POLÍTICA
SEGURIDAD DIGITAL

INDEPORTES ANTIOQUIA

GOBERNACIÓN DE ANTIOQUIA

UNIDOS
DEJAMOS EN **ALTO**
EL **DEPORTE DE**
ANTIOQUIA

INTRODUCCIÓN

El Modelo Integrado de Planeación y Gestión –MIPG-, regulado mediante el Decreto Nacional 1499 de 2017, es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio, y el mismo debe ser adoptado por los organismos y entidades de los órdenes nacional y territorial de la Rama Ejecutiva del Poder Público.

MIPG cuenta con siete dimensiones, entre ellas la de **Gestión con Valores para los Resultados** cuyo propósito es la realización de actividades orientadas a lograr los resultados propuestos y materializar la planeación estratégica del instituto en el marco de los valores contenidos en el código de integridad. A través de las políticas diseñadas en esta dimensión, el Instituto busca garantizar los derechos de los ciudadanos, de acuerdo al modelo de operación por procesos desde la organización administrativa interna y la interacción con los ciudadanos.

De acuerdo al Departamento Administrativo de la Función Pública, con la política de Seguridad Digital se fortalecen las capacidades de los grupos del valor de la entidad, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital.

INDEPORTES ANTIOQUIA, diseña esta política adoptando los lineamientos del Modelo de Gestión de Riesgos de la Seguridad Digital -MGRSD- y el Modelo de Seguridad y Privacidad de la Información-MSPI, diseñados por el Ministerio de las Tecnologías de la Información y Comunicación de Colombia-Mintic, los cuales son desarrollados para las entidades públicas para implementar la Política Nacional de Seguridad Digital Conpes 3854 de 2016. Es de anotar que el modelo MGRSD retoma fundamentos de la Norma Técnica ISO 27001:2013.

INTRODUCCIÓN

En esta medida, este documento presenta los componentes que integran la política: Principios fundamentales y Generales, las cuatro fases planeación, ejecución, monitoreo y revisión, y mejora continua de gestión del riesgo de seguridad digital; a su vez contempla la consulta y las comunicaciones como ejes transversales.

OBJETIVO

Definir los lineamientos para identificar, gestionar, tratar y mitigar los riesgos y amenazas que puedan afectar la seguridad digital y el uso de las TIC en INDEPORTES ANTIOQUIA.

ALCANCE

El alcance de esta política es proteger la información del instituto, minimizar los riesgos y asegurar la continuidad del servicio en del INDEPORTES ANTIOQUIA.

INDEPORTES ANTIOQUIA

GOBERNACIÓN DE ANTIOQUIA

OBJETIVOS ESPECÍFICOS

- Definir los elementos en la fase de planeación para la gestión de riesgos de seguridad digital.
- Establecer las herramientas institucionales para la identificación, valoración, evaluación de controles y tratamiento a los riesgos de seguridad digital.
- Determinar los mecanismos para el seguimiento de los riesgos asociados a la seguridad digital.

FUNDAMENTOS NORMATIVOS

- **Ley 1928 de 2018** *"Por medio de la cual se aprueba el «convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en budapest.*

- **Acuerdo 02 de 2018.** *"Por el cual se establece la estructura de la Jurisdicción Especial para La Paz – JEP".*

- **Conpes 3854 de 2016.** *Política Nacional de Seguridad Digital*.

- **Decreto 1078 de 2015.** *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"*

- **Ley 1712 de 2014** . *"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".*

- **Ley estatutaria 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.

