GOBIERNO DE LA
REPÚBLICA DOMINICANA

CONTRALORÍA

CONTRALORIA GENERAL DE LA REPÚBLICA

NORMAS BASICAS DE CONTROL INTERNO ESPECÍFICA DE SEGUNDO GRADO

NOBACI 3 – ACTIVIDADES DE CONTROL

"Gestión de la Tecnología de la Información y Comunicación en las Entidades Públicas"

ADC-3-009

(VERSION 1 – JUNIO 2024)

Santo Domingo – 2024

INDICE

ACRÓNIMOS:

- **CGR:** Contraloría General de la República.
- **NOBACI:** Normas Básicas de Control Interno.
- **TIC**: Tecnología de la información y Comunicación.
- **MAP**: Ministerio de Administración Pública.
- **OPTIC:** Oficina Presidencial de Tecnología de la Información y Comunicación.
- **OGTIC:** Oficina Gubernamental para la Tecnología de la Información y la Comunicación.
- **NORTIC**: Norma Tecnología de la Información y Comunicación.
- **NIU**: Número de Identificación Único.
- **CIEN**: Comité Interno para la Evaluación de las Normas. Está conformado por expertos en TIC dentro de la OPTIC/OGTIC.
- **COETIC**: Comité de Estándares de Tecnologías de la Información y Comunicación.
- **IVR**: Sistema de Respuesta de Voz Interactiva.
- **ISO**: Organización encargada de la creación de normas y estándares internacionales en diferentes áreas como tecnologías, seguridad, servicios, entre otros.
- **SASI**: Sistema para la Administración de la Seguridad de la Información.
- **CONTI:** Comité de Continuidad.
- **OAI:** Oficina de Libre Acceso a la Información.
- **URI (por sus siglas en inglés):** Identificador Uniforme de Recursos. Es una dirección exacta y precisa que permite ubicar un recurso en internet o en una red de cómputo.
- **SIAFE:** Sistema Integrado de Administración Financiera del Estado.
- **SIGEF:** Sistema Integrado de Gestión Financiera.
- **SINACI:** Sistema Nacional de Control Interno.
- **UAI:** Unidad de Auditoría Interna.
- **DIGECOG:** Dirección General de Contabilidad Gubernamental.
- **DIGEPRES:** Dirección General de Presupuesto.

- **MEPyD:** Ministerio de Economía, Planificación y Desarrollo.
- **DAF:** Dirección Administrativa y Financiera.
- **iTICge:** Institucionalizado en el Estado Dominicano como la herramienta oficial de medición de avances, implementaciones y mejoras de los sectores TIC y de gobierno electrónico público de la República Dominicana.
- **SMMGP:** Sistema de Monitoreo y Medición de la Gestión Pública de la Presidencia de la República.
- **COBIT:** (Control Objectives for Information and Related Technologies) por sus siglas en inglés. Objetivos de Control para las Tecnologías de la Información y Relacionadas.
- **ISACA:** (*Information Systems Audit and Control Association) por sus siglas en inglés.* Asociación de Auditoría y Control de Sistemas de Información.

INTRODUCCION

El artículo 22 de la Ley 10-07 define el control interno como un proceso en el cual intervienen en distintos roles las diferentes instituciones que entran en el ámbito de aplicación de las disposiciones que crean el Sistema Nacional de Control Interno (SINACI) de la República Dominicana. La responsabilidad principal de la gestión del mismo corresponde a la dirección superior y a los servidores públicos de cada entidad u organismo y de manera especial la Contraloría General de la República que es el responsable de la fiscalización y evaluación del debido recaudo, uso e inversión de los recursos públicos, como lo establece el artículo 247 de la Constitución de la República y el artículo 11 de la citada Ley 10-07.

Igualmente, la Constitución de la República designa como órgano rector del control interno a la Contraloría General de la República y lo hace también responsable de emitir las normas básicas de control interno de primer y segundo grado, las cuales deben servir como requisitos mínimos para que las entidades públicas que están bajo el ámbito de aplicación de esta ley desarrollen las normas, políticas, procedimientos y controles específicos que mejor se adapten a sus fines y proyectos y al cumplimiento de sus objetivos institucionales.

