ANEXO TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/07/2026	GTI02-MAN01	03	**1** de **20**

ANEXO TÉRMINOS Y DEFINICIONES

MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

JULIO DE 2026

ANEXO TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/07/2026	GTI02-MAN01	03	**2** de **20**

1. OBJETIVO

Estandarizar la terminología técnica aplicable al Sistema de Gestión de Seguridad de la Información (SGSI) mediante la recopilación y definición de conceptos clave sobre seguridad de la información, ciberseguridad y protección de datos. El marco de referencia conceptual integra las directrices del estándar ISO/IEC 27000:2022, los lineamientos institucionales del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y los requerimientos específicos de la organización para asegurar la claridad y el rigor en la gestión del riesgo.

Además, la Organización Internacional de Normalización (ISO, por su sigla en inglés) y la Comisión Electrotécnica Internacional (IEC, por su sigla en inglés) mantienen bases de datos terminológicas para su uso en la normalización en las siguientes páginas web:

- Plataforma de navegación en línea de ISO: https://www.iso.org/
- Electropedia IEC: https://www.electropedia.org/

2. Términos Y DEFINICIONES

2.1. Acción correctiva: remediación de los requisitos o acciones que dieron origen al establecimiento de una no conformidad, de tal forma que no se vuelva a presentar.

1.1 Acción preventiva: disposición de operaciones que buscan de forma preliminar que no se presente en su ejecución, desarrollo e implementación una no conformidad.

1.2 Aceptación del riesgo: decisión informada de asumir un riesgo particular.

1.3 Acuerdo de confidencialidad: contrato suscrito entre las partes con el fin de compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso público.

1.4 Activo de información: en relación con la seguridad de la información, se refiere a cualquier tipo de dato, archivo, documento o recurso digital

que tiene un valor para una organización y que debe ser protegido debido a su importancia para el funcionamiento o los objetivos de esta.

1.5 **Activo crítico:** son aquellos elementos o componentes que hacen parte de la infraestructura crítica.

1.6 **Archivo:** conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

1.7 **Adware:** aplicación que muestra publicidad a los usuarios y/o recolecta comportamiento del usuario en línea.

1.8 **Alcance de la auditoría:** extensión y límites de una auditoría.

1.9 **Alta dirección:** persona o grupo de personas que dirige y controla una organización al más alto nivel.

1.10 **Amenaza:** causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización.

1.11 **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.

1.12 **Análisis de riesgo:** proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

1.13 **Ataque:** intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.

ANEXO TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/07/2026	GTI02-MAN01	03	**4** de **20**

1.14 **Ataque informático:** conjunto de actividades realizadas por atacantes para vulnerar la seguridad informática de un sistema.

1.15 **Ataque cibernético:** acción organizada o premeditada de uno o más agentes para causar daño o problemas a un sistema a través del Ciberespacio. Este concepto se desarrolla de manera más profunda como ciberataque.

1.16 **Auditoría:** proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarla objetivamente para determinar en qué medida se cumplen los criterios de auditoría.

1.17 **Autenticación:** garantía de que una característica declarada de una entidad es correcta.

1.18 **Autenticidad:** propiedad de que una entidad es lo que dice ser.

1.19 **Autoridad:** es la facultad asignada por la alta dirección, para que un cargo pueda mandar sobre otros cargos y tomar decisiones con respecto a un área determinada o a los sistemas de gestión implementados.

1.20 **Batch (Instrucciones en lote):** archivo magnético que tiene almacenada una secuencia de comandos; el cual, al ejecutarse, reemplaza la operación de digitar los comandos de secuencia cada vez que se requiere efectuar una operación. Se utiliza para almacenar operaciones repetitivas.

