

FOMVIVIENDA
Empresa de Fomento
de Vivienda de Armenia

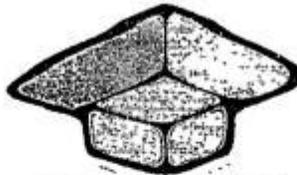
RESOLUCIÓN NÚMERO 014 DE 2025 (27 DE ENERO DE 2025)

"POR MEDIO DEL CUAL SE ADOPTA EL PLAN DE TRATAMIENTO DE RIESGOS DE LA INFORMACIÓN DE LA EMPRESA DE FOMENTO DE VIVIENDA DE ARMENIA "FOMVIVIENDA" Y SE REGULA SU FUNCIONAMIENTO

El Gerente General de la Empresa de Fomento de Vivienda de Armenia "FOMVIVIENDA", en uso de sus facultades legales y reglamentarias, en especial las que le confiere el artículo 29 del Acuerdo de Junta No. 004 del 01 de abril del 2024, y

CONSIDERANDO:

- Que en el artículo 15 de la Constitución Política consagra el derecho fundamental de las personas a conservar su intimidad y familiar, al buen nombre y a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellos en bancos de datos y en archivos de las entidades públicas.
- Que la Ley 1273 de 2009 por medio del cual se modifica el código penal, crea un nuevo bien jurídico tutelado denominado "De la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones "TIC", entre otras disposiciones.
- Que la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales reglamentado por el decreto 1377 de 2013, incorporo los lineamiento necesarios para que los organismos públicos y privados identificaran los roles y la tipología de datos que son objeto de protección constitucional, así mismo, dispuso las condiciones las cuales se deben recolectar los datos personales que posteriormente serán vinculados con la administración de una base datos.
- Que la Ley 1712 de 2014, Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública en las instituciones del Estado, estableció los procedimientos para el ejercicio y garantías para el registro de activos de información.
- Que por medio del Decreto 1078 de 2015, se expidió el Reglamento del Sector de Tecnologías de la Información y de las Comunicaciones en el Artículo 2.2.9.1.2,1 de dicho decreto se instituye los componentes de la Estrategia y es cuarto componente denominado Seguridad y Privacidad de la Información "Comprende las acciones las acciones transversales en los demás componentes enunciados, tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada.
- Que por medio de CONPES 3854 de 2016 se fijó la plan Nacional de seguridad digital, para que las entidades del Estado constituyan mecanismos para la gestión de los riesgos digitales
- Que conforme de la normatividad citada surge la necesidad de adoptar una plan de seguridad y privacidad de la información y protección de datos considerando el papel estratégico de las tecnologías de información y comunicaciones – TIC; además de la importancia de mitigar riesgos alrededor de la información mediante la implementación de planes para el manejo de incidentes, así como las herramientas para respaldar las actividades ejecutadas en FOMVIVIENDA, incentivando la cultura de seguridad de la información a los usuarios, previniendo o solucionando posibles ataques informáticos, virus, robos, uso indebido de software o pérdida de información.



FOMVIVIENDA
Empresa de Fomento
de Vivienda de Armenia

RESOLUCIÓN NÚMERO 014 DE 2025

- Que el fundamento de un plan de seguridad y privacidad de la información y protección de datos de buscar la gestión del conocimiento como base para la mejora continua de la misma, adaptándola a la normatividad vigente en el sector, las tendencias tecnológicas y los cambios de la gestión de procesos y procedimientos tecnológicos en la Empresa de Fomento de Vivienda de Armenia "FOMVIVIENDA".
- Que la Empresa de Fomento de Vivienda de Armenia "FOMVIVIENDA" presenta la tecnología como uno de los procesos estratégicos, lo que origina la necesidad de generar un Plan Estratégico de Tecnologías de la información acorde con los lineamientos y exigencias del Ministerio de las tecnologías de la Información y las Comunicaciones
- Que la Empresa de Fomento de Vivienda de Armenia" FOMVIVIENDA, propende por ser una entidad alineada con las nuevas tecnologías y marcos de trabajo de TI.

