INSTRUCTIVO GESTIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. PROPOSITO

A través de esta guía se busca orientar a la Entidad Distrital a gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) buscando la integración con la Metodología de riesgos del DAFP. Ayudando a que se logre vincular la identificación y análisis de Riesgos del Distrito hacia los temas de la Seguridad de la Información.

2. ALCANCE

El presente documento aplica a todo el distrito de Cartagena y parte desde el planteamiento de la política de seguridad digital hasta las estrategias de seguimiento y mejora de este.

3. GLOSARIO

- **Acceso remoto:** conexión con los recursos informáticos de la entidad desde una ubicación remota a través de una red pública.
- **Activos de información:** son aquellos recursos con los que cuenta una empresa. Es decir, todo elemento que compone el proceso completo de comunicación, partiendo desde la información, el emisor, el medio de transmisión y receptor.
- **Amenaza:** causa potencial de incidente no deseado, el cual puede resultar en daño al Sistema o la Organización. [Fuente: ISO 27000].
- Brecha: se denomina al espacio o ruta a recorrer entre un estado actual y un estado deseado.
- **Calidad:** es la cualidad de un conjunto de información recogida, que reúne entre sus atributos la exactitud, completitud, integridad, actualización, coherencia, relevancia, accesibilidad y confiabilidad necesarias para resultar útiles al procesamiento, análisis y cualquier otro fin que un usuario quiera darles.
- **Confidencialidad:** propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados, asegurando el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.
- **Conservación:** mantener y cuidar la información para que no pierda sus características y propiedades con el paso del tiempo.

- **Disponibilidad:** característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- **Dispositivo móvil:** son todos los equipos tecnológicos que acceden a Internet, tales como: portátiles, teléfonos IP, celulares, TV, tabletas, entre otros.
- **Entrenamiento:** proceso utilizado para enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo u objeto contractual.
- **Equipos de cómputo:** se reconoce como los portátiles o computadores de escritorios que se le asigna a un funcionario o contratista de la entidad.
- **Estándar:** regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.
- **Información:** conjunto organizado de datos generados, obtenidos, adquiridos, transformados o controlados que constituyen un mensaje sin importar el medio que lo contenga (digital y no digital).
- **Ingeniería social:** técnica que utilizan las personas para obtener información, acceso o privilegios en sistemas de información, permitiendo que algún acto perjudique o exponga a la persona o entidad.
- **Integridad:** propiedad que busca mantener los datos libres de modificaciones no autorizadas. A grosso modo, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
- **Monitoreo:** verificación, supervisión, observación crítica o determinación continua del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.
- **MSPI:** Modelo Seguridad y Privacidad de la Información.
- Política: declaración de alto nivel que describe la posición de la entidad sobre un tema específico.
- **Privacidad de la información:** es el aspecto que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos pueden ser compartidos con terceros.

- **Procedimiento:** define específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada.
- **Propietario del activo:** persona o cargo que administra, autoriza el uso, regula o gestiona el activo de información. El propietario del activo aprueba el nivel de protección requerido frente a confidencialidad, integridad y disponibilidad.
- **Riesgo:** efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional, toda la organización). [Fuente: ISO 31000]
- **Sensibilización:** es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.
- **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información. NTC-ISO/IEC 27001.
- **Teletrabajo:** En Colombia, el teletrabajo se encuentra definido en la Ley 1221 de 2008 como: "Una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y comunicación -TIC- para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio especifico de trabajo".
- **TIC:** Tecnologías de la Información y Comunicaciones.
- **Vulnerabilidad:** debilidad identificada sobre un activo y que puede ser aprovechado por una amenaza para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información.

4. RESPONSABLE DE SEGURIDAD DIGITAL

El distrito de Cartagena debe designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información, el cual debe pertenecer a un área que haga parte de la Alta Dirección o Línea Estratégica y las responsabilidades que deberá cumplir respecto a la gestión del riesgo de seguridad digital serán las siguientes:

- Definir el procedimiento para la Identificación y Valoración de Activos.

- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
- Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
- Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

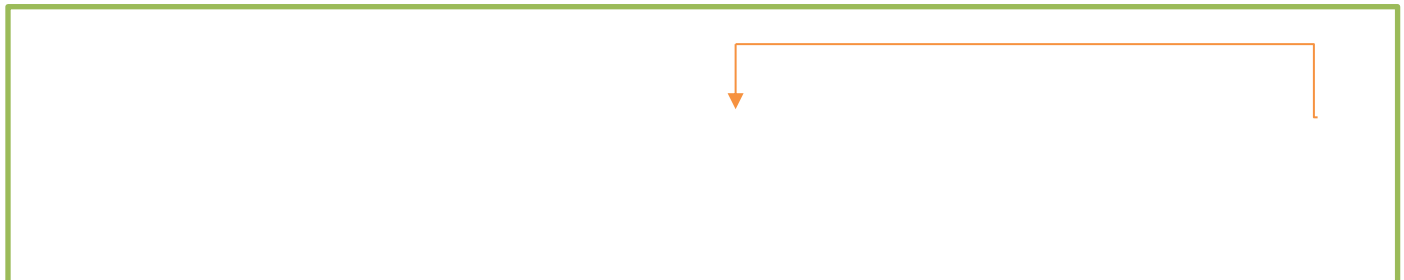
Nota: Como complemento de esta actividad, el distrito de Cartagena debe tomar como referencia lo definido en los Ro