El artículo 47 del Reglamento 491-07 de Aplicación de la Ley 10-07, en su numeral 3, que se refiere al componente actividades de control, establece de manera específica en su literal d, que se debe diseñar actividades orientadas al control interno de la información en las entidades sujetas al ámbito de aplicación de la ley; de igual manera en el numeral 4, del artículo de referencia del mismo reglamento de la Ley 10-07, en los literales a, b, c, d, y e, que se refieren al componente información y comunicación, se establece la obligación de las entidades de diseñar políticas y procedimientos orientados a la calidad de la información que generan los sistemas, para lo cual se hace imprescindible incorporar la tecnología más avanzada que permita apoyar el logro de los objetivos de las entidades públicas.

Asimismo, el Reglamento 491-07, Art.8, numeral 1, establece la obligación de que el sistema de control interno se desarrolle sobre "base técnica uniforme", de manera que todas las entidades puedan acogerse sin dificultad a las disposiciones contenidas en las normas emitidas por la Contraloría General de la República de acuerdo a las atribuciones establecidas en la ley.

En ese sentido, el órgano rector del SINACI debe emitir las normas de primer y de segundo grado, así como mantenerlas actualizadas de manera tal que las entidades puedan adaptar su sistema de control a las necesidades y cambios que requieran en sus diferentes procesos. Las normas básicas de primer grado son normas fundamentales del proceso de control interno y las de segundo grado son normas básicas generales, que desarrollan los elementos de las normas básicas fundamentales.

En ese sentido, es importante destacar el rol fundamental de la tecnología aplicada a los distintos procesos del control interno institucional. Hoy por hoy es imposible diseñar un proceso de gestión apoyado en los principios de eficiencia, efectividad, economía, transparencia, confiabilidad, legalidad, entre otros principios, sin el apoyo de las Tecnología de la Información y Comunicación (TIC) para su consecución.

El Estado Dominicano ha formulado una serie de políticas y estrategias, orientadas al desarrollo y uso de tecnología de información y comunicación en los diferentes procesos de la gestión pública, las cuales están contenidas primeramente en varios decretos, con el propósito de crear la estructura que se encargue de la rectoría para la emisión de las normativas relacionadas con las TIC en las instituciones públicas, para lo cual se creó a través del Decreto No.1090-04, la Oficina Presidencial de Tecnología de la Información y Comunicación, hoy denominada como Oficina Gubernamental de Tecnología de la Información y Comunicación, dependencia del Ministerio de Administración Pública.

En el referido decreto se establecen las atribuciones de la OGTIC, entre las cuales está la de ser órgano rector y la de emitir las normas a través de las cuales las entidades públicas deben estructurar sus áreas de tecnología de información y comunicación. Estas normas,

según establece el decreto en cuestión, deben estar apoyadas en estándares internacionales y las mejores prácticas aplicadas en la materia.

Visto lo anterior y con el propósito de orientar el trabajo de los evaluadores y auditores de la Contraloría General de la República, así como las labores de autoevaluación y autocontrol que deben realizar las propias entidades sujetas al ámbito de aplicación de la Ley 10-07 y del decreto mencionado más arriba, se emite la presente norma específica de segundo grado sobre las TIC, las cuales, de una manera resumida procuran unificar los criterios relacionados con las directrices contenidas en las normas de tecnología de información y comunicación emitidas por la OGTIC y como medida de fortalecimiento del control interno de las entidades públicas.

Las Normas de Tecnología de Información y Comunicación (NORTIC) fueron concebidas para sistematizar, estandarizar y tener una herramienta efectiva de auditoría para el correcto uso e implementación de las TIC en la administración pública, con el objetivo de crear ciclos de mejora continua en los procesos de los organismos gubernamentales y contribuir a la eficiencia en el logro de sus objetivos.

MARCO JURÍDICO

LEYES, DECRETOS, NORMAS, REGLAMENTOS Y RESOLUCIONES	FECHA	DESCRIPCION
Constitución	26 de enero del 2010	Constitución Política de la República Dominicana.
Ley 10-07	08 de enero de 2007	Que instituye el Sistema Nacional de Control Interno y de la Contraloría General de la República.
Reglamento 491-07	30 de agosto del 2007	Que instituye el Sistema Nacional de Control Interno y de la Contraloría General de la República.
Ley 153-98	27 de mayo del 1998	Ley General de las Telecomunicaciones
Ley 107-13	08 agosto del 2013	Ley que regula los deberes y derechos de la Administración Pública con las personas.
Ley No. 310-14	11 de junio del 2014	Ley que regula el envío de Correos Electrónicos
Ley No. 53-07	10 de abril del 2007	Crímenes y Delitos de Alta Tecnología
Decreto 1090-04	3 septiembre del 2004	Crea la Oficina Presidencial de Tecnologías de la información y Comunicación (OPTIC)
Decreto 54-21	2 de febrero del 2021	Cambio de nombre a la OPTIC ahora OGTIC y traspaso al MAP
Decreto 229-18	19 de junio del 2018	Crea el Programa de Simplificación de Trámite (PST).