En mérito de lo antes expuesto:

RESUELVE:

ARTÍCULO 1º. Objeto. Adoptar el PLAN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, en la Empresa de Fomento de Vivienda de Armenia como norma fundamental para el desarrollo de proyectos de tecnología con una gestión eficiente y optimización de los recursos, servicios TIC, y los sistemas de información.

ARTÍCULO 2º. Ámbito de Aplicación: Los planes aplican a los servidores públicos, contratistas, proveedores y/o terceros usuarios de la información impresa, digital y la soportada sobre las tecnologías de información y las comunicaciones de la Empresa de Fomento de Vivienda de Armenia.

ARTÍCULO 3º Implementación. Todas las áreas de la Empresa de Fomento de Vivienda de Armenia deberán implementar los planes adoptados a través del presente acto administrativo, conforme a sus responsabilidades y competencias.

ARTICULO 4 Vigencia. La presente Resolución rige a partir de su publicación

Dada en Armenia Quindío, a los Veintisiete (27) días del mes de enero de 2025.

PUBLÍQUESE Y CÚMPLASE,


HARRISON SANTAMARÍA HUERTAS
Gerente General

Empresa de Fomento de Vivienda de Armenia FOMVIVIENDA

Proyectó: M. Alejandra Atehortua Arias Contratista 
Revisó: Claudia Lorena Sierra Gómez - Directora Administrativa y Financiera 
Archivado en: C.I.; Serie Documental



ALCALDÍA DE
ARMENIA



FOMVIVIENDA
Empresa de Fomento
de Vivienda de Armenia

**GESTIONAMOS
CALIDAD DE VIDA
EN ARMENIA.**

2025

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



www.fomvivienda.gov.co

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

EMPRESA DE FOMENTO DE VIVIENDA DE ARMENIA - FOMVIVIENDA

Responsables:

Ingeniero de Sistemas – Dirección Administrativa y Financiera

Armenia, Enero 2025

TABLA DE CONTENIDO

1	INTRODUCCIÓN	3
2	OBJETIVO	4
3	ALCANCE	5
4	MARCO NORMATIVO	6
5	VISIÓN DE LA GESTIÓN DE RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN	7
6	ANÁLISIS DE RIESGOS DE FOMVIVIENDA	8
7	TERMINOLOGIA	25

1. INTRODUCCIÓN

La gerencia de la empresa de fomento de vivienda de Armenia – FOMVIVIENDA ha señalado una política y claro apoyo a los temas relacionados con el área de Seguridad de la información, la cual se ve reflejado en el Plan Estratégico de Tecnologías de la Información “PETI”, el cual fue actualizado mediante **resolución 024 del 28 de Enero del año 2024** **“POR MEDIO DEL CUAL SE ADOPTA EL PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACIÓN “PETI” DE LA EMPRESA DE FOMENTO DE VIVIENDA DE ARMENIA “FOMVIVIENDA” Y SE REGULA SU FUNCIONAMIENTO**”, donde se instauran cada uno de los comprometidos dentro la Política de “Gobierno Digital” antes “Gobierno en Línea” y demás instrumentos que reglamentan ésta política.

3. ALCANCE

El tratamiento de riesgos de seguridad de la información, teniendo en cuenta su tratamiento será aplicado sobre todos los activos de información de FOMVIVIENDA identificados por cada uno de los procesos y que hacen parte del PETI de FOMVIVIENDA; teniendo como referencia las normas vigentes, las técnicas definidas por la entidad para la gestión del riesgo definida, las políticas y recomendaciones previstas en la ISO 27001 para su rastreo, monitoreo y estimación enfocado al acatamiento y mejoramiento continuo.

4. MARCO NORMATIVO

- **MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA:** Documento se elaboró con la recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPi de la Estrategia de Gobierno en Línea – GEL / Gobierno Digital.
- **PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA:** Establecer las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad del servicio, en el Mapa de Procesos del Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC.
- **Ley 1712 de 2014:** Ley de Transparencia y de acceso a la información pública nacional.
- **Decreto 1008 del 14 de Junio de 2018:** "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".



6. ANÁLISIS DE RIESGOS DE FOMVIVIENDA



<p>Modificaciones a la constitución política</p>	<p>Acto administrativo de cumplimiento, en el que la empresa para el fomento de vivienda de armenia se vea en la necesidad de modificar el tratamiento de la información.</p>	<p>SI</p>	<p>Raro</p>	<p>1</p>	<p>Insignificante</p>	<p>1</p>	<p>1</p>	<p>11</p>	<p>BAJO Leyes, decretos, resoluciones, ordenanzas, etc. Que expida el gobierno nacional a cargo del ministerio de Tecnologías de la información y comunicaciones MinTic, sobre el trato, seguridad y manejo de la información que tienen los entes gubernamentales.</p>	<p>Raro</p>	<p>1</p>	<p>Insignificante</p>	<p>1</p>	<p>1</p>	<p>11</p>	<p>BAJO Mantener actualizado sobre los actos administrativos, noticias y/o políticas que expide el MinTIC</p>	<p>1. Acatar las nuevas leyes y intentar aplicar cada una de las recomendaciones del gobierno nacional</p>	<p>Dirección Administrativa y Financiera y Control Interno.</p>	<p>Acto administrativo gobierno nacional</p>	<p>Abierto</p>
--	---	-----------	-------------	----------	-----------------------	----------	----------	-----------	--	-------------	----------	-----------------------	----------	----------	-----------	--	--	---	--	----------------

Virus informáticos	Los virus informáticos tienen por objeto alterar el funcionamiento normal de los equipos de cómputo, tienen la facilidad de propagarse con facilidad con el uso de memorias USB, correo electrónico, etc.	SI	Poco probable	2	Moderado	3	6	23	MODERADO FOMVIVENDA cuenta con antivirus en cada uno de los equipos de cómputo de la misma (incluido el equipo que hace de servidor), protegiendo o los equipos en tiempo real. Es de destacar que a través del año, se realiza mantenimiento preventivo incluyendo mantenimiento de software y sistema operativo (desinfección).	Poco probable	2	Menor	2	4	22	BAJO	Se debe estar en constante alerta prestando atención a la actualización de las bases de datos del antivirus en cada uno de los equipos de cómputo de la entidad.	1. Inspeccionar con utensilios de software libre el equipo afectado. 2. Detectar si se es necesario realizar la restauración del sistema operativo y revisar dentro de las copias de seguridad la información pertinente a solicitud del funcionario afectado.	Contratista de Apoyo de la gestión Administrativa como ingeniero de Sistemas.	Fallas de tipo software en equipos de cómputo de FOMVIVIENDA	Abierto
Seguridad o Robo	Hurto de información, equipos de cómputo o equipos de red con los que cuenta FOMVIVIENDA	SI	Poco probable	2	Menor	2	4	22	BAJO Para reducir el riesgo de robo el centro administrativo municipal de armenia donde se encuentra físicamente FOMVIVENDA	Poco probable	2	Insignificante	1	2	21	BAJO	Realizar una sistema de seguimiento de préstamo de equipos para llevar la trazabilidad de que funcionario tiene equipos de la entidad.	Aplicar pólizas de equipos para la correspondiente compra del equipo robado.	Contratista de Apoyo de la gestión Administrativa como ingeniero de Sistemas, Dirección Administrativa y Financiera.	Robo de equipo	Abierto

									control y monitoreo de temperatura.													
Copias de seguridad sistemas de información	Riesgo asociado a la falta de copias de seguridad de las bases de datos de los sistemas de información con los que cuenta la entidad, también se tiene en cuenta la falta de implementación de documentos de trazabilidad así como de falta de implementos tecnológicos para dicha tarea, dichas copias se realizan quincenalmente para contratistas y semestral para personal de Planta.	SI	Raro	1	Menor	2	2	12	BAJO	FOMVIVENDA cuenta con una política de respaldo de la información de los equipos de la entidad, este respaldo se periódicamente en discos duros externos que se encuentran en el área de sistemas.	Poco probable	2	Moderado	3	6	23	MODERADO	Comprobar que las copias de seguridad si se realicen correctamente y de que se tenga la documentación correspondiente para llevar la trazabilidad	N/A	Contratista de Apoyo de la gestión Administrativa como ingeniero de Sistemas	Servidores sin respaldo de base de datos por mas de 3 tres días	Abierto

Falta de Actualización de la infraestructura tecnológica	Se refiere a la falta de adquisición y/o actualización de equipos que se van quedando obsoletos por su tiempo de uso, así como la debida actualización de el cableado pertinente de la red de ethernet	SI	Poco probable	2	Moderado	3	6	23	MODERADO FOMVIVIE NDA cuenta con un plan de anual de adquisición, dentro del cual se tiene proyecta la adquisición de equipos y/o dispositivos que ayuden a actualizar la infraestructura tecnológica de la misma.	Raro	1	Menor	2	2	12	BAJO	Confirmar que dentro del plan de compras anual, se indique la adquisición de equipos informativos así como de buscar en la transición a los protocolos de IPV4 a IPV6	Incluir dentro del presupuesto de FOMVIVIENDA un ítem que destine recursos para la actualización de equipos informáticos y actualización de la red.	Contratista de Apoyo de la gestión Administrativa como ingeniero de Sistemas, Dirección Administrativa y Financiera.	Presupuesto insuficiente para actualizaciones tecnológicas	Abierto
--	--	----	---------------	---	----------	---	---	----	--	------	---	-------	---	---	----	-------------	---	---	--	--	---------

<p>Incumplimiento de los contratistas</p>	<p>Este riesgo puede ocurrir a causa del posible atraso en la contratación, ejecución o trasgresión del de los contratos de actualización, modificación, mantenimiento, que se asumen durante la vigencia, contratos como licenciamiento de antivirus, outsourcing de impresoras, proveedor de internet, proveedor de línea telefónica, Sistema de software contable, Intranet y Página virtual, etc.</p>	<p>SI</p>	<p>Poco probable</p>	<p>2</p>	<p>Moderado</p>	<p>3</p>	<p>6</p>	<p>23</p>	<p>MODERADO</p> <p>Dentro de los procesos de contratación que tiene FOMVIVIENDA, con los proveedores de sistemas de información, se cuenta cláusulas de cumplimiento y responsabilidad que ayudan a mitigar el riesgo inherente al incumplimiento.</p>	<p>Poco probable</p>	<p>2</p>	<p>Menor</p>	<p>2</p>	<p>4</p>	<p>22</p>	<p>BAJO</p> <p>Monitorear a través de actas de supervisión y/o informes periódicos que proveedores de sistemas de información y el personal si estén cumpliendo con sus contratos</p>	<p>1. Terminación anticipada del contrato. 2. Búsqueda de nuevos proveedores de servicios. 3. Contratación del nuevo proveedor</p>	<p>Dirección Administrativa y Financiera.</p>	<p>Informe de actividades mensual incompleto</p>	<p>Abierto</p>
---	---	-----------	----------------------	----------	-----------------	----------	----------	-----------	---	----------------------	----------	--------------	----------	----------	-----------	--	--	---	--	----------------

Retrasos en Procesos Administrativos	Implementar los procesos tecnológicos relacionados con la ejecución de los contratos, involucrando el correcto desarrollo de trámites administrativos, llegando a retrasar por exigencias en el cumplimiento de requisitos.	SI	Poco probable	2	Menor	2	4	22	BAJO FOMVIVIENDA busca el resguardo de la seguridad de la información, por tal motivo se intenta contar como primer lugar con todas las políticas necesarias personal capacitado en el área de Sistemas.	Poco probable	2	Menor	2	4	22	BAJO	Verificar y dar prioridad a los procesos de contratación involucrados en esta tarea dentro de FOMVIVIENDA.	Indagar las posibles causas de la no contratación y adquisición de herramientas TIC y proveedores de sistemas de información.	Contratista de Apoyo de la gestión Administrativa como ingeniero de Sistemas, Dirección Administrativa y Financiera.	No continuidad de los procesos de contratación	Abierto
--------------------------------------	---	----	---------------	---	-------	---	---	----	--	---------------	---	-------	---	---	----	-------------	--	---	--	--	---------