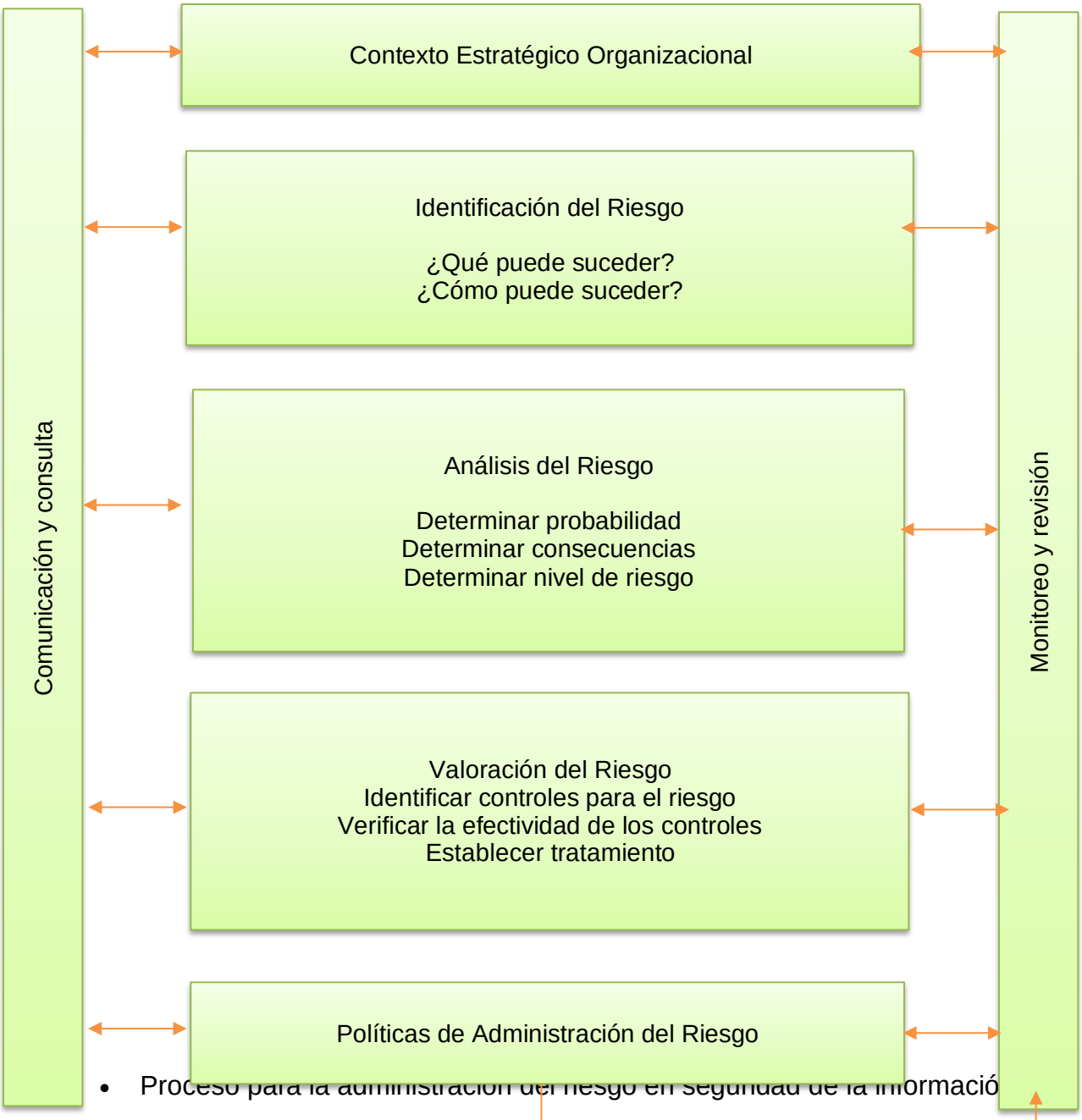
5. INSTRUCCIONES

5.1 VISION GENERAL PARA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACÓN.

El proceso de gestión de riesgo en la seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento.

- Proceso para la administración del riesgo:





- Proceso para la administración del riesgo en seguridad de la información
- Proceso para la administración del riesgo en seguridad de la información

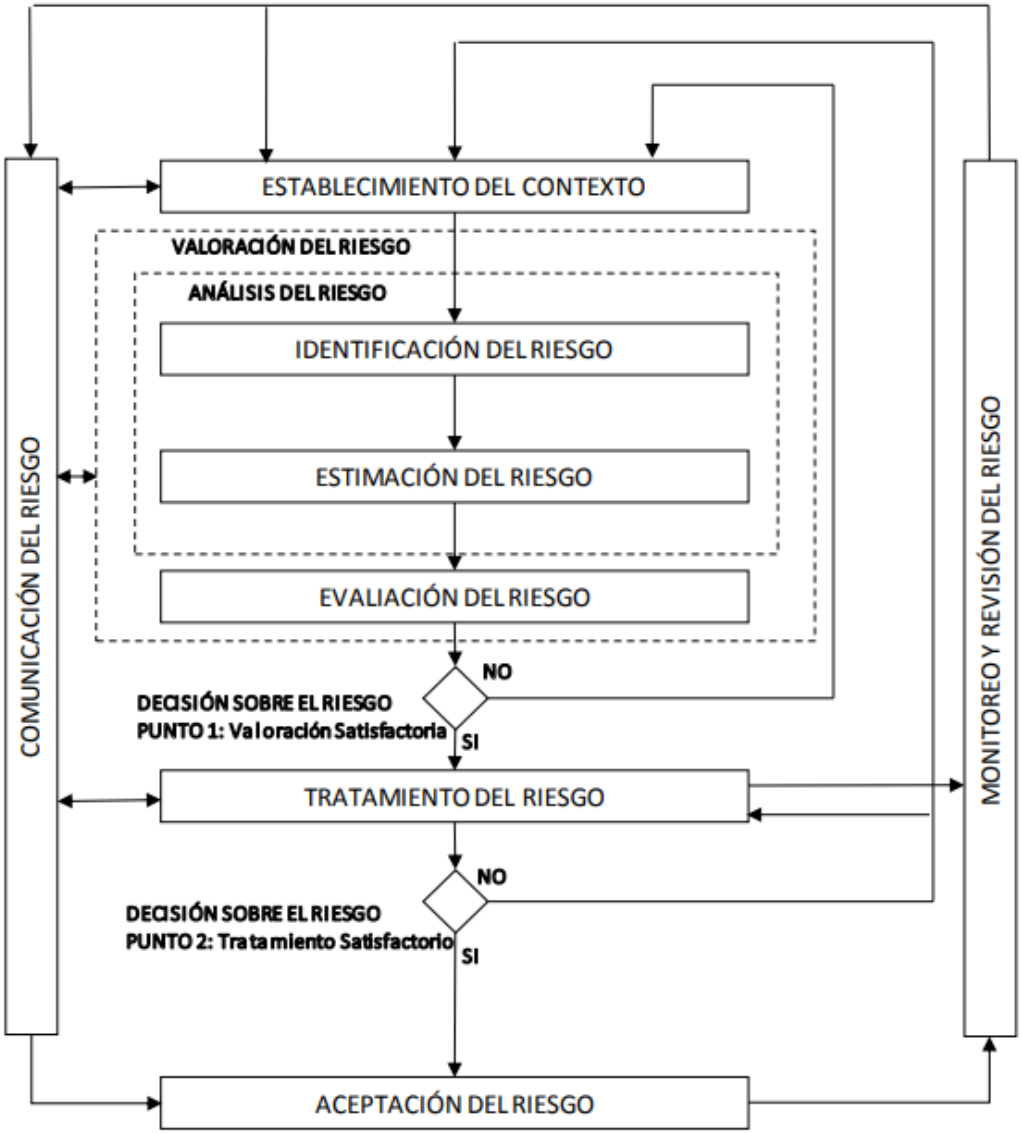


Ilustración 2 Tomado de la NTC-ISO/IEC 27005

Así como se observa la ilustración 2 el proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o el tratamiento de este. Un enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración.

El contexto se establece como primera medida, luego se realiza la valoración del riesgo y si esta suministra información suficiente para determinar de manera eficaz

las acciones que se necesitan para modificar los riesgos a un nivel aceptable entonces la labor está terminada y sigue el tratamiento del riesgo. Si la información no es suficiente, se llevará a cabo otra iteración de la valoración del riesgo con un contexto revisado (por ejemplo, los criterios de evaluación del riesgo, los criterios para aceptar el riesgo o los criterios de impacto).

La eficacia del tratamiento del riesgo depende de los resultados de la valoración del riesgo. Es posible que el tratamiento del riesgo no produzca inmediatamente un nivel aceptable de riesgo residual, en esta situación, si es necesaria, se puede requerir otra iteración de la valoración del riesgo con cambios en los parámetros del contexto (por ejemplo, criterios para la valoración del riesgo, de aceptación o de impacto del riesgo).

La actividad de aceptación del riesgo debe asegurar que los riesgos residuales son aceptados explícitamente por los directores de la entidad. Esto es especialmente importante en una situación en la que la implementación de los controles se omite o se pospone, por ejemplo, por costos.

La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del MSPI.

ETAPAS DEL MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDADDE LA INFORMACION
Planear	• Establecer Contexto • Valoración del Riesgo • Planificación del Tratamiento del Riesgo • Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

Tabla 1 Etapas de la Gestión del Riesgo a lo Largo del MSPI

5.2 CONTEXTO ESTRATÉGICO

El contexto estratégico se tiene en cuenta en el proyecto del MSPI desde el inicio, sobre todo en el momento de definir el objetivo y el alcance del proyecto, así como la política de Seguridad de la Entidad, esto debido a que es necesario tener claro el entorno en el cual se desarrollará el proyecto, precisando cuál será el contexto en el que se desenvolverá, qué procesos involucrará, cual es el flujo de dicho o dichos procesos, y de ésta forma identificar sus objetivos y finalmente, de allí obtener los riesgos de Seguridad asociados.

De igual forma el personal asignado para el desarrollo del MSPI tiene como ventaja, el contexto estratégico avanzado para los modelos de Gestión establecidos en la Entidad, analizando los flujos de procesos ya identificados, para aportar su visión desde el MSPI.

Sin embargo, cabe mencionar que la guía señala las siguientes estrategias a través de las cuales se puede hacer ese levantamiento del contexto Estratégico:

1. Inventario de Eventos
2. Talleres de Trabajo
3. Análisis de Flujo de Procesos

Es esencial determinar el propósito de la gestión del riego en la seguridad de la información ya que esto afecta al proceso total y, en particular, al establecimiento del contexto. Este propósito puede ser:

- Dar soporte al modelo de seguridad de la información al interior de la entidad.
- Conformidad legal y evidencias de la debida diligencia.
- Preparación de un BCP.
- Preparación de un plan de respuesta a incidentes.
- Descripción de los requisitos de seguridad de la información para un producto un servicio o un mecanismo.
- El resultado de la especificación del contexto estratégico es la especificación de los criterios básicos alcance, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

5.2.1 Definición del contexto interno, externo y de los procesos de la entidad pública

Se entiende por contexto externo para la entidad el siguiente:

- Clientes, proveedores de servicios y empresas que sean competencia directa y/o se relacionen con la misión de la entidad pública analizada.
- Normativas o aspectos jurídicos que apliquen directa o indirectamente a la entidad pública; ejemplo, la ley 1581 de 2012 o la ley 1712 de 2014, circulares o regulaciones emitidas por superintendencias o ministerios, como el decreto 1078 de 2015 o el decreto 1499 de 2017.
- Dependencias económicas y financieras por parte de otras empresas.
- Entorno cultural.
- Cualquier otro factor externo de tipo internacional, nacional (gobierno), regional o local.

- Cantidad de ciudadanos a los cuales la entidad pública brinda servicios a través del entorno digital como trámites a través de páginas web.
- Aspectos externos que pueden verse afectados con los riesgos de seguridad digital, tales como el ambiente social, económico y ambiental que tengan alguna relación con las operaciones asociadas a la entidad pública.

El contexto interno considera factores que impactan directamente a:

- Al distrito de Cartagena y sus dependencias, en general, su organización, sistemas de información o servicios, reglamentación interna, número de sedes, empleados, entre otros aspectos.
- Cada uno de los procesos sobre los cuales están soportadas las operaciones.

PARA EL DISTRITO DE CARTAGENA EN GENERAL	PARA LOS PROCESOS
• Recursos económicos, sociales, ambientales, físicos, tecnológicos, financieros, jurídicos, entre otros • Flujos de información y los procesos de toma de decisiones • Empleados, contratistas • Objetivos estratégicos y la forma de alcanzarlos • La misión, visión, valores y cultura de la organización • Sus políticas, procesos y procedimientos Sistemas de gestión (calidad, seguridad en el trabajo, seguridad de la información, riesgos, entre otros) • Toda la estructura organizacional • Roles y responsabilidades • Sistemas de información o servicios	• Identificación de los procesos y su respectiva caracterización • Detalle de las actividades que se llevan a cabo en el proceso • Flujos de información • Identificación y actualización de los activos en la cadena de valor de la entidad pública • Recursos • Alcance del proceso • Relaciones con otros procesos de la entidad pública • Cantidad de ciudadanos afectados por el proceso • Procesos de gestión de riesgos que se tienen actualmente implementados • Personal involucrado en la toma de decisiones

Tabla 2 Factores influyentes en el análisis del contexto

El alcance de la administración del riesgo de seguridad digital debe ser extensible y aplicable a TODOS los procesos de la Alcaldía de Cartagena que indiquen los criterios diferenciales del Modelo de Seguridad y Privacidad de la Información.

6. CRITERIOS BÁSICOS

Dependiendo del alcance y los objetivos de la gestión del riesgo, se pueden aplicar diferentes enfoques, pero debe ser adecuado y que contenga criterios como: criterios de evaluación del riesgo, criterios de impacto, y criterios de aceptación del riesgo:

6.1 CRITERIOS DE EVALUACIÓN DEL RIESGO:

Se recomienda desarrollar criterios para la evaluación del riesgo con el fin de determinar el riesgo en la seguridad de la información de la organización teniendo en cuenta los siguientes aspectos:

- El valor estratégico del proceso de información para la entidad
- La criticidad de los activos de información involucrados en el proceso
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales
- La importancia de la disponibilidad de la, confidencialidad, e integridad de la información para las operaciones y la entidad.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación de la entidad.

De igual modo, los criterios de evaluación de impacto del riesgo y se pueden utilizar para especificar las prioridades del tratamiento del riesgo.

6.2 CRITERIOS DE IMPACTO.

Es recomendable desarrollar criterios de impacto del riesgo y especificarlos en términos del grado de daño o de los costos para la entidad, causados por un evento de seguridad de la información, considerando los siguientes aspectos:

- Nivel de clasificación de los activos de información de los procesos
- Brechas en la seguridad de la información (ejemplo: perdidas de confidencialidad, integridad y disponibilidad de la información)
- Operaciones deterioradas
- Perdida del negocio y del valor financiero
- Alteración de planes y fechas limites
- Daños para la reputación

- Incumplimiento de los requisitos legales

6.3 CRITERIOS DE ACEPTACIÓN DEL RIESGO

Es recomendable desarrollar y especificar criterios de aceptación del riesgo. Estos criterios dependen con frecuencia de las políticas, metas, objetivos de la organización y de las partes interesadas La organización debería definir sus propias escalas para los niveles de aceptación del riesgo. Durante el desarrollo, se deberían considerar los siguientes aspectos:

- Los criterios de aceptación del riesgo pueden incluir umbrales múltiples, con una meta de nivel de riesgo deseable, pero con disposiciones para que la alta dirección acepte los riesgos por encima de este nivel, en circunstancias definidas
- Los criterios de aceptación del riesgo se pueden expresar como la relación entre el beneficio estimado (u otros beneficios del negocio) y el riesgo estimado
- Los diferentes criterios de aceptación del riesgo pueden aplicar a diferentes clases de riesgos, por ejemplo, los riesgos que podrían resultar en incumplimiento con reglamentos o leyes podrían no ser aceptados, aunque se puede permitir la aceptación de riesgos altos si esto se especifica como un requisito contractual
- Los criterios de aceptación del riesgo pueden incluir requisitos para tratamiento adicional en el futuro, por ejemplo, se puede aceptar un riesgo si existe aprobación y compromiso para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo.

Los criterios de aceptación del riesgo pueden diferir de acuerdo con la expectativa de duración que se tenga del riesgo y se podrían considerar los siguientes elementos:

- Criterios del negocio
- Aspectos legales y reglamentarios
- Operaciones
- Tecnología
- Finanzas
- Factores sociales y humanitarios

7. ALCANDE Y LÍMITES PARA LA GESTION DE RIESGOS EN SEGURIDAD DE LA INFORMACION

Es importante que la entidad defina el alcance y los límites y el alcance para de esta manera garantizar que todos los activos relevantes se toman en consideración en la valoración del riesgo.

Al definir el alcance y los límites la entidad debería considerar la siguiente información:

- Objetivos estratégicos de negocio, políticas y estrategias de la organización
- Procesos del negocio
- Funciones y estructura de la organización
- Los requisitos legales, reglamentarios y contractuales aplicables a la organización
- La política de seguridad de la información de la organización
- El enfoque global de la organización hacia la gestión del riesgo
- Activos de información
- Ubicación de la organización y sus características geográficas
- Restricciones que afectan a la organización
- Expectativas de las partes interesadas
- Entorno sociocultural
- Interfaces (Ej. Intercambio de información con otras entidades)

8. IDENTIFICACIÓN DE LOS ACTIVOS

Según la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección. La identificación de activos se debería llevar a cabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo.

8.1.1 Pasos para la identificación de activos

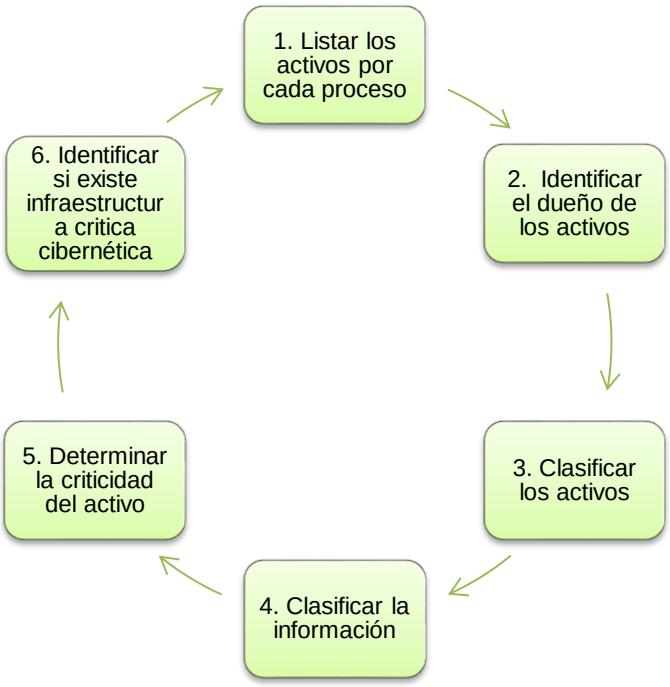


Ilustración 3 Pasos para la identificación de los activos

8.1.1.1 Paso 1. Listar los activos por cada proceso

para realizar la identificación de activos deberá remitirse a la sección 3.1.6 del anexo 4 “Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas” que hace parte de los anexos de la presente guía. En cada proceso, deberán listarse los activos, indicando algún consecutivo, nombre y descripción breve de cada uno.

PROCESO	ACTIVO	DESCRIPCIÓN
Gestión Financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad
Gestión Financiera	Aplicativo de Nómina	Sistema que permite gestionar la nómina y los pagos
Gestión Financiera	Cuentas de Cobro	Formatos de cobro diligenciados

Ilustración 4 Ejemplo para listar activos por cada proceso

NOTA: Las entidades públicas pueden adicionar identificadores o nemónicos para complementar la identificación de los activos.

8.1.1.2 Paso 2. Identificar el dueño de los activos

Cada uno de los activos identificados deberá tener un dueño designado, Si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.

ACTIVO	DESCRIPCIÓN	DUEÑO DEL ACTIVO
Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe Oficina de Nómina
Aplicativo de Nómina	Sistema que permite gestionar la nómina y los pagos	Jefe Oficina de Nómina
Cuentas de Cobro	Formatos de cobro diligenciados	Jefe Oficina de Nómina

Ilustración 5 Ejemplo para identificar el dueño de los activos

NOTA: Generalmente el dueño del activo es el líder del proceso o el jefe de una de las áreas pertenecientes al proceso.

8.1.1.3 Paso 3. Clasificar los activos

Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, servicios, intangibles, componentes de red, personas instalaciones.

La siguiente tabla presenta una propuesta de tipología de activos con el fin de hacer la clasificación mencionada.

Tipo de activo	Descripción
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades
Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información
Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software)

Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el 'Good Will', entre otros
Componentes de red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros
Personas	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa.

Tabla 3 Tipos de activos

ACTIVO	TIPO DE ACTIVO
Base de datos de nómina	Información
Aplicativo de Nómina	Software
Cuentas de Cobro	Información

Tabla 4 Ejemplo clasificación de activos

8.1.1.4 Paso 4. Clasificar la información

Realizar la clasificación de la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos, el dominio 8 del Anexo A de la norma ISO27001:2013 y demás normatividad aplicable. Esto adicionalmente ayudará a dilucidar la importancia de los activos de información en el siguiente Paso 5.

ACTIVO	TIPO DE ACTIVO	Ley 1712 de 2014	Ley 1581 de 2012
Base de datos de nómina	Información	Información Reservada	No contiene datos personales
Aplicativo de Nómina	Software	N/A	N/A
Factura de venta	Información	Información Pública	No contiene datos personales

Tabla 5 Ejemplo para clasificación de información

NOTA: Al realizar la identificación del contexto externo, la entidad debería tener plenamente identificados los aspectos regulatorios y normativos con los que deberá cumplir, las leyes enunciadas (1712 de 2014 y 1581 de 2012) pueden ser de cumplimiento para la mayoría de las entidades públicas sin embargo es tarea de la entidad pública determinar si hay más o menos aspectos regulatorios para tener en cuenta respecto a la información. El área jurídica de la entidad debe colaborar en esta tarea específica.

8.1.1.5 Paso 5. Determinar la criticidad del activo

Ahora la entidad pública debe evaluar la criticidad de los activos, a través de preguntas que le permitan determinar el grado de importancia de cada uno, para posteriormente, durante el análisis de riesgos tener presente esta criticidad para hacer una valoración adecuada de cada caso.

En este paso la entidad pública debe definir las escalas (que significa criticidad ALTA, MEDIA y BAJA) para valorar los activos respecto a la confidencialidad, integridad y disponibilidad e identificar su nivel de importancia o criticidad para el proceso. Para definir estas escalas puede tomar como referencia la Guía de Gestión de Activos del Modelo de Seguridad y Privacidad de la Información (MSPI), estas escalas deberán ser definidas y documentadas en un procedimiento de gestión de activos que debe ser aprobado por parte de la línea estratégica de la entidad pública.

ACTIVO	TIPO DE ACTIVO	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Base de datos de nómina	Información	ALTA	ALTA	ALTA	ALTA
Aplicativo de Nómina	Software	BAJA	BAJA	BAJA	BAJA
Listas de asistencia	Información	BAJA	BAJA	BAJA	BAJA

Tabla 6 Ejemplo para determinar la criticidad del activo

Una vez se ejecute la identificación de los activos, la entidad pública debe definir si gestionará los riesgos en todos los activos del inventario o solo en aquellos que tengan un nivel de criticidad Alto, esto debe estar debidamente documentando y aprobado por la Línea Estratégica – Alta dirección.

8.1.1.6 Paso 6. Identificar si existe infraestructura critica cibernética

Se invita a que la entidad identifique y reporte a las instancias y autoridades respectivas en el Gobierno nacional si poseen ICC. Un activo es considerado infraestructura crítica si su impacto o afectación podría superar alguno de los siguientes 3 criterios:

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

Fuente 1 Tomado de Comando Conjunto Cibernético (CCOC), Comando General Fuerzas

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).

Con base a los seis (6) pasos vistos previamente, la entidad pública podría generar un formato como el siguiente (ejemplo de referencia) para generar tanto su procedimiento de identificación e inventario de activos como el formato para hacer su levantamiento. El formato puede variar en cada entidad según la necesidad y normatividad aplicable o si desea integrar otra información.

PROCESO	ACTIVO	DESCRIPCIÓN	DUEÑO DEL ACTIVO	TIPO DEL ACTIVO	LEY 1712 DE 2014	LEY 1581 DE 2012	CRITICIDAD RESPECTO A SU CONFIDENCIALIDAD	CRITICIDAD RESPECTO A COMPLETITUD O INTEGRIDAD	CRITICIDAD RESPECTO A SU DISPONIBILIDAD	NIVEL DE CRITICIDAD

Tabla 7 Formato para la identificación de los activos

9. IDENTIFICACIÓN DE RIESGOS

De acuerdo con lo planteado en la guía, la identificación del riesgo se hace con base en causas identificadas para los procesos, dichas causas pueden ser internas o externas, según lo que haya identificado la Entidad a través del Contexto estratégico.

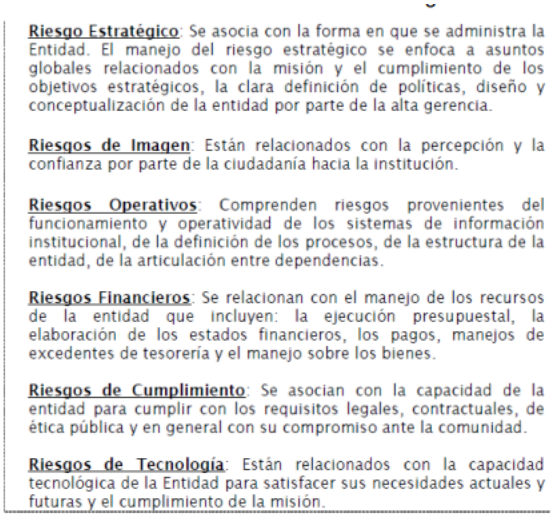
En este momento es importante establecer cuáles son los activos críticos para asociarlos a los procesos correspondientes y de allí generar el listado de procesos críticos. Inventariar los activos de información sensible, revisar los procesos según la clasificación del MECI y del modelo de gestión, con este punto se revisa la pertinencia del alcance planteado para el MSPI.

En esta etapa es especialmente importante la participación del personal designado para la implementación del MSPI, dentro de la mesa interdisciplinaria en la cual se revisan los procesos, tomando parte en la identificación de los riesgos de seguridad, para los procesos identificados como críticos dentro del planteamiento del MSPI.

Para este capítulo, la guía inicia con la definición de algunos términos que son necesarios dentro del empleo de esta metodología, estos términos son comúnmente empleados en las Entidades para efectos de la aplicación del sistema de Calidad o el MECI, y se listarán a continuación:

- Proceso
- Objetivo del Proceso
- Identificación de Activos
- Riesgo
- Causas (Amenazas y Vulnerabilidades).
- Descripción del Riesgo.
- Efectos de la materialización del Riesgo

Como acto seguido se debe realizar la clasificación de los riesgos, para esto la guía presenta las siguientes opciones:



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 de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.

Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

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 Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

Fuente: Guía de Riesgos DAFP

Ilustración 6 Lista de Clasificación de Riesgos

La entidad tiene la posibilidad de agregar a este listado los riesgos de seguridad que considere pertinentes dentro del desarrollo del MSPI en el proceso de identificación del riesgo, teniendo en cuenta cómo se podría vulnerar alguno de los pilares de la seguridad de la información:

- Disponibilidad
- Confidencialidad
- Integridad

9.1 ANÁLISIS DE RIESGOS

Para la entidad es muy importante documentar y especificar cada una de las etapas surtidas para el proceso de Gestión de Riesgos, de allí la Entidad tendrá su propia guía para poder replicar este mismo procedimiento para cualquier etapa que sea necesaria, ya sea para el momento en la que la Entidad decida extender el alcance de la aplicación del MSPI, o para la etapa de revisión de los controles, en la cual la entidad sólo debería poder aplicar la misma metodología simplemente teniendo como base el trabajo ya adelantado en las primeras etapas del MSPI.

A continuación, se presentan una serie de etapas propuestas para la Generación del análisis de riesgos de las Entidades, basadas la norma ISO27005.

9.2 IDENTIFICACIÓN DEL RIESGO

El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida, las siguientes etapas deberían recolectar datos de entrada para esta actividad.

9.3 IDENTIFICACIÓN DE LAS AMENAZAS

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo (ej. Acciones no autorizadas, daño físico, fallas técnicas).

Algunas amenazas pueden afectar a más de un activo y en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

A continuación, se describen una serie de amenazas comunes.

D= Deliberadas, A= Accidentales, E= Ambientales

TIPO	AMENAZA
Daño físico	Fuego
	Agua
	Contaminación
	Accidente Importante
	Destrucción del equipo o medios
	Polvo, corrosión, congelamiento
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
	Fenómenos volcánicos
	Fenómenos meteorológicos
	Inundación
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado
	Perdida de suministro de energía

	Falla en equipo de telecomunicaciones
Perturbación debida a la radiación	Radiación electromagnética
	Radiación térmica
	Impulsos electromagnéticos
Compromiso de la información	Interceptación de señales de interferencia comprometida
	Espionaje remoto
	Escucha encubierta
	Hurto de medios o documentos
	Hurto de equipo
	Recuperación de medios reciclados o desechados
	Divulgación
	Datos provenientes de fuentes no confiables
	Manipulación con hardware
	Manipulación con software
	Detección de la posición
Fallas técnicas	Fallas del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información.
Acciones no autorizadas	Uso no autorizado del equipo
	Copia fraudulenta del software
	Uso de software falso o copiado
	Corrupción de los datos
	Procesamiento ilegal de datos
Compromiso de las funciones	Error en el uso
	Abuso de derechos
	Falsificación de derechos
	Negación de acciones
	Incumplimiento en la disponibilidad del personal

Tabla 8 Tipos de amenazas

Es recomendable tener particular atención a las fuentes de amenazas humanas. Estas se desglosan específicamente en la siguiente tabla:

AMENAZAS DIRIGIDA POR EL HOMBRE		
FUENTE DE AMENAZA	**MOTIVACIÓN**	**ACCIONES AMENAZANTES**
Pirata informático, intruso ilegal	• Reto • Ego • Rebelión • Estatus • Dinero	• Piratería • Ingeniería Social • Intrusión, accesos forzados al sistema • Acceso no autorizado
Criminal de la computación	• Destrucción de la información • Divulgación ilegal de la información • Ganancia monetaria • Alteración no autorizada de los datos	• Crimen por computador • Acto fraudulento • Soborno de la información • Suplantación de identidad • Intrusión en el sistema
Terrorismo	• Chantaje • Destrucción • Explotación • Venganza • Ganancia política • Cubrimiento de los medios de comunicación	• Bomba/Terrorismo • Guerra de la información • Ataques contra el sistema DDoS • Penetración en el sistema • Manipulación en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	• Ventaja competitiva • Espionaje económico	• Ventaja de defensa • Ventaja política • Explotación económica • Hurto de información • Intrusión en privacidad personal • Ingeniería social • Penetración en el sistema • Acceso no autorizado al sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	• Curiosidad • Ego • Inteligencia • Ganancia monetaria • Venganza • Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	• Asalto a un empleado • Chantaje • Observar información reservada • Uso inadecuado del computador • Fraude y hurto • Soborno de información • Ingreso de datos falsos o corruptos • Interceptación • Código malicioso • Venta de información personal

		• Errores en el sistema • Intrusión al sistema • Sabotaje del sistema • Acceso no autorizado al sistema.

Tabla 9 Amenazas dirigidas por el hombre

9.4 IDENTIFICACIÓN DE LAS VULNERABILIDADES

Para realizar una correcta identificación de vulnerabilidades es necesario conocer la lista de amenazas comunes, la lista de inventario de activos y el listado de controles existentes.
Se pueden identificar vulnerabilidades en las siguientes áreas:

- Organización.
- Procesos y procedimientos.
- Rutinas de gestión.
- Personal
- Ambiente físico
- Configuración del sistema de información.
- Hardware, software y equipos de comunicaciones.
- Dependencia de partes externas.

NOTA: La sola presencia de una vulnerabilidad no causa daños por sí misma, dado que es necesario que exista una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

A continuación, se enunciarán vulnerabilidades conocidas:

TIPO	VULNERABILIDADES
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software

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

Tabla 10 Vulnerabilidades

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

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

TABLA DE VULNERABILIDADES COMUNES		
TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios.
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección física	Hurtos medios o documentos.
	Falta de cuidado en la disposición final	Hurtos medios o documentos.
	Copia no controlada	Hurtos medios o documentos.
SOFTWARE	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencias de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos

	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
RED	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlado de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Fallas en la producción de informes	Uso no autorizado del equipo
	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables	Fallas del equipo de telecomunicaciones
	Punto único de fallas	Fallas del equipo de telecomunicaciones

	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
	Ausencia del personal	Incumplimiento en la disponibilidad
	Procedimientos inadecuados de contratación	Destrucción de equipos y medios
	Entrenamiento insuficiente en seguridad	Error en el uso
PERSONAL	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos.
LUGAR	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Hurto de medios o documentos
	Ubicación en área susceptible de inundación	Destrucción de equipos o medios
	Red energética inestable	Falla en equipo de telecomunicaciones
	Ausencia de protección física de la edificación (Puertas y ventanas)	Hurto de medios o documentos
	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos

	Ausencia de proceso formal para la revisión de los derechos de acceso	Abuso de los derechos
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)	Abuso de los derechos
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información	Abuso de los derechos
	Ausencia de auditorias	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
ORGANIZACIÓN	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de nivel de servicio o insuficiencia de estos	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento formal para la documentación del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso de correo electrónico	Error en el uso

	Ausencia de procedimientos para introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en bitácoras	Error en el uso
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia de política sobre limpieza de escritorio y pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado de equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado de equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	Uso de software falsificado o copiado

Tabla 11 Vulnerabilidades comunes

9.5 MÉTODOS PARA LA VALORACIÓN DE LAS VULNERABILIDADES TÉCNICAS:

Ver guía de pruebas de efectividad.

9.5.1 IDENTIFICACIÓN DE LAS CONSECUENCIAS

Para la identificación de las consecuencias es necesario tener:

- Lista de activos de información y su relación con cada proceso de la entidad.
- Lista de las amenazas y vulnerabilidades con respecto a los activos y su pertinencia.

NOTA: Una consecuencia puede ser la pérdida de la eficacia, condiciones adversas de operación, pérdida del negocio, reputación, daño, entre otros.

En esta actividad se deben identificar los daños o las consecuencias para entidad que podrían ser causadas por un escenario de incidente. Un escenario de incidente es la descripción de una amenaza que explota una vulnerabilidad determinada o un conjunto de vulnerabilidades relacionadas a un activo.

Las entidades deberían identificar las consecuencias operativas de los escenarios de incidentes en términos de:

- Tiempo de investigación y reparación
- Pérdida de tiempo operacional
- Pérdida de oportunidad
- Salud y seguridad
- Costo financiero
- Imagen, reputación y buen nombre

Número del riesgo	RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/VULNERABILIDADES	CONSECUENCIAS
R1							
R2							
R3							
R4							
R5							
R6							
R7							
R8							
R9							
R10							
R11							
R12							
R13							
R14							
R15							

Tabla 12 Identificación del riesgo

10. EVALUACIÓN DE RIESGO

Para continuar con el análisis y la evaluación del riesgo depende de la información obtenida en las fases de identificación anteriormente descritas de Identificación de los riesgos, es por ello por lo que la entidad debe crear los criterios de riesgo definiendo los niveles de riesgo aceptado por la Organización.

De esta forma la guía menciona cuales son los pasos claves en el análisis de riesgos, probabilidad e impacto, definiendo como sigue cada uno de ellos:

“Por Probabilidad se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.

Por Impacto se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo”.

De esta forma se procede a hacer la “calificación del riesgo”, en la cual se realiza una estimación, de cuál podría ser la probabilidad de ocurrencia del riesgo y el impacto que traería éste, en caso de materializarse.

De igual forma la guía presenta una “tabla de probabilidad” y una “Tabla de Impacto”, en las cuales presenta 5 niveles para medir la probabilidad de ocurrencia y 5 niveles para lograr medir el impacto, dando las herramientas con las cuales se definen los criterios de riesgo.

Por otro lado, presenta la tabla en la cual se señalan “los impactos de mayor ocurrencia en las Entidades del Estado”, en este punto se toca el impacto sobre la Confidencialidad de la Información, el cual es uno de los pilares de la Seguridad de la Información.

Extremo	
Alto	
Moderado	
Bajo	

		20%	40%	60%	80%	100%
		Leve	Menor	Moderado	Mayor	Catastrófico
100%	Muy Alta	Alto	Alto	Alto	Alto	Extremo
80%	Alta	Moderado	Moderado	Alto	Alto	Extremo
60%	Media	Moderado	Moderado	Moderado	Alto	Extremo
40%	Baja	Bajo	Moderado	Moderado	Alto	Extremo
20%	Muy Baja	Bajo	Bajo	Moderado	Alto	Extremo

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

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

NUMERO DEL RIESGO	RIESGO	ACTIVO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
R1							
R2							
R3							
R4							
R5							
R6							

Tabla 13 Evaluación del riesgo

11. IDENTIFICACIÓN DE CONTROLES EXISTENTES

Se debe realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, por ejemplo, la duplicidad de controles, además de esto mientras se identifican los controles se recomienda hacer una verificación para garantizar que los existentes funcionan correctamente.

Los controles que se planifican para implementar de acuerdo con los planes de implementación de tratamiento de riesgo se deberían considerar en la misma forma que aquellos que ya están implementados.

Un control existente planificado se podría calificar como ineficaz, insuficiente o injustificado, si es injustificado o insuficiente, se debería revisar el control para determinar si se debe eliminar o reemplazar por otro más adecuado. Actividades para revisar controles existentes o planificados:

- Revisando los documentos que contengan información sobre los controles.
- Verificación con las personas responsables de la seguridad de la información y los usuarios.
- Efectuar revisiones en sitio comparando los controles implementados contra la lista de controles que deberían estar.
- Cuáles están implementados correctamente y si son o no eficaces.
- Revisión de los resultados de las auditorías internas.

El distrito de Cartagena podrá mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles sugeridos en la ISO/IEC 27001:2013.

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

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

Procedimientos operacionales y responsabilidades	Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
Procedimientos de operación documentados	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	Control: se deberían controlar los cambios

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

Tabla 14 Ejemplos de controles y los dominios a los que pertenece

RIESGO	FECHA DE INICIO	FECHA FINAL	RESPONSABLE	CONTROLES	OBSERVACIONES
R1					
R2					
R3					
R4					
R5					
R6					
R7					
R8					
R9					
R10					
R11					
R12					
R13					
R14					
R15					
R16					

Tabla 15 Controles asociados

12. DOCUMENTOS DE REFERENCIA:

Guía MinTIC Gestión de Riesgos
Plan de tratamiento de riesgos de seguridad y privacidad de la información
Guía para la administración del riesgo y el diseño de controles en entidades públicas
Anexo 4 Modelo nacional de gestión de riesgos de seguridad de la información

13. CONTROL DE CAMBIOS

FECHA	DESCRIPCION DE CAMBIOS	VERSION
28/06/2023	Elaboración del documento	1.0

14. VALIDACION DEL DOCUMENTO

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre: Jasmin Herrera – Diana Manrique Cargo: Asesor externo Fecha: 28/06/2023	Nombre: Jasmin Herrera – Diana Manrique Cargo: Asesor externo Fecha: 28/06/2023	Nombre: Ingrid Solano Cargo: Jefe Oficina Asesora de Informática Fecha: 28/06/2023