NORTIC A1:2014	15 de mayo del 2014	Norma General sobre el Uso e Implementación de las Tecnologías de la Información y Comunicación en el Estado Dominicano
NORTIC A2:2021	Marzo 2021	Norma Para el Desarrollo y Gestión De Los Portales Web y La Transparencia de Los Organismos del Estado Dominicano.
NORTIC A2:2023	Marzo 2023	Norma Para el Desarrollo y Gestión de los Portales Web y la Transparencia de los Organismos del Estado Dominicano
NORTIC E1:2022	Abril 2022	Norma para la Gestión de las Redes Sociales en los Organismos Gubernamentales
NORTIC A8:2019	Enero 2019	Norma para la Gestión de los Residuos de los Aparatos Eléctricos y Electrónicos (RAEE) en los Organismos del Estado Dominicano.
NORTIC A4:2022	Diciembre 2022	Norma para la Interoperabilidad entre Los Organismos del Estado Dominicano
Resolución MAP Núm. 51-2013	Diciembre 2013	Que aprueba los Modelos de Estructura Organizativa de las Unidades de Tecnologías de la Información y Comunicación
Declaración Técnica No.002-19	17 de mayo del 2019	Principios en los que se sustenta el Sistema Nacional de Control Interno y el proceso de Control Interno.

CAPITULO I.

1.1 Objetivo

La presente norma de segundo grado procura aportar un marco referencial que sirva de elemento, en primer lugar, para armonizar las normas emitidas por la Oficina Gubernamental de Tecnología de la Información y Comunicación (OGTIC), con los requerimientos establecidos en los numerales 3 y 4 del artículo 47 del Reglamento 491-07 de aplicación de la Ley 10-07, de manera que le sirva como herramienta que le permita diseñar y evaluar los procesos asociados a la generación de información y comunicación de calidad, así como los medios tecnológicos más apropiados para asegurar el logro de los objetivos planteados más arriba.

En segundo lugar, esta herramienta facilita a las entidades las fases de identificación y evaluación de los riesgos, así como controles claves que pueden ser considerados para mitigarlos, en el marco del desarrollo de sus normas secundarias de control interno y en su rol normativo contenido en las leyes especiales, normas, políticas y procedimientos que rigen las áreas de tecnología en las diferentes instituciones públicas.

1.2 Alcance

Esta norma de segundo grado es de aplicación y cumplimiento obligatorio para todas las entidades comprendidas en el ámbito de aplicación de la Ley 10-07 que establece el Sistema Nacional de Control Interno (SINACI).

Las demás entidades, para las cuales se establecen excepciones y limitaciones en el alcance y aplicación de la Ley 10-07 y su Reglamento de aplicación 491-07, en el marco de sus atribuciones y funciones, podrán solicitar apoyo y asesoría técnica en la materia a la Oficina Gubernamental para la Tecnología de la Información y Comunicación (OGTIC) en aquellos proyectos que lo consideren útil.

1.3 Definición y conceptos relacionados a la Tecnología de la Información y Comunicación (TIC)

Como parte integral de las normas secundarias de control interno es esencial que en todo el Sector Público se apliquen las normas básicas de control interno, guías e instrucciones emitidas por la Contraloría General de la República y para este caso que nos ocupa las normas, guías e instrucciones dadas por la Oficina Gubernamental de Tecnología de la Información y Comunicación (OGTIC), como institución responsable de la gestión de la tecnología de la información y comunicación en la entidades pública. Para efectos de asegurar una gestión eficiente en el uso de la tecnología de la información y comunicación en las entidades sujetas a la presente norma, se hace necesario la existencia de normas, políticas y procedimientos que aseguren una gestión efectiva de las TIC.

Los siguientes términos y conceptos serán utilizados a los fines de esta norma de segundo grado.