1.21 **Bases de datos personales:** conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

1.22 **BCP** (Business Continuity Planning / Plan de Continuidad de Negocios): es un plan logístico detallado de cómo una entidad debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

ANEXO TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/07/2026	GTI02-MAN01	03	**5** de **20**

1.23 **BIA** significa **Business Impact Analysis**, en español: **Análisis de Impacto al Negocio**: es un análisis que permite identificar qué procesos, servicios, activos de información o actividades críticas podrían verse afectados ante una interrupción, incidente de seguridad, falla tecnológica, desastre o evento que afecte la operación normal de la entidad.

1.24 **Ciberamenaza:** se refiere a aquellas actividades "malignas" que tienen lugar en un entorno digital, para acceder o dañar un sistema de computadoras o redes.

1.25 **Ciberdefensa:** conjunto de lineamientos, procedimientos o estrategias preventivas o reactivas desarrolladas e implementadas para gestionar las transacciones del entorno digital.

1.26 **Ciberespacio:** ambiente complejo resultante de la interacción de personas, software y servicios en internet por medio de dispositivos tecnológicos y redes conectadas a internet, por lo cual no existe en forma física alguna.

1.27 **Ciberseguridad:** se refiere a las actividades y medidas necesarias para proteger los activos de información, como la información procesada, almacenada y transportada por los sistemas de información interconectados, los usuarios involucrados y otros afectados por las ciberamenazas.

1.28 **Ciberespionaje:** "*el Ciberespionaje se utiliza principalmente como un medio para recopilar datos sensibles o clasificados, secretos comerciales u otras formas de propiedad intelectual que pueden ser utilizados por el agresor para crear una ventaja competitiva o vendidos para obtener beneficios financieros. En algunos casos, la violación simplemente pretende causar un daño reputacional a la víctima exponiendo información privada o prácticas empresariales cuestionables*." - Crowdstrike.

ANEXO TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/07/2026	GTI02-MAN01	03	**6** de **20**

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

1.30 **CISO (Chief Information Security Officer):** profesional líder delegado por la alta dirección que establece, implementa, mantiene y mejora continuamente los procesos del Sistema de Gestión de Seguridad de la Información (SGSI), asesora en materia de seguridad de la información a la Contaduría General de la Nación y supervisa el cumplimiento de la presente política.

1.31 **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.

1.32 **ColCERT:** Grupo de Respuesta a Emergencias Cibernéticas de Colombia.

1.33 **Control:** 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. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

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

1.35 **Código malicioso**: conjunto de instrucciones o códigos informáticos que se inserta en los programas de computador, tiene la capacidad de auto replicarse y usualmente porta una carga útil que afecta el funcionamiento del computador, destruye datos, altera y pone en riesgo la información.

1.36 **Competencia:** capacidad de aplicar conocimientos y habilidades para lograr los resultados previstos.

ANEXO TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/07/2026	GTI02-MAN01	03	**7** de **20**

1.37 **Comunicación y consulta de riesgos:** conjunto de procesos continuos e iterativos que lleva a cabo una organización para proporcionar, compartir u obtener información, y para entablar un diálogo con las partes interesadas en relación con la gestión de riesgos.

1.38 **Comunidad de intercambio de información:** grupo de organizaciones que acuerdan compartir información.

1.39 **Confiabilidad:** propiedad de comportamiento y resultados consistentes previstos.

1.40 **Confidencialidad:** propiedad de que la información no se pone a disposición ni se divulga a personas, entidades o procesos no autorizados.

1.41 **Conformidad:** cumplimiento de un requisito.

1.42 **Consecuencia:** resultado de un evento que afecta los objetivos.

1.43 **Contexto externo:** entorno externo en el que la organización busca lograr sus objetivos.

1.44 **Contexto interno:** ambiente interno en el que la organización busca alcanzar sus objetivos.

1.45 **Control:** medida que está modificando el riesgo.

1.46 **Control de acceso:** medios para garantizar que el acceso a los activos esté autorizado y restringido en función de los requisitos comerciales y de seguridad.

1.47 **Cookie:** datos intercambiados entre un servidor HTTP y un navegador para almacenar información de estado en el lado del cliente y recuperarlo posteriormente para uso en el servidor.

1.48 **Corrección:** acción para eliminar una no-conformidad detectada.

ANEXO TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/07/2026	GTI02-MAN01	03	**8** de **20**

1.49 **Criterios de riesgo:** términos de referencia contra los cuales se evalúa la importancia del riesgo.

1.50 **CSIRT Gobierno:** Equipo de Respuesta a Incidentes de Seguridad en sus siglas en inglés (Computer Security Incident & Response Team), integrado por un grupo de personas técnicas especializadas, que implementan y desarrollan medidas tendientes a prevenir y gestionar incidentes de ciberseguridad de las entidades del estado.

1.51 **CSIRT-Ponal:** CSIRT es la sigla en inglés de Computer Security Incident Response Team (equipo de Respuesta ante Incidencias de Seguridad Informáticas). Es un equipo de respuesta ante emergencias informáticas o un centro de respuesta a incidentes de seguridad en tecnologías de la información de la Policía Nacional.

1.52 **Datos personales**: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

1.53 **Datos personales públicos:** es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

1.54 **Datos personales sensibles:** se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3, numeral 3)

ANEXO TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/07/2026	GTI02-MAN01	03	**9** de **20**

1.55 **Defacement:** ataque sobre un servidor web como consecuencia del cual se cambia su apariencia.

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

1.57 **DoS** / DDoS (Denial of Service / Distributed Denial of Service): se entiende como denegación de servicio, en términos de seguridad digital, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma no permitir que sus legítimos usuarios puedan utilizar los servicios prestados por él. El ataque consiste en saturar con peticiones de servicio al servidor, hasta que éste no puede atenderlas, provocando su colapso.

1.58 **DRP** (Disaster Recovery Plan / Plan de Recuperación ante Desastres): es un documento formal creado por una organización que contiene instrucciones detalladas con la definición de los procedimientos, estrategias, y roles y responsabilidades establecidos para recuperar y mantener el servicio de tecnología ante un evento de interrupción.

1.59 **Gestión de incidentes de seguridad de la información:** procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27001:2022).

1.60 **Gobernanza de la seguridad digital para Colombia:** corresponde al conjunto de interacciones y enfoques entre las múltiples partes interesadas para identificar, enmarcar, proponer, y coordinar respuestas proactivas y reactivas a posibles amenazas a la confidencialidad, integridad o disponibilidad de los servicios tecnológicos, sistemas de información, infraestructura tecnológica, redes e información que en conjunto constituyen el entorno digital

1.61 **Disponibilidad:** propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada.

ANEXO TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/07/2026	GTI02-MAN01	03	**10** de **20**

1.62 **Encriptación (cifrado, codificación):** la encriptación es el proceso para volver ilegible información considerada importante. La información una vez encriptada solo puede leerse aplicándole una clave. Se trata de una medida de seguridad que es usada para almacenar o transferir información sensible que no debería ser accesible a terceros.

1.63 **Eficacia:** medida en que se realizan las actividades planificadas y se logran los resultados planificados.

1.64 **Evaluación de riesgos:** proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.

1.65 **Evento:** ocurrencia o cambio de un conjunto particular de circunstancias.

1.66 **Evento de seguridad de la información:** ocurrencia identificada de un sistema, servicio o estado de la red que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

1.67 **Firewall (Cortafuego):** dispositivo tecnológico que tiene como función proteger la red interna de una compañía de accesos no autorizados del exterior vía internet.

1.68 **Gestión de incidentes de seguridad de la información:** conjunto de procesos para detectar, informar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

1.69 **Gestión de riesgos:** actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

1.70 **GIT:** sigla de Grupo Interno de Trabajo en la Contaduría General de la Nación.

1.71 **Gobernanza de la seguridad de la información:** corresponde al conjunto de interacciones y enfoques entre las múltiples partes

interesadas para identificar, enmarcar, proponer y coordinar respuestas proactivas y reactivas a posibles amenazas a la confidencialidad, integridad o disponibilidad de los servicios tecnológicos, sistemas de información, infraestructura tecnológica, redes e información que en conjunto constituyen el entorno digital.

1.72 **Identificación de riesgos:** proceso de encontrar, reconocer y describir riesgos.

1.73 **Impacto:** el costo para la entidad de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros, por ejemplo: pérdida de reputación, implicaciones legales, etc.

1.74 **Incidente de seguridad de la información:** evento único o serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.

1.75 **Indicador:** medida que proporciona una estimación o evaluación.

1.76 **Información pública:** es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. (Literal b, artículo. 6 de la Ley 1712 de 2014)

1.77 **Información pública 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*". (Literal c, artículo. 6 de la Ley 1712 de 2014)

1.78 **Información pública 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 la Ley 1712 de 2014*". (Ley 1712 de 2014, art 6).

ANEXO TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/07/2026	GTI02-MAN01	03	**12** de **20**

1.79 **Ingeniería social**: son técnicas basadas en engaños que se emplean para dirigir la conducta de una persona u obtener información sensible. El afectado es inducido a actuar de determinada forma (pulsar en enlaces, introducir contraseñas, visitar páginas, etc.) convencido de que está haciendo lo correcto cuando realmente está siendo engañado por el ingeniero social.

1.80 **Información documentada:** información requerida para ser controlada y mantenida por una organización y el medio en el que está contenida.

1.81 **Incidente de seguridad digital - Ciberincidente:** ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable.

1.82 **Infraestructura crítica cibernética (ICC)**: sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía.

1.83 **Internet:** sistema global de redes interconectadas en el dominio público.

1.84 **Instalaciones de procesamiento de información:** cualquier sistema, servicio o infraestructura de procesamiento de información, o la ubicación física que lo alberga.

1.85 **Integridad:** propiedad de exactitud y completitud de la información. Este principio de seguridad de la información asegura que la información se mantenga íntegra; es decir, que no haya sido alterada, manipulada o dañada de manera intencionada o accidental, y que permanezca exacta y fiable a lo largo del tiempo y en su transmisión o almacenamiento.

ANEXO TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/07/2026	GTI02-MAN01	03	**13** de **20**

1.86 **Impacto:** el costo para la entidad de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros, por ejemplo: pérdida de reputación, implicaciones legales, etc.

1.87 **Malware (software malicioso):** software diseñado con intención malicioso e incluye características o capacidades que potencialmente pueden causar daño, directa o indirectamente, al usuario o al sistema del equipo de cómputo del usuario.

1.88 **Medición:** proceso para determinar un valor.

1.89 **Medio removible y extraíble:** todo dispositivo de almacenamiento de información que sea extraíble de su fuente de información o todo lo que permita almacenar y transportar información.

1.90 **Mejora continua:** actividad recurrente para mejorar el desempeño.

1.91 **Método de medición:** secuencia lógica de operaciones, descritas genéricamente, utilizadas para cuantificar un atributo con respecto a una escala específica.

1.92 **Módem:** dispositivo de comunicación que permite establecer una conexión a través de la línea telefónica.

1.93 **Modelo de gobernanza de seguridad digital**: es el esquema de trabajo compuesto por un conjunto de políticas de operación, principios, normas, reglas, procedimientos de toma de decisiones y programas compartidos por las múltiples partes interesadas de la seguridad digital del país, con el fin de fortalecer las capacidades para la gestión de riesgos e incidentes de seguridad digital y para la respuesta proactiva y reactiva a posibles amenazas a la confidencialidad, integridad o disponibilidad de los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes e información que, en conjunto, constituyen el entorno digital en el país. (Decreto 338-2022).

1.94 **MSPI:** el Modelo de Seguridad y Privacidad de la Información imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares

internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad.

1.95 **Nivel de riesgo:** magnitud de un riesgo expresada en términos de la combinación de consecuencias y su probabilidad.

1.96 **No conformidad:** incumplimiento de un requisito.

1.97 **No repudio:** capacidad de probar la ocurrencia de un evento o acción alegado y sus entidades de origen.

1.98 **Objetivo de control:** declaración que describe lo que se logrará como resultado de la implementación de controles.

1.99 **Objetivo:** resultado a lograr.

1.100 **Oficial de Seguridad de la Información:** ver numeral 2.21 CISO de este manual.

1.101 **Organización:** persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos.

1.102 **Parte interesada (término preferido), Stakeholder (término admitido):** persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad.

1.103 **Password:** palabra en inglés que significa contraseña, clave o llave. Es la forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso o servicio tecnológico.

1.104 **Plan de respuesta a ciberincidentes:** conjunto predeterminado y ordenado de instrucciones o procedimientos para detectar, analizar, contener, erradicar y recuperar para minimizar las consecuencias de un ciberincidente.

1.105 **Plan de tratamiento de riesgos**: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e

implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

1.106 Phishing (suplantación de identidad): proceso fraudulento de intentar adquirir información privada o confidencial al presentarse como la organización de confianza en comunicaciones electrónicas.

1.107 Política: intenciones y dirección de una organización, expresadas formalmente por su alta dirección.

1.108 Probabilidad: posibilidad de que algo suceda.

1.109 Problema: es la causa de uno o más incidentes, aun cuando la causa no se conoce normalmente en el momento, se crea un registro de problema.

1.110 Proceso de gestión de riesgos: aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, contextualización e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo.

1.111 Proceso: conjunto de actividades interrelacionadas o que interactúan, las cuales transforman entradas en salidas.

1.112 Procedimiento: manera especificada de llevar a cabo una actividad o un proceso.

1.113 Propietario del riesgo: persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

1.114 RDP: sigla en inglés de Remote Desktop Protocol (Protocolo de Escritorio Remoto). El protocolo RDP, entonces, permite que el escritorio de un equipo informático sea controlado a distancia por un usuario remoto.

1.115 Red Privada Virtual (VPN): metodología de conexión vía internet que permite a los usuarios conectarse a la red institucional utilizando conexiones públicas, a través de canales seguros de comunicación.

ANEXO TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/07/2026	GTI02-MAN01	03	**16** de **20**

1.116 Rendimiento: resultado medible.

1.117 Requisito: necesidad o expectativa declarada, generalmente implícita u obligatoria.

1.118 Responsabilidad: obligaciones por las que debe responder el colaborador según el cargo que desempeña.

1.119 Revisión: actividad realizada para determinar la idoneidad, adecuación y eficacia del tema en cuestión para lograr los objetivos establecidos.

1.120 Riesgo: efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

1.121 Riesgo de seguridad de la información: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

1.122 Riesgo residual: riesgo remanente después del tratamiento del riesgo.

1.123 Rol: es un conjunto de permisos que pueden asignarse a un usuario que se registra en un sistema.

1.124 Scam (estafa): fraude o truco frente a la confianza.

1.125 Scanner (Scanning): Escáner de vulnerabilidades, programa que analiza un sistema buscando vulnerabilidades. Utiliza una base de datos de defectos conocidos y determina si el sistema bajo examen es vulnerable o no.

1.126 Spam (correo basura): correo electrónico no deseado que se envía aleatoriamente en procesos por lotes. Es extremadamente eficiente y barata forma de comercializar cualquier producto. La mayoría de los usuarios que están expuestos a este correo basura que se confirma en encuestas que muestran que más del 50% de todos los e-mails son correos basura. No es una amenaza directa, pero la cantidad de e-mails generados y el tiempo que lleva a las entidades públicas, empresas y

particulares relacionarlo y eliminarlo, representa un elemento molesto para los usuarios de Internet.

1.127 Spear Phising: Phishing dirigido de forma que se maximiza la probabilidad de que el sujeto objeto del ataque pique el anzuelo (suelen basarse en un trabajo previo de ingeniera social sobre la victima).

1.128 Spyware "spy software": tipo de software malicioso que al instalarse intercepta o toma control parcial de la computadora del usuario sin el consentimiento de este último.

1.129 Suplantación (Spoofing): técnica basada en la creación de tramas TCP/IP utilizando una dirección IP falseada; desde su equipo, un atacante simula la 18 identidad de otra máquina de la red (que previamente ha obtenido por diversos métodos) para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del anfitrión suplantado

1.130 Script: archivo que contiene una secuencia de comandos que se utiliza para comunicarse en forma automática entre dos aplicaciones.

1.131 Seguimiento: determina el estado de un sistema, un proceso o una actividad.

1.132 Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información.

1.133 Seguridad digital: preservación de la confidencialidad, integridad y disponibilidad de la información que se encuentra en medios digitales.

1.134 Seguridad informática: conjunto de tecnologías, procesos y prácticas diseñadas para la protección de redes, dispositivos, programas y datos en caso de algún ciberataque, daño o acceso no autorizado.

1.135 SGSI: sigla de Sistema de Gestión de Seguridad de la Información.

ANEXO TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/07/2026	GTI02-MAN01	03	**18** de **20**

1.136 Sistema de gestión: conjunto de elementos interrelacionados o que interactúan entre sí de una organización para establecer políticas, objetivos y procesos para lograr esos objetivos.

1.137 Servicio crítico: conjunto de actividades que la organización realiza, al generar un producto o en la prestación de un servicio fundamental para la organización o sector del país, que al interrumpirse afectaría su operación.

1.138 Sistema de información: conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información.

1.139 Spam (mensajería no deseada): abuso de sistemas de mensajería electrónica para enviar de forma no discriminada mensajes no solicitados.

1.140 Subcontratar (tercerizar): hacer un arreglo donde una organización externa realiza parte de la función o proceso de una organización.

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

1.142 Ransomware: código malicioso para secuestrar datos, una forma de explotación en la cual el atacante, cifra los datos de la víctima y exige un pago por la clave de descifrado; se propaga a través de archivos adjuntos de correo electrónico, programas infectados y sitios web comprometidos, secuestrando computadores y servidores (imposibilidad de usarlo) o cifrando los archivos, con la promesa de liberarlo tras el pago de una cantidad de dinero por el rescate.

1.143 Registro Nacional de Bases de Datos (RNBD): directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

ANEXO TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/07/2026	GTI02-MAN01	03	**19** de **20**

1.144 Responsabilidad Demostrada: conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

1.145 Responsable del Tratamiento de Datos: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).

1.146 Plan de tratamiento de riesgos: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

1.147 Teletrabajo: es el término bajo el cual se conoce el esquema acordado formalmente entre un empleado y su empleador para trabajar en un lugar diferente a la oficina. El aprovechamiento de las ventajas de las TICs permite lograr la realización de actividades en forma no presencial, trayendo consigo la ventaja de evitar pérdidas de tiempo en desplazamiento y poder trabajar desde la comodidad de su lugar de vivienda.

1.148 TIC: sigla de Tecnologías de la Información y las Comunicaciones.

1.149 Titulares de la información: personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

1.150 Token (vale digital): es una herramienta digital o física que genera una clave irremplazable de forma aleatoria y temporal. El token se utiliza como complemento o en lugar de una contraseña.

1.151 Tercero: cualquier persona natural o jurídica en calidad de proveedor, *outsourcing* o consultor.

ANEXO TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/07/2026	GTI02-MAN01	03	**20** de **20**

1.152 Tratamiento del riesgo: proceso para modificar el riesgo.

1.153 Troyano: programa que aparentemente, o realmente, ejecuta una función útil, pero oculta un subprograma dañino que abusa de los privilegios concedidos para la ejecución del citado programa.

1.154 Virus informático / malware / software malicioso: Programa informático que está diseñado para realizar acciones maliciosas sobre un activo informático como copiarse a sí mismo, cifrar información, recolectar y filtrar información, entre otros, sin el consentimiento del propietario

1.155 Vulnerabilidad: debilidad de un activo o control que puede ser explotado por una o más amenazas.