9.1 Seguimiento y Monitoreo.

Los líderes del proceso serán los responsables en el seguimiento, medición, control y mitigación de los riesgos de cada uno de los procesos, como mínimo realizarán un seguimiento y monitoreo trimestral, respondiendo preguntas sobre el riesgo como: ¿Se materializó?, ¿Por qué? y las observaciones correspondientes de acuerdo con el siguiente cuadro:

¿Se materializó?	
¿Por qué?	
Observaciones	

Al momento de que un riesgo se materialice, el líder del proceso debe formular un plan de mejoramiento en un plazo de quince días hábiles.



Los reportes de los Seguidimientos y Monitoreos se realizarán mediante informes de seguimiento y evaluación.

9.9.2 Revisión.

Las revisiones se realizarán por la Oficina de Control Interno de la SDDE.

9.10 COMUNICACIÓN Y CONSULTA.

Para una gestión de la administración del riesgo exitosa se requiere la divulgación, socialización y capacitación, para la aplicación de los pasos dispuestos en la metodología de administración del riesgo.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE DESARROLLO ECONÓMICO</p>	<p>PROCESO: GESTIÓN DE TIC</p> <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>	<p>Página:</p>	<p>Página 32 de 42</p>	 <p>BAJO ENTENDER MIPG SISTEMA INTEGRADO DE GESTIÓN</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------	----------------	-------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------

La consulta es un aspecto importante a desarrollar, la cual busca tener una difusión de los planes de tratamiento que conllevará a identificar los responsables de la gestión del riesgo de la Secretaría Distrital de Desarrollo Económico.

La política de comunicación de la Secretaría Distrital de Desarrollo Económico está direccionada al mejoramiento de las relaciones, empoderamiento de la entidad y el clima laboral que origine una comunicación transparente con la ciudadanía y un fortalecimiento de los valores de integridad.



La comunicación de la administración de riesgos será realizada de las siguientes formas:

9.10.1 Publicación en la Intranet y página Web institucional.

Una vez aprobados por los líderes de proceso se publicará la matriz de riesgos en su respectivo proceso y en la página web de la entidad Link de Transparencia para consulta.

9.10.2 Procesos de socialización.

El proceso de socialización se llevará a cabo en jornadas a todos los funcionarios y contratistas de la Secretaria Distrital de Desarrollo Económico.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE DESARROLLO ECONÓMICO</p>	<p>PROCESO: GESTIÓN DE TIC</p> <p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>	<p>Página:</p>	<p>Página 33 de 42</p>	 <p>BAJO ESTÁNDAR MIPG SISTEMA INTEGRADO DE GESTIÓN</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------	----------------	-------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------

10. BUENAS PRÁCTICAS PARA LA MITIGACIÓN DE RIESGOS.

El tratamiento de riesgos debe ser un proceso activo en la gestión de riesgos de seguridad de la información, por ello se invita a los líderes o responsables de seguridad de la entidad a:

1. Evaluar el costo beneficio de la definición e implementación de uno o varios controles.
2. Si no es posible implementar un control cuando se tiene un riesgo alto o extremo, evaluar posibles controles compensatorios que ayuden a reducir la probabilidad, el impacto o las dos variables.
3. Los controles deben ser evaluados al menos en término de su eficacia para conocer e informar a la Alta Dirección sobre el avance y mitigación de riesgos latentes en la entidad relacionados con la seguridad.
4. La definición e implantación de controles no debe ir en contra de la operación o flujo normal de las actividades y procesos, es decir, no debo implementar controles que al final terminen afectando alguna característica de la seguridad de la información.
5. Realizar monitoreo constante de los controles definidos e implementados en la entidad.
6. Determinar en el tiempo, la reducción de pérdidas derivadas de materialización de riesgos respecto a la inversión realizada en controles.

12. CRONOGRAMA.

El Plan de Tratamiento de Riesgos de Seguridad de la Información 2023 contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos identificados en la entidad, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información del MinTIC.

CRONOGRAMA PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN				Enero				Febrero				Marzo				Abril				Mayo				Junio				Julio				Agosto				Septiembre				Octubre				Noviembre				Diciembre			
Componente	Responsable	Actividad	Tareas	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4				
Gestión de Riesgos de Seguridad de la Información	Subdirección de Informática y Sistemas	Presentación del Plana Comité de Gestión y Desempeño	Presentar el plan ante el comité																																																
		Sensibilización	Socialización de lineamientos y Herramienta - Gestión de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital.																																																
		Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Contexto, Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información.																																																
			Realimentación, revisión y verificación de los riesgos identificados (Ajustes)																																																
		Aceptación de Riesgos Identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento																																																
		Publicación	Publicación mapas de riesgos en las páginas institucionales																																																
		Seguimiento Fase de Tratamiento	Seguimiento a controles y planes de tratamiento de riesgos identificados (verificación de evidencias)																																																

13. ANEXOS.

Anexo 1. Lista de amenazas a la seguridad de la información.

AMENAZAS MÁS COMUNES		
TIPO	ID	AMENAZAS
1. Personas	1.1	Sobrecarga laboral.
	1.2	Ingeniería social.
	1.3	Coacción.
	1.4	Sabotaje.
	1.5	Errores humanos en el cumplimiento de las labores.
	1.6	Acciones fraudulentas
	1.7	Entrega indebida de la información.
	1.8	Modificación indebida de la información.
	1.9	Situaciones administrativas durante la relación laboral (incapacidades, vacaciones, muerte, licencias).
2. Infraestructura Física	2.1	Contaminación, Polvo, Corrosión.
	2.2	Niveles de temperatura o humedad por fuera de los rangos aceptables.
	2.3	Fallas de electricidad.
	2.4	Señales de interferencia.
	2.5	Daño en instalaciones físicas.
	2.6	Fallas en el aire acondicionado.
	2.7	Fallas en las UPS.
	2.8	Fallas en la planta eléctrica.
	2.9	Desastres naturales.
	2.10	Incendio.
	2.11	Inundación.
	2.12	Asonada/Conmoción civil / Terrorismo/Vandalismo.
	2.13	Desastre accidental.
	2.14	Daño en componentes tecnológicos
3. Sistemas de Información/Servicios informáticos/Información	3.1	Ataque informático para acceder a información reservada o clasificada.
	3.2	Ataque informático para modificar datos.
	3.3	Ingeniería social.
	3.4	Interceptación de información.

	3.5	Cifrado no autorizado de la información por malware o acción mal intencionada.
	3.6	Corrupción de los datos por fallas en el software.
	3.7	Suplantación de usuarios.
	3.8	Abuso de privilegios.
	3.9	Elevación de privilegios.
	3.10	Exposición de información confidencial y de uso interno por errores de configuración.
	3.11	Malware / software malicioso.
	3.12	Denegación de servicios.
	3.13	Alteración de la información
	3.14	Divulgación de la información
	3.15	Uso indebido de la información
	3.16	Uso no autorizado de la información
4. Hardware	4.1	Fallas en los componentes de hardware.
	4.2	Falla de medios de respaldo y recuperación.
	4.3	Fallas en el aire acondicionado.
	4.4	Uso de equipos no autorizados como piñas, videocámaras, y grabadoras entre otros.
	4.5	Hurto de equipos, medios magnéticos o documentos.
	4.6	Fallas en el suministro de energía eléctrica
	4.7	Acceso a información confidencial y de uso interno desde componentes tecnológicos reciclados o desechados.

Anexo 2. Lista de vulnerabilidades que puede afectar a los activos de información.

VULNERABILIDADES MÁS COMUNES DE LOS ACTIVOS		
TIPO	ID	CAUSAS
1. Recursos Humanos	1.1	Ausencia o carencia de personal idóneo.
	1.2	Ausencia o carencia de conocimientos y habilidades en informática.
	1.3	Desconocimiento de políticas, normas, o procedimientos de Seguridad de la Información.
	1.4	Falta de conciencia en el reporte de incidentes de Seguridad de la Información.

	1.5	Ausencia o carencia de conocimiento para el manejo de herramientas de seguridad informática.	
	1.6	Falta de conciencia en Seguridad de la Información.	
	1.7	Desconocimiento de las políticas para el buen uso de los activos de información (Red, Correo, Internet, Sistemas de Información, Chat, Redes Sociales, etc.).	
	1.8	Desconocimiento del marco legal y regulatorio de seguridad de la información.	
	1.9	Desconocimiento de los controles de seguridad informática aplicados a los activos de información que son de su responsabilidad.	
	1.10	Desconocimiento del marco legal y regulatorio de la protección de los datos personales.	
	1.11	Falta de conciencia en Protección de Datos Personales	
	1.12	Desconocimiento de políticas, normas, o procedimientos para el tratamiento de los datos personales.	
	1.13	Sobrecarga en la asignación de funciones.	
	1.14	Ausencia de personal de respaldo para los cargos críticos	
	1.15	Capacidad reducida del proceso en cuanto a recursos humanos	
	2. Procesos	2.1	Ausencia de segregación de funciones o separación de deberes.
		2.2	Ausencia de lineamientos para la divulgación de información al público.
		2.3	Ausencia de procedimientos para la clasificación, etiquetado y manejo de la información.
		2.4	Ausencia de lineamientos de seguridad de la información en todo el ciclo de la relación con los proveedores.
2.5		Ausencia de lineamientos de seguridad de la información para antes de asumir el empleo, durante la ejecución del empleo y para la terminación y cambio del empleo.	
2.6		Ausencia de pruebas de vulnerabilidades técnicas de forma regular.	
2.7		Ausencia de medidas apropiadas para corregir las vulnerabilidades técnicas.	
2.8		Ausencia de registros sobre las actividades del usuario, excepciones, fallas y eventos.	
2.9		Falta de revisión periódica de los registros de eventos de auditoría.	

2.10	Falta de documentación técnica sobre los componentes tecnológicos.
2.11	Falta de integrar la seguridad de la información en todas las fases de la gestión del proyecto.
2.12	Ausencia de lineamientos para el tratamiento de los datos personales.
2.13	Falta definición de requisitos contractuales para la transmisión o transferencia de datos personales.
2.14	Ausencia de procedimientos claros y de herramientas adecuadas para garantizar la eliminación segura de la información o datos personales cuando ya no se requieran.
2.15	Carencia de procedimientos y herramientas para la atención de consultas, reclamos, peticiones de rectificación, actualización y supresión de datos personales.
2.16	Falta de la autorización por parte del titular para el tratamiento de los datos personales.
2.17	Falta de contactos apropiados con las autoridades y grupos de interés de seguridad de la información.
2.18	Inadecuada gestión de los medios removibles (manejo y protección de la información, retiro de los medios removibles, copias de respaldo, control y registro, habilitación de puertos y transferencia de información, disposición final).
2.19	Falta o deficiencia de los procedimientos para el control en los cambios en las instalaciones de procesamiento de información y software que puedan afectar la seguridad de la información.
2.20	Ausencia de procedimientos para controlar la instalación de software en sistemas operativos.
2.21	Falta de reglas para instalación de software por parte de los colaboradores
2.22	Falta de acuerdos de confidencialidad o de no divulgación de la información.
2.23	Falta de acuerdos para la transferencia de información (internos y externos).
2.24	Inadecuada gestión de incidentes y debilidades de seguridad de la información.
2.25	Falta de considerar la seguridad de la información en los Planes de Continuidad del negocio.
2.26	Falta de revisiones periódicas del cumplimiento técnico y de políticas de seguridad.
2.27	Ausencia o deficiencia en los procedimientos de notificación de cambios técnicos y operativos al personal y grupos de trabajo.

	2.28	Falta de verificación de la continuidad de seguridad de la información.
	2.29	Ausencia de controles para restringir el acceso a los códigos fuente de programas.
	2.30	Ausencia de controles sobre los datos de pruebas.
	2.31	Ausencia de controles para la protección de los ambientes de desarrollo.
	2.32	Ausencia de controles para protección de la integridad de los datos que pasan sobre redes públicas o redes inalámbricas.
	2.33	Falta de incluir en los procedimientos de gestión de cambios la revisión de los controles y procedimientos de integridad para asegurar que no se hayan comprometido.
	2.34	Falta de la revisión técnica de las aplicaciones después de cambios en la plataforma de operación.
3. Infraestructura Física /Activo Hardware	3.1	Insuficiencia o mal funcionamiento de controles de acceso físico.
	3.2	Falta de monitoreo en los controles de acceso físico a las edificaciones y recintos.
	3.3	Falta de mantenimiento a la infraestructura física: cableado, racks, aire acondicionado, sistemas de extinción de incendios (detectores de humo, extinguidores etc.), UPS y planta eléctrica.
	3.4	Ubicación en un área susceptible de inundación.
	3.5	Ausencia de protección contra la humedad, polvo y suciedad.
	3.6	Insuficiencia de muebles o archivadores para el almacenamiento de la información.
	3.7	Ausencia de controles antisísmicos.
	3.8	Ausencia o deficiencia en los controles para prevención de incendios.
	3.9	Almacenamiento de documentos impresos sin medidas de protección.
	3.10	Manejo inadecuado de la información.
	3.11	Ubicado en una zona de susceptible de vandalismo, protestas y manifestaciones
	3.12	Acceso a zonas seguras sin control.
4. Sistemas de	4.1	Gestión deficiente de contraseñas.

Información , Servicios informáticos, Información	4.2	Asignación errada de privilegios o derechos de acceso.
	4.3	Ausencia o debilidades de mecanismos de identificación y autenticación de usuario.
	4.4	Inadecuada segregación de funciones, roles y perfiles de usuario.
	4.5	Ausencia de un proceso formal para la revisión periódica de los permisos de acceso de los usuarios.
	4.6	Notificación inoportuna de novedades de usuario a TI.
	4.7	Ausencia de documentación actualizada de los Sistemas de Información.
	4.8	Ausencia de protección a los datos de producción en los ambientes de prueba.
	4.9	Uso de software que no cumple con los requerimientos de los usuarios.
	4.10	Uso de software desactualizado o con vulnerabilidades.
	4.11	Falta de control en el cumplimiento de estándares de actualización de software.
	4.12	Ausencia o insuficiencia de pruebas de aceptación en los sistemas.
	4.13	Ausencia o insuficiencia de pruebas de la funcionalidad de la seguridad de los sistemas.
	4.14	Conexiones a redes públicas sin mecanismos de protección.
	4.15	Configuraciones por defecto.
	4.16	Los ambientes de pruebas, desarrollo y producción no se encuentran separados.
	4.17	Incapacidad del sistema para atender un alto volumen de conexiones.
	4.18	Permitir la ejecución de sesiones simultáneas del mismo usuario en el sistema de información o servicio.
	4.19	Ausencia de alertas de seguridad en los componentes tecnológicos.
	4.20	Uso de protocolos con vulnerabilidades para la protección de la confidencialidad o integridad.
	4.21	Ausencia o deficiencia en los recursos de almacenamiento y procesamiento.

	4.22	Ausencia o deficiencia de seguimiento y monitoreo a los recursos de almacenamiento y procesamiento de información.
	4.23	Habilitación de servicios de red innecesarios.
	4.24	Ausencia de documentación de los puertos que utilizan los sistemas de información o servicios informáticos.
	4.25	Ausencia de líneas base para la instalación de los componentes tecnológicos.
	4.26	Ausencia de control para "terminar sesión" luego de un tiempo determinado de inactividad.
	4.27	Ausencia de controles criptográficos o uso de cifrado débil.
	4.28	Inadecuado uso y protección a las llaves criptográficas durante su ciclo de vida.
	4.29	Ausencia de controles de detección, de prevención y de recuperación para proteger contra códigos maliciosos.
	4.30	Ausencia de copias de respaldo de la información, software e imágenes de los sistemas.
	4.31	Falta de pruebas de verificación de las copias de respaldo.
	4.32	Inadecuada protección de la información de registro.
	4.33	Protección inadecuada de la información en las redes de la información.
	4.34	Protección inadecuada a la información manejada por mensajería electrónica.
	4.35	Falta de integrar la seguridad de la información durante todo el ciclo de vida de los sistemas.
	4.36	Falta o fallas de sincronización de los relojes de los sistemas de procesamiento de información.
	4.37	Ausencia de Planes de Recuperación de Desastres (DRP).
	4.38	Falta de pruebas de verificación a los planes de recuperación de desastres.
	4.39	Ausencia de sistemas redundantes (Alta Disponibilidad), que permita dar una respuesta más rápida en eventos de falla.
5. Hardware	5.1	Mantenimiento insuficiente o inoportuno de los componentes de hardware.
	5.2	Ausencia de mantenimientos preventivos programados.

	5.3	Debilidades en la seguridad perimetral de la red de datos.
	5.4	Arquitectura de red de datos sin cumplir con los requerimientos de seguridad de la información.
	5.5	Ausencia de control sobre dispositivos móviles.
	5.6	Dependencia de un sólo proveedor de Internet.
	5.7	Ausencia o insuficiencia de ANS (Acuerdos de Niveles de Servicio).
	5.8	Susceptibilidad a las variaciones de temperatura.
	5.9	Susceptibilidad a las variaciones de voltaje.
	5.10	Obsolescencia tecnológica.
	5.11	Uso inadecuado de los componentes tecnológicos (equipos de cómputo, dispositivos de red, servidores, etc.).

ELABORÓ	APROBÓ
Joe Alexander Nuñez Yaguna Profesional Universitario SIS	Diego Alonso Arias Murcia Subdirector de Informática y Sistemas