- **Declaración Técnica:** Es una explicación detallada de la forma en que deben entenderse los elementos o aspectos expresados en la norma, con el propósito de facilitar su comprensión a la hora de ser aplicada para el desarrollo de las normas secundarias a las cual se refiere.
- **Gestión de la Continuidad**: Proceso general de gestión holístico que identifica amenazas potenciales a una organización y el impacto que se podría causar a la operación de la entidad en caso de materializarse.
- **Interfaz de datos:** Se refiere a toda unidad funcional que transmita o reciba **datos** a través de una red en forma de señal digital o analógica. Toma los **datos** generados por el terminal o computador llamado ETD. los circuitos de conexión con la red (módem) se les llama ETCD.[1]
- **Interfaz de sistema:** Es la conexión física y funcional que se establece entre dos aparatos, dispositivos o sistemas que funcionan independientemente uno del otro.

[1] https://www.ecured.cu/Interfaz_de_transmisi%C3%B3n_de_datos

- **Informaciones clasificadas:** Informaciones sensitivas y/o confidenciales, generalmente protegida por ley.
- **Software:** Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.
- **Aplicación o programa:** Es un tipo de software que funciona como un conjunto de herramientas diseñadas para realizar tareas y trabajos específicos en tu computador.
- **Controles de salida:** Controles diseñados para asegurar que los datos generados por el equipo de cómputo sean válidos, precisos, completos y distribuidos únicamente a personas autorizadas.
- **DRP:** (Por sus siglas en inglés, Disaster Recovery Plan - Plan de Recuperación de Desastres), es la estrategia que se sigue para restablecer los servicios de tecnología (red, servidores, hardware y software) después de haber sufrido una afectación por un incidente o catástrofe de cualquier tipo, el cual atente contra la continuidad del negocio.
- **Gobierno Electrónico** o **E-Gobierno** (en inglés: *e-government*), es el uso de dispositivos tecnológicos de comunicación, como computadoras e Internet para proporcionar servicios públicos a ciudadanos y otras personas en un país o región.
- **Metadatos:** Conjunto de información que describe las características de otra información. Es un dato sobre otro dato.
- **Formato:** Tipo de codificación de la información en un archivo.
- **Estándares Abiertos**: Es un formato de archivo, cuya codificación permite el uso y manipulación de la información libremente.
- **Estándares cerrados**: Es un formato de archivo de archivo de información restringido que solo permite su uso para solo lectura, pero no permite su manipulación.
- **INTRANET:** Se refiere a una red de comunicación interna a la cual no se puede acceder libremente. Son utilizadas por las organizaciones para sus procesos de comunicación entre sus colaboradores.

- **EXTRANET**: Es una red limitada, cerrada, similar a la intranet, solo que a esta se puede acceder desde cualquier punto o área geográfica.
- **Metodología Scrum:** Marco de referencia para la gestión y desarrollo de software, permitiendo realizar un desarrollo ágil.
- **Mantenimiento Preventivo:** Acción que se realiza para eliminar las causas potenciales que pudiesen ocasionar alguna falla o degradación en el funcionamiento del Hardware y/o Software.
- **COBIT:** (Control Objectives for Information and related Technology). Es una guía de mejores prácticas presentada como *framework*, dirigida al control y supervisión de tecnología de la información (TI). Mantenida por ISACA.
- **ISACA:** (*Information Systems Audit and Control Association*). Es una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información.
- **Hardware:** se trata del medio tecnológico utilizado para el almacenamiento, información, entradas y salidas de datos.
- **Software:** son las aplicaciones, programas utilizados para recoger los datos, almacenarlos, procesarlos y analizarlos, con la cual se produce información para el usuario final.
- **Datos:** son el input (entrada) inicial, a partir del cual puede procesarse y estructurarse la información.
- **Procedimientos:** son las políticas y controles aplicables a los procesos de la organización.
- **Usuarios:** ellos son quienes se interactúan con la información extraída de los datos, constituyendo el componente decisivo para el éxito o el fracaso de cualquier iniciativa organizacional.
- **Retroalimentación:** es el elemento clave de cualquier sistema de información al ser la base para la mejora continua.

1.4 El Control Interno de la Gestión de la Tecnología de la Información y Comunicación (TIC) en las entidades públicas

La Contraloría General de la República emitió las Normas Básicas de Control Interno (NOBACI) de primer grado y en la NOBACI 3 de Actividades de Control se establecen las normas básicas generales de segundo grado, y de manera específica las relacionadas con el control de las tecnologías, específicamente la NOBACI 3.2 Actividades de control de sistemas de información, la cual establece que *" La entidad, a través del titular y el nivel directivo, debe definir y desarrollar actividades de control en el ámbito de la tecnología para el logro de los objetivos institucionales"*. En esa norma de primer grado se describen los aspectos siguientes:

a) Uso de la tecnología en los procesos internos y los controles generales sobre la tecnología.
b) Establecimiento de las actividades de control relevantes sobre las infraestructuras tecnológicas.
c) Establecimiento de las actividades de control relevantes sobre los procesos de gestión de la seguridad.
d) Actividades de control relevantes sobre los procesos de adquisición, desarrollo y mantenimiento de tecnologías.

Una buena gestión de las TIC incorporadas en los diferentes procesos diseñados por las instituciones para asegurar el logro de sus objetivos, debe tomar en cuenta en primer lugar, las normas, políticas y estrategias diseñadas por la Oficina Gubernamental de Tecnología de Información y Comunicación (OGTIC), así como, disponer de manera prioritaria de la asesoría de los técnicos que en el marco de las funciones de la OGTIC deben tener disponibles para asistir a las entidades en el desarrollo e implementación de la tecnología más apropiada para ejecutar sus procesos.

Además de las normas emitidas por las entidades que están bajo el alcance de las presentes disposiciones sobre el control interno relacionadas con la gestión de la tecnología de información y comunicación, otros enfoques, marcos de referencia y normativas emitidas

por la OGTIC deberán ser incorporadas en el desarrollo de las normas secundarias diseñadas por las instituciones públicas para desarrollar y fortalecer sus áreas de tecnología de información y comunicación.

Un buen sistema de gestión de TIC debe estar alineado con las estrategias de las entidades orientadas al cumplimiento de su misión y las respuestas que deben dar a los diferentes grupos de interés. Es de mucha utilidad los aportes que diferentes enfoques o marcos de referencia ofrecen para apoyar a las entidades en el diseño de procesos en un entorno tecnológico, siendo el Marco COBIT5 y su versión COBIT2019 el más utilizado para gestionar la T&I en las entidades tanto públicas como privadas.

Este marco de referencia COBIT integra las mejores prácticas y los elementos y principios claves incorporados en otros referentes como las diferentes versiones de ISO 22301-2012, 27000, 27001-2005, 27002, 31001-2009, COSO-1992, 2004, 2013 y su versión 2017 orientada a la gestión de riesgos, entre otros. Todos estos estándares internacionales son referentes obligatorios, los cuales han sido incorporados por la OGTIC, a través de la NORTIC A1:2014, en la elaboración y actualización de la normativa que deben ser incorporadas en los procesos de gestión de la tecnología de información y comunicación en las entidades públicas.

A modo de orientación y para mayor comprensión de la armonización de las NORTIC con el control interno institucional, para garantizar una gestión eficiente, eficaz y alineada con sus objetivos, las entidades sujetas a la aplicación de la presente norma básica especifica de segundo grado, al elaborar las políticas y procedimientos, así como los procesos en la gestión de las TIC, deben considerar los siguientes aspectos:

- Los estándares incorporados por la OGTIC en sus normas generales emitidas a través de la NORTIC A1:2014.
- Las directrices generales incluidas en la sección 1.05, de la NORTIC A1:2014.
- Dada la importancia de la directriz contenida en la subsección 1.05.1, de la NORTIC A1:2014, que se refiere al libre acceso a la información pública, las entidades públicas deben poner especial atención a este apartado.

- Respeto al derecho de autor, para lo cual se debe prestar atención debida a la sub-sección 1.05.2, sobre licencias indicada en la NORTIC A1:2014.
- Como elemento esencial en la administración de la TIC, se debe tomar en cuenta la estructuración de los departamentos responsables de la gestión de los servicios tecnológicos en las instituciones, tal como se aprecia en la NORTIC A1:2014, Capitulo II.
- Las entidades públicas están en el deber de crear una estructura departamental para apoyar la gestión de la TIC, para lo cual deben observar la resolución 51-2013 elaborada entre la OPTIC y el MAP, señalada en la sub-sección 2.01.1 de la NORTIC A1:2014.
- Además de las directrices generales establecidas en la NORTIC A1: 2014, de manera específica deben tomar en cuenta las NORTIC-A2-2021, A2-2023, A6-2016, A7-2016, A5-2019, entre otras normas emitidas por el órgano rector.
- Otro aspecto importante que deben tomar en cuenta las entidades públicas en el diseño de sus políticas y procedimientos relacionada con la TIC, es el contenido de la Ley 107-13, sobre los derechos de las personas en sus relaciones con la administración pública y de procedimiento administrativo.
- Es de vital importancia que las entidades públicas, especialmente las responsables de la investigación y persecución de los crímenes y delitos contra la propiedad, tomen en consideración las disposiciones contenidