| TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL | | | |
|---|---|---|---|
| **PROCESO:** | GESTIÓN TICS | | |
| **PROCEDIMIENTO:** | POLÍTICA GENERAL DE GOBIERNO DIGITAL | | |
| **FECHA DE APROBACIÓN:** | **CÓDIGO:** | **VERSIÓN:** | **PÁGINA:** |
| 15/11/2024 | GTI02-MAN02 | 01 | **1** de **12** |

# TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

**NOVIEMBRE DE 2024**

| TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL | | | |
|---|---|---|---|
| **PROCESO:** | GESTIÓN TICS | | |
| **PROCEDIMIENTO:** | POLÍTICA GENERAL DE GOBIERNO DIGITAL | | |
| **FECHA DE APROBACIÓN:** | **CÓDIGO:** | **VERSIÓN:** | **PÁGINA:** |
| 15/11/2024 | GTI02-MAN02 | 01 | **2** de **12** |

## 1. OBJETIVO

El presente documento reúne los términos referentes a seguridad de la información, protección de datos personales y seguridad digital más comúnmente utilizados. Toma como base el estándar internacional de vocabulario ISO/IEC 27000, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones e incluye cualquier otra definición requerida por el Sistema de Gestión de Seguridad de la Información, en adelante SGSI.

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. DEFINICIONES

**1.1** **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.

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

**1.3** **Aceptación del riesgo:** decisión informada de asumir un riesgo particular.

**1.4** **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.

**1.5** **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.

| TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL | | | |
|---|---|---|---|
| **PROCESO:** | GESTIÓN TICS | | |
| **PROCEDIMIENTO:** | POLÍTICA GENERAL DE GOBIERNO DIGITAL | | |
| **FECHA DE APROBACIÓN:** | **CÓDIGO:** | **VERSIÓN:** | **PÁGINA:** |
| 15/11/2024 | GTI02-MAN02 | 01 | **3** de **12** |

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

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

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

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

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

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

**1.12** **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.

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

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

**1.15** **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.

**1.16** **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.

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

**1.18** **Ciberdefensa:** conjunto de lineamientos, procedimientos o estrategias

preventivas o reactivas desarrolladas e implementadas para gestionar las transacciones del entorno digital.

**1.19** **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.

**1.20** **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.

**1.21** **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.

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

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

**1.24** **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.

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

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

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

| TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL | | | |
|---|---|---|---|
| **PROCESO:** | GESTIÓN TICS | | |
| **PROCEDIMIENTO:** | POLÍTICA GENERAL DE GOBIERNO DIGITAL | | |
| **FECHA DE APROBACIÓN:** | **CÓDIGO:** | **VERSIÓN:** | **PÁGINA:** |
| 15/11/2024 | GTI02-MAN02 | 01 | **5** de **12** |

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

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

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

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

**1.32** **Continuidad de la seguridad de la información:** procesos y procedimientos para garantizar operaciones continuas de seguridad de la información.

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

**1.34** **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.

**1.35** **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.

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

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

**1.38** **CSIRT-Gobierno:** 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 del gobierno.

**1.39** **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.

| TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL | | | |
|---|---|---|---|
| **PROCESO:** | GESTIÓN TICS | | |
| **PROCEDIMIENTO:** | POLÍTICA GENERAL DE GOBIERNO DIGITAL | | |
| **FECHA DE APROBACIÓN:** | **CÓDIGO:** | **VERSIÓN:** | **PÁGINA:** |
| 15/11/2024 | GTI02-MAN02 | 01 | **6** de **12** |

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

**1.41** **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.

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

**1.43** **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.

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

**1.45** **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.

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

**1.47** **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.

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

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

**1.50** **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.

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

**1.52** **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.

**1.53** **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.

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

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

**1.56** **Infraestructura Crítica Cibernética:** 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.

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

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

**1.59** **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.

| TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL | | | |
|---|---|---|---|
| **PROCESO:** | GESTIÓN TICS | | |
| **PROCEDIMIENTO:** | POLÍTICA GENERAL DE GOBIERNO DIGITAL | | |
| **FECHA DE APROBACIÓN:** | **CÓDIGO:** | **VERSIÓN:** | **PÁGINA:** |
| 15/11/2024 | GTI02-MAN02 | 01 | **8** de **12** |

**1.60** **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.

**1.61** **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.

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

**1.63** **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.

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

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

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

**1.67** **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.

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

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

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

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

| TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL | | | |
|---|---|---|---|
| **PROCESO:** | GESTIÓN TICS | | |
| **PROCEDIMIENTO:** | POLÍTICA GENERAL DE GOBIERNO DIGITAL | | |
| **FECHA DE APROBACIÓN:** | **CÓDIGO:** | **VERSIÓN:** | **PÁGINA:** |
| 15/11/2024 | GTI02-MAN02 | 01 | **9** de **12** |

**1.72** **Objetivo:** resultado a lograr.

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

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

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

**1.76** **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.

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

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

**1.79** **Probabilidad:** posibilidad de que algo suceda.

**1.80** **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.

**1.81** **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.

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

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

| TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL | | | |
|---|---|---|---|
| **PROCESO:** | GESTIÓN TICS | | |
| **PROCEDIMIENTO:** | POLÍTICA GENERAL DE GOBIERNO DIGITAL | | |
| **FECHA DE APROBACIÓN:** | **CÓDIGO:** | **VERSIÓN:** | **PÁGINA:** |
| 15/11/2024 | GTI02-MAN02 | 01 | **10** de **12** |

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

**1.85** **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.

**1.86** **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.

**1.87** **Rendimiento:** resultado medible.

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

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

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

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

**1.92** **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.

**1.93** **Riesgo residual:** riesgo remanente después del tratamiento del riesgo.

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

**1.95** **Scam (estafa):** Fraude o truco frente a la confianza.

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

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

| TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL | | | |
|---|---|---|---|
| **PROCESO:** | GESTIÓN TICS | | |
| **PROCEDIMIENTO:** | POLÍTICA GENERAL DE GOBIERNO DIGITAL | | |
| **FECHA DE APROBACIÓN:** | **CÓDIGO:** | **VERSIÓN:** | **PÁGINA:** |
| 15/11/2024 | GTI02-MAN02 | 01 | **11** de **12** |

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

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

**1.100 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.

**1.101 SGSI:** sigla de Sistema de Gestión de Seguridad de la Información.

**1.102 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.

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

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

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

**1.106 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.

**1.107 TIC:** sigla de Tecnologías de la Información y las Comunicaciones.

**1.108 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.

| TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL | | | |
|---|---|---|---|
| **PROCESO:** | GESTIÓN TICS | | |
| **PROCEDIMIENTO:** | POLÍTICA GENERAL DE GOBIERNO DIGITAL | | |
| **FECHA DE APROBACIÓN:** | **CÓDIGO:** | **VERSIÓN:** | **PÁGINA:** |
| 15/11/2024 | GTI02-MAN02 | 01 | **12** de **12** |

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

**1.110 Tratamiento del riesgo:** proceso para modificar el riesgo.

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

| | |
|---|---|
| **Revisado por:** Jamir Mosquera Rubio | **Aprobado por:** Vilma Narváez Narváez |
| **LÍDER DEL PROCESO DE GESTIÓN TICs** | **REPRESENTANTE DE LA DIRECCIÓN LÍDER DELPROCESO DE PLANEACIÓN INTEGRAL** |