- **Decreto 103 de 2015.** "por el cual se reglamenta parcialmente la Ley **1712** de 2014 y se dictan otras disposiciones". **Derogado Parcialmente por el Decreto 1081 de 2015.**

- **Ley 1273 de 2009.** "*Por medio de la cual se modifica el Código Penal, se 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, entre otras disposiciones".*

FUNDAMENTOS NORMATIVOS

- ***Norma Técnica Colombiana NTC ISO 27000:2013****: Requisitos para la Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la información.*

POLÍTICA
SEGURIDAD DIGITAL

El Gobierno Nacional a través del Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC, da cumplimiento a la Política Nacional con la implementación del Modelo Nacional de Gestión de Riesgos de Seguridad Digital, de ahora en adelante (MGRSD), que contribuye a unas mejores prácticas en la ejecución y desarrollo de la gestión de riesgos digitales en las organizaciones carácter público o privado. Para ellos en necesario precisar el propósito de cada uno de los instrumentos diseñados por el gobierno nacional

La Política Nacional de Seguridad Digital busca "fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el País". (CONPES 3854 del 11 de abril de 2016 - numeral 5.1 objetivo general).

De otro lado, el **Modelo Gestión de Riesgos de Seguridad Digital** (GRSD) busca "brindar un marco para la identificación de las amenazas y vulnerabilidades a las que una entidad pueda estar expuesta desde la perspectiva del entorno cibernético, con el fin de fortalecer el ambiente de control, intensificar la confianza de las múltiples partes interesadas en el medio digital e impulsar la prosperidad económica, social de la entidad y, por ende, del país". (Documento Modelo Nacional de Gestión de Riesgos de Seguridad Digital, objetivo general).

El **Modelo de Seguridad y Privacidad de la Información (MSPI)** El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases: Diagnóstico, planificación, implementación, evaluación de desempeño y mejora continua, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

PRINCIPIOS DE LA POLÍTICA
SEGURIDAD DIGITAL

El Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD) plantea principios fundamentales y generales para que las partes interesadas puedan gestionar la seguridad digital, fomentando confianza con el entorno digital. A continuación de relacionan:

PRINCIPIOS FUNDAMENTALES:

- Salvaguardar los derechos humanos y los valores fundamentales de los ciudadanos
- Adoptar un enfoque incluyente y colaborativo
- Asegurar una responsabilidad compartida entre las múltiples partes interesadas
- Adoptar un enfoque basado en la gestión de riesgos

PRINCIPIOS DE LA POLÍTICA

SEGURIDAD DIGITAL

PRINCIPIOS GENERALES:

INDEPORTES ANTIOQUIA

GOBERNACIÓN DE ANTIOQUIA

La Gestión de Riesgos de Seguridad Digital crea y protege el valor

La Gestión de Riesgos de Seguridad Digital es una parte integral de todos los procesos del Instituto

La Gestión de Riesgos de Seguridad Digital aborda explícitamente la incertidumbre

La Gestión de Riesgos de Seguridad Digital es parte de la toma de decisiones, una vez evaluada las posibles consecuencias de las amenzas y vulberabilidades digitales

La Gestión de Riesgos de Seguridad Digital se basa en la mejor información disponible

La Gestión de Riesgos de Seguridad Digital está adaptada

La Gestión de Riesgos de Seguridad Digital toma en consideración los factores humanos y culturales

La Gestión de Riesgos de Seguridad Digital es transparente e inclusiva

La Gestión de Riesgos de Seguridad Digital facilita la mejora continua de la organización

FASES DE LA POLÍTICA DE
SEGURIDAD DIGITAL

INDEPORTES ANTIQUIA, en materia de Seguridad Digital adopta para la implementación de la política el Modelo de Gestión de Riesgos de Seguridad Digital desarrollado por Min Tic, el cual contempla cuatro fases:

INDEPORTES ANTIOQUIA

GOBERNACIÓN DE ANTIOQUIA

FASES POLÍTICA DE SEGURIDAD DIGITAL

A continuación, se presentan las Fases que implementan el Modelo de Gestión de Riesgo de Seguridad Digital- MGRSD.

FASE # 1. PLANIFICACIÓN DE LA GESTIÓN DE RIESGO DE SEGURIDAD DIGITAL (GRSD)

Esta fase es fundamental ya que establece los elementos como punto de partida para el proceso de gestión de riesgos de seguridad digital en el instituto, se desarrolla a través de las etapas de: Compromiso de la alta dirección, contexto de la entidad, establecimiento del contexto externo e interno, identificación de las partes interesadas, Asociación de la política de gestión de riesgos de seguridad digital con políticas existentes, definición de roles y responsabilidades y definición de recursos GRSD.

1.1. Compromiso de la Alta Dirección

La dirección del INSTITUTO DEPARTAMENTAL DE ANTIOQUIA "INDEPORTES", entendiendo la importancia de una adecuada gestión de la seguridad digital, se comprometerá con la implementación del **Modelo de Gestión del Riesgo de la Seguridad Digital -MGRSD**, estableciendo un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

El INSTITUTO, con la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

FASES POLÍTICA DE SEGURIDAD DIGITAL

2. Contexto Estratégico

Para el análisis del contexto estratégico en materia de riesgos de seguridad digital, se acogen los lineamientos definidos en la política de Planeación Institucional de INDEPORTES ANTIOQUIA.

3. Identificación de partes interesadas

En la caracterización del proceso de Gestión de la Plataforma TIC, se identifican las partes interesadas.

4. Asociación de la política de gestión de riesgos de seguridad digital con políticas existentes

INDEPORTES ANTIOQUIA, para implementar el Modelo de Gestión de Riesgos determina en la política de Planeación Institucional los lineamientos para la administración del riesgo y el diseño de controles para los Riesgos de gestión, corrupción y seguridad digital de acuerdo a la guía de la Función Pública.

5. Definición de roles y responsabilidades para la gestión de riesgos de seguridad digital (GRSD)

La Gestión del Riesgo de Seguridad Digital del instituto está bajo la responsabilidad de la Gerencia, pero así mismo las diferentes áreas del instituto en cabeza de los líderes, servidores y/o contratistas y usuarios, tienen responsabilidades frente a la infraestructura tecnológica y los sistemas de información.

6. Recursos para el desarrollo de la gestión de riesgos de seguridad digital

Para el desarrollo del Modelo de Gestión de Riesgos de Seguridad Digital, se tendrán en cuenta los recursos económicos y de talento humano necesarios para la definición, seguimiento, control y mejoramiento continuo. Estas necesidades son contempladas en el instrumento Plan Anual de Adquisiciones y el PETI.

7. Criterios para la gestión del riesgo de seguridad digital

El instituto acoge los lineamientos para la Gestión de Riesgos de Seguridad Digital establecidos por el Departamento Administrativo de Función Pública - DAFP.

FASE #2. EJECUCIÓN DEL MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL (MGRSD)

En esta fase se desarrollan un conjunto de actividades que permite la implementación del MGRSD, a saber:

2.1 Identificación de activos de información

Todos los activos deben estar claramente identificados, para ello el Instituto elabora y mantiene un inventario incluyendo la clasificación de los mismos, recibiendo los niveles de protección adecuados, ya que con base en su valor y de acuerdo a otras características particulares requiere un tipo de manejo especial y se clasifica así: información pública reservada, información pública clasificada, información pública, No clasificada. Así mismo, se identifica el

responsable del activo.

FASES POLÍTICA DE SEGURIDAD DIGITAL

Así mismo, el instituto establece a través de las políticas, estándares de seguridad y uso de recursos informáticos para proteger:

- La información generada, procesada o resguardada por los procesos y activos de información que hacen parte de los mismos.
- La información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La información de las amenazas originadas por parte del personal.
- el Data Center, Centros de Cableados y la infraestructura tecnológica que soporta sus procesos críticos.

Por otro lado, controla la operación de sus procesos misionales garantizando la seguridad de los recursos tecnológicos y las redes de datos e implementa control de acceso a la información, sistemas y recursos de red.

De igual manera garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información, que haya una adecuada gestión de los eventos.

La disponibilidad de sus procesos y la continuidad de su operación basada en el impacto que pueden generar los eventos y el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

FASES POLÍTICA DE SEGURIDAD DIGITAL

Además de los lineamientos de las políticas internas, dispuestas a cumplir en INDEPORTES ANTIOQUIA, se adoptan las estrategias para la seguridad de la información definidas en la NTC ISO 27001:2013, y las que la Entidad disponga a partir del análisis de los riesgos de la seguridad de la Información.

FASE#3. MONITOREO, REVISIÓN Y REPORTE DEL MGRSD

El seguimiento y evaluación de riesgos se realiza de acuerdo a la orientación de la alta dirección y los lineamientos del Departamento Administrativo de La Función Pública- DAFP. Así mismo, la Oficina de Sistemas e Informática, monitorea de forma permanente que los sistemas y recursos de la red operen adecuadamente

Así mismo, con la Asesoría de Control Interno se realizan las auditorías internas para determinar si los controles, sus objetivos, los procesos y procedimientos continúan de conformidad a este documento y para analizar y planificar acciones de mejora.

La Rendición de cuentas en materia de riesgos de seguridad digital se realiza conforme a las orientaciones establecidas en la **Política de Participación Ciudadana en la Gestión Pública de INDEPORTES ANTIOQUIA.**

Por último, para la medición del desempeño, se Formulan indicadores de acuerdo a los lineamientos establecidos en la política de Planeación Institucional, acogiéndose al procedimiento establecido por INDEPORTES ANTIOQUIA, que describe los lineamientos para la identificación, seguimiento, control y análisis de los indicadores. Además, se diligencia el reporte oficial de la implementación de la política a través del FURAG, dispuesto por el Departamento Administrativo de la Función Pública.

FASES POLÍTICA DE SEGURIDAD DIGITAL

FASE #4. MEJORA PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD DIGITAL

Para el mejoramiento continuo de la gestión de riesgos de seguridad digital, el instituto da tratamiento a través de la matriz de registro de mejoras. Una vez realizado el seguimiento y evaluación se determina si hay materialización o no. En caso de presentarse hallazgos productos de auditorías internas o externas o de la identificación de no conformidades, se procede a diseñar las acciones de mejora correspondientes para disminuir las causas que han dado origen a los hallazgos.

CONCEPTOS ATENER

EN CUENTA

Acceso a la información pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Actitud hacia el riesgo: Enfoque de la organización para evaluar y eventualmente buscar, retener, tomar o alejarse del riesgo. (NTC ISO 31000:2011).

Activo: Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854:2016, pág.56).

Activo cibernético: En relación con la privacidad de la información, se refiere al activo que contiene información que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización. (ISO 2700:2016).

Amenaza cibernética: Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (CONPES 3854).

CONCEPTOS ATENER
EN CUENTA

Ataque cibernético: Acción organizada y premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (Ministerio de Defensa de Colombia).

CCOC: Comando Conjunto Cibernético, grupo de ciberseguridad y ciberdefensa creado por el Ministerio de Defensa para apoyar todos los aspectos relacionados con seguridad cibernética en conjunto con el CCP y el Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT.

CERT: *Computer Emergency Response Team* (Equipo de respuesta a emergencias cibernéticas). (Universidad Carnegie-Mellón).

Cibercrímen (Delito cibernético): Conjunto de actividades ilegales asociadas con el uso de las tecnologías de la información y las comunicaciones, como fin o como medio. (CONPES 3854, pág. 87).

Ciberdefensa: Empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. (CONPES 3854, pág. 88).

Ciberseguridad: Conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio. (CONPES 3854, pág. 87).

CONCEPTOS ATENER

EN CUENTA

Ciberterrorismo: Es el uso del ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o Estado trayendo como consecuencia una violación a la voluntad de las personas. (CONPES 3854, pág. 88).

Ciberdelincuencia: Acciones ilícitas que son cometidas mediante la utilización de un bien o servicio informático. (Ministerio de Defensa de Colombia).

Ciberdelito/Delito cibernético: Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Cibernética: Ciencia o disciplina que estudia los mecanismos automáticos de comunicación y de control o técnica de funcionamiento de las conexiones de los seres vivos y de las máquinas. (Diccionario de la lengua española).

Cibernético: Adjetivo masculino y femenino para denominar todo cuanto tiene relación con la cibernética: órgano cibernético, proceso cibernético o que está especializado en cibernética, así como también a la persona que se dedica a ella. (Diccionario de la lengua española).

Convergencia: Evolución coordinada de redes que antes eran independientes hacia una uniformidad que permita el soporte común de servicios y aplicaciones. (Rec. UIT-T Q.1761, 3.1).

CONCEPTOS ATENER

EN CUENTA

CSIRT: Por su sigla en inglés: *Computer Security Incident Response Team* (Equipo de respuesta a incidentes de seguridad cibernética). (http:// www.first.org).

Comunicación y consulta: Procesos continuos y reiterativos que una organización lleva a cabo para suministrar, compartir u obtener información e involucrarse en un diálogo con las partes involucradas con respecto a la gestión del riesgo. (NTC ISO 31000:2011).

Consulta: La consulta es un proceso de doble vía de la comunicación informada entre una organización y sus partes involucradas, acerca de algún tema, antes de tomar una decisión o determinar una dirección para dicho tema. La consulta es: un proceso que tiene impacto en la decisión a través de la influencia más que del poder; y: una entrada para la toma de decisiones, no para la toma conjunta de decisiones. (NTC ISO 31000 definición 2.12.).

Compartir el riesgo: Compartir con otra de las partes el peso de la pérdida o el beneficio de la ganancia proveniente de un riesgo particular. (NTC ISO 31000:2011).

Conocimiento, capacidades y empoderamiento: Las múltiples partes interesadas deben entender los riesgos de seguridad digital. Deben ser conscientes de que el riesgo de seguridad digital puede afectar el logro de sus objetivos económicos y sociales, y el de otros. Deben estar educados al respecto, poseer las habilidades necesarias para entender el riesgo, administrarlo y evaluar su impacto. (CONPES 3854, pág. 25).

Consecuencia: Resultado o impacto de un evento que afecta a los objetivos. (NTC ISO 31000:2011).

Contexto externo: Ambiente externo en el cual la organización busca alcanzar sus objetivos. (NTC ISO 31000:2011).

CONCEPTOS ATENER

EN CUENTA

Contexto interno: Ambiente interno en el cual la organización busca alcanzar sus objetivos. (NTC ISO 31000:2011).

Control: Medida que modifica al riesgo. (NTC ISO 31000:2011), medios para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Cooperación: Las múltiples partes interesadas deben cooperar, incluso más allá de sus fronteras, a nivel regional e internacional.

Criterios del riesgo: Términos de referencia frente a los cuales se evalúa la importancia de un riesgo. (NTC ISO 31000:2011).

Derechos humanos y valores fundamentales: Las múltiples partes interesadas deben gestionar los riesgos de seguridad digital de manera transparente y compatible con los derechos humanos y los valores fundamentales. La implementación de la gestión de riesgos de seguridad digital debe ser compatible con la libertad de expresión, el libre flujo de la información, la confidencialidad de la información, la protección de la privacidad y los datos personales. Las organizaciones deben tener una política general de transparencia acerca de sus prácticas y procedimientos para la gestión de riesgos de seguridad digital.

Entorno digital: Ambiente, tanto físico como virtual, sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web. (CONPES 3854, pág. 87).

CONCEPTOS ATENER EN CUENTA

Entorno digital abierto: En el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica. (CONPES 3854, pág. 87).

Establecimiento del contexto: Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo y establecimiento del alcance y los criterios del riesgo para la política para la gestión del riesgo. (NTC ISO 31000:2011).

Evaluación del control: Revisión sistemática de los procesos para garantizar que los controles son adecuados y eficaces. (NTC ISO 31000:2011).

Evaluación del riesgo: 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. (NTC ISO 31000:2011).

Evento de seguridad de la información: Ocurrencia que indica una posible brecha de seguridad de la información o falla de los controles. (ISO/IEC 27035:2016).

Evitar el riesgo: Decisión de no involucrarse o de retirarse de una situación de riesgo. (NTC ISO 31000:2011).

Evento: Presencia o cambio de un conjunto particular de circunstancias. (NTC ISO 31000:2011).

Fuente de riesgo: Elemento que solo o en combinación tiene el potencial intrínseco de originar un riesgo. (NTC ISO 31000:2011).

CONCEPTOS ATENER

EN CUENTA

Frecuencia: Medición del número de ocurrencias por unidad de tiempo. (NTC ISO 31000:2011).

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. (NTC ISO 31000:2011).

Gestión de riesgos de seguridad digital: Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego. (CONPES 3854, pág. 24).

ICC: Es la denominación de lo que el CCOC ha definido como infraestructuras críticas cibernéticas en el ámbito colombiano.

Identificación del riesgo: Proceso para encontrar, reconocer y describir el riesgo. (NTC ISO 31000:2011).

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).

Incidente de seguridad de la información: Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de información de la organización o comprometer sus operaciones. (ISO/IEC 27035:2016).

CONCEPTOS ATENER EN CUENTA

Infraestructura crítica cibernética nacional: Aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública. (CONPES 3854, pág. 29).

Inventario de activos: Sigla en inglés: *Assets inventory*. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos (ISO 27000.ES).

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización, cuyo objetivo es establecer, promocionar y gestionar estándares. (http://www.iso.org).
Marco de referencia para la gestión del riesgo: Conjunto de componentes que brindan las bases y las disposiciones de la organización para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión del riesgo, a través de toda la organización. (NTC ISO 31000:2011).

Monitoreo: Verificación, supervisión, observación crítica o determinación continúa del Estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado. (NTC ISO 31000:2011).

CONCEPTOS ATENER EN CUENTA

Múltiples partes interesadas: El Gobierno nacional y los territoriales, las organizaciones públicas y privadas, la fuerza pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil, quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales, y quienes pueden ejercer distintos roles y tener distintas responsabilidades. (CONPES 3854, pág. 29).

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad. (NTC ISO 31000:2011).

Organización: Grupo de personas e instalaciones con distribución de responsabilidades, autoridades y relaciones. (NTC ISO 31000:2011).

Parte involucrada: Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada, por una decisión o una actividad. (NTC ISO 31000:2011).

Peligro: Una fuente de daño potencial. (NTC ISO 31000:2011).

Pérdida: Cualquier consecuencia negativa o efecto adverso, financiero u otro. (NTC ISO 31000:2011).

Perfil del riesgo: Descripción de cualquier conjunto de riesgos. (NTC ISO 31000:2011).

CONCEPTOS A TENER EN CUENTA

Política: Intenciones y dirección de una organización como las expresa formalmente su alta dirección. (ISO/IEC 27000:2016).

Política para la gestión del riesgo: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. (NTC ISO 31000:2011).

Posibilidad: Se utiliza como descripción general de la probabilidad o la frecuencia. (NTC ISO 31000:2011).

Plan para la gestión del riesgo: Esquema dentro del marco de referencia para la gestión del riesgo que especifica el enfoque, los componentes y los recursos de la gestión que se van a aplicar a la gestión del riesgo. (NTC ISO 31000:2011).

Probabilidad: Oportunidad de que algo suceda. (NTC ISO 31000:2011).

Proceso para la gestión del riesgo: Aplicación sistemática de las políticas, los procedimientos y las prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, y de identificación, análisis, evaluación, tratamiento, monitoreo y revisión del riesgo. (NTC ISO 31000:2011).

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo. (ISO GUIA 73:2009).

Responsabilidad: Las múltiples partes interesadas deben asumir la responsabilidad de la gestión del riesgo de seguridad digital. Deben rendir cuentas sobre la base de sus funciones y su capacidad para actuar, teniendo en cuenta el posible impacto de sus decisiones sobre los demás. Deben también reconocer que un cierto nivel de riesgo de seguridad digital tiene que ser aceptado para

lograr los objetivos económicos y sociales. (CONPES 3854, pág. 25).

CONCEPTOS ATENER

EN CUENTA

Revisión: Acción que se emprende para determinar la idoneidad, conveniencia y eficacia de la materia en cuestión para lograr los objetivos establecidos. (NTC ISO 31000:2011).

Reducción del riesgo: Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo. (NTC ISO 31000:2011).

Resiliencia: Es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. (CONPES 3854, pág. 87).

Retención del riesgo: Aceptación del peso de la pérdida o del beneficio de la ganancia proveniente de un riesgo particular. (NTC ISO 31000:2011).

Riesgo: Efecto de la incertidumbre sobre los objetivos. (NTC ISO 31000:2011).

Riesgo inherente: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto. (NTC ISO 31000:2011).

Riesgo residual: Remanente después del tratamiento del riesgo. (NTC ISO 31000:2011).

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas. (ISO/IEC 27001:2016).

CONCEPTOS ATENER

EN CUENTA

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 (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) 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. (CONPES 3854, pág. 29).

Servicios esenciales: Los necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del Estado y las administraciones públicas (Tomado del documento ICC del CCOC).

SGC: Sistema de gestión de calidad.

SGSI: Sistema de gestión de seguridad de la información.

Sistema para la gestión del riesgo: Conjunto de elementos del sistema de gestión de una organización involucrados en la gestión del riesgo. (NTC ISO 31000:2011).

Telecomunicaciones: Toda transmisión y recepción de signos, señales, escritos, imágenes y sonidos, datos o información de cualquier naturaleza por hilo, radiofrecuencia, medios ópticos u otros sistemas electromagnéticos. (Resolución MinTIC 202 de 2010).

TI: Tecnologías de la información.

TO: Tecnología de operación.

TIC (Tecnologías de la información y las comunicaciones): Conjunto de recursos, herramientas, equipos, programas informáticos aplicaciones, redes y medios que permiten la compilación,

procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes. (Ley 1341/2009 TIC).

Tratamiento del riesgo: Proceso para modificar el riesgo. (ISO/IEC Guía 73:2009).

Valoración del riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo. (ISO GUÍA 73:2009).

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).

Información Publica Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley; Ley 1712/2014.

Información Publica Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley; Ley 1712/2014.

Información Pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. Ley 1712/2014 que ha sido declarada legalmente o por su propietario, de conocimiento público y accesible a cualquier persona. Ej. Rendición de cuentas presentada por la entidad, Plan de acción de la Entidad, datos abiertos, entre otros.

CONCEPTOS ATENER

EN CUENTA

Información Semi – Privada: Es aquella que por versar sobre información personal o impersonal y no estar comprendida por la regla general anterior, presenta para su acceso y conocimiento un grado mínimo de limitación, de tal forma que la misma sólo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales. Es el caso de los datos relativos a las relaciones con las entidades de la seguridad social o de los datos relativos al comportamiento financiero de las personas. Sentencia T-828/14 corte constitucional.

Información Privada: Es aquella que por versar sobre información personal o no, y que, por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Es el caso de los libros de los comerciantes, de los documentos privados, de las historias clínicas o de la información extraída a partir de la inspección del domicilio. Sentencia T-828/14 corte constitucional.

Conceptos tomados del Glosario del Modelo Nacional de Gestión de Riesgos de Seguridad Digital. Gobierno de Colombia y del Archivo General de la Nación.