<p>Procesos de capacitación constante del personal TI</p>	<p>Tener en cuenta la actualización y capacitación de los conocimientos en sistemas de información del ingeniero contratista del Area de Sistemas, pero también tener en cuenta las distintas capacitaciones a contratistas en general de FOMVIVIENDA sobre el area TIC</p>	<p>SI</p>	<p>Poco probable</p>	<p>2</p>	<p>Moderado</p>	<p>3</p>	<p>6</p>	<p>23</p>	<p>MODERADO El profesional contratado para el area de Sistemas debe estar debidamente actualizado y contextualizado con cada uno de los sistemas de información que tiene la empresa FOMVIVIENDA para dar un soporte primario en caso de inconvenientes. Paralelamente dicho personal debe capacitar periodicamente a los funcionarios de las otras areas de la empresa en temas de las tecnologías, información y las comunicaciones</p>	<p>Raro</p>	<p>1</p>	<p>Menor</p>	<p>2</p>	<p>2</p>	<p>12</p>	<p>BAJO</p>	<p>Capacitación constantemente al personal TIC y contratistas en general de FOMVIVIENDA en el área TIC.</p>	<p>El gobierno nacional a través de la estrategia de gobierno digital, de Min TIC motiva a las entidades de todo el país a mejorar procesos y realizar capacitación en nuestras políticas de orden nacional.</p>	<p>Contratista de Apoyo de la gestión Administrativa como ingeniero de Sistemas.</p>	<p>N/A</p>	<p>Abierto</p>
---	---	-----------	----------------------	----------	-----------------	----------	----------	-----------	--	-------------	----------	--------------	----------	----------	-----------	--------------------	---	--	--	------------	----------------

<p>Accesos no autorizados a los sistemas de información</p>	<p>Referente al acceso a las bases de datos no autorizados de los diferentes aplicativos de sistemas de información utilizados por parte de la entidad y de computadores que manejen información confidencial de la misma.</p>	<p>SI</p>	<p>Poco probable</p>	<p>2</p>	<p>Mayor</p>	<p>4</p>	<p>8</p>	<p>24</p>	<p>ALTO Como parte de las políticas de seguridad de la información aprobadas por la dirección administrativa y financiera, la entidad cuenta con una política de bloqueo de sesión de los equipos cada 5 minutos de inactividad. Lo anterior con el fin de evitar accesos no autorizados a los sistemas cuando el funcionario responsable del equipo no se encuentre en el sitio de trabajo. Por otra parte, y con el fin de evitar acceso no autorizado a los sistemas de información por parte</p>	<p>Poco probable</p>	<p>2</p>	<p>Menor</p>	<p>2</p>	<p>4</p>	<p>22</p>	<p>BAJO</p>	<p>Actualizar bases de datos de antivirus y firewall. Además de mantener actualizadas las políticas de seguridad de la información, estar en constante vigilancia de las posibles puertas digitales y/o físico de acceso a la red de datos de FOMVIEDA</p>	<p>Ejecutar los protocolos de seguridad de la información y las acciones contingentes establecidas en el DRP de la entidad</p>	<p>Contratista de Apoyo de la gestión Administrativa como ingeniero de Sistemas.</p>	<p>Reportes de firewall y antivirus</p>	<p>Abierto</p>
---	--	-----------	----------------------	----------	--------------	----------	----------	-----------	---	----------------------	----------	--------------	----------	----------	-----------	--------------------	--	--	--	---	----------------

Equivocaciones humanas	Nace del desconocimiento, descuido, o mal uso de un sistema de información o aplicativo de la entidad.	SI	Posible	3	Moderado	3	9	33	<p>ALTO</p> <p>Se deben brindar capacitaciones continuas a los funcionarios de la entidad, sobre el manejo de los aplicativos de la entidad, además de eso, se deben generar copias de seguridad quincenales de los funcionarios contratistas y de los aplicativos mensualmente.</p>	Raro	1	Menor	2	2	12	<p>BAJO</p>	Capacitaciones por parte del Área de Sistemas y copias de seguridad de contratistas y de las bases de datos de los aplicativos de la entidad	Si el daño es grande, se puede respaldar la información con las copias de seguridad realizadas por parte del ingeniero de Sistemas,	Contratista de Apoyo de la gestión Administrativa como ingeniero de Sistemas.	Anomalia presentada al área de Sistemas	Abierto
------------------------	--	----	---------	---	----------	---	---	----	---	------	---	-------	---	---	----	--------------------	--	---	---	---	---------

Activos de la información desactualizados	La no actualización de los activos de la información por parte de la Dirección Administrativa y Financiera, puede llegar a generar un riesgo inherente a la pérdida de la información y/o desconocimiento de lo que se encuentra instalado en cada equipo de la entidad.	SI	Raro	1	Moderado	3	3	13	MODERADO Se deben tener actualizados los activos de la información para su correspondiente actualización anual. Igualmente, tener un levantamiento de la información de los equipos de la entidad, su licenciamiento y sus características de hardware.	Raro	1	Menor	2	2	12	BAJO	Generar un inventario anual de cada uno de los activos de información con sus respectivas características técnicas.	1. De acuerdo a los resultados del inventario anual generar un documento de necesidad tecnológica ante la dirección administrativa y financiera. 2. Tener en cuenta cada una de las necesidades halladas en el inventario para el momento de crear el PETI del año posterior a la generación del inventario.	Dirección Administrativa y Financiera de FOMVIVIENDA, Contratista de Apoyo de la gestión Administrativa como ingeniero de Sistemas.	Posible deterioro y/o obsolescencia de equipos tecnológicos en los centros de trabajo de cada uno de los funcionarios de FOMVIVIENDA	Abierto
---	--	----	------	---	----------	---	---	----	---	------	---	-------	---	---	----	-------------	---	--	---	--	---------

Equipos de red (switch y WiFi) conectados a la vista de funcionarios y de fácil acceso, así como no autorizados.	Riesgo asociado a equipos de red identificados en cada una de las áreas de la entidad, los cuales tienen acceso cualquier funcionario o persona ajena a la entidad, pudiéndose conectar a internet, así como equipos no autorizados previamente a la red WiFi de Fomvivienda.	SI	Posible	3	Moderado	3	9	33	ALTO	Períodicamente se revisan equipos no autorizados conectados a la red de Fomvivienda tanto en la red LAN o WLAN.	Raro	1	Menor	2	2	12	BAJO	Tener una revisión constante desde el router principal de FOMVIVIENDA que equipos no autorizados están conectados en la red de la entidad.	1. Inspeccionar en la configuración de la red de FOMVIVIENDA los equipos conectados. 2. estar pendiente de los equipos físicos que se conectan a algún punto de la red interna de FOMVIVIENDA.	Contratista de Apoyo de la gestión Administrativa como ingeniero de Sistemas.	Reportes generados tras auditoria de equipos conectados a la red de datos de FOMVIVIENDA
--	---	----	---------	---	----------	---	---	----	-------------	---	------	---	-------	---	---	----	-------------	--	--	---	--

7. TERMINOLOGIA

Administración del riesgo: Conjunto de elementos de control que al interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
(ISO/IEC 27000)

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evalúa.

Control: Medida que modifica el riesgo. Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo: Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto: Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación de los controles de seguridad de la información sobre cada uno de los procesos.

Tratamiento del Riesgo: Proceso para modificar el riesgo” (Icontec Internacional, 2011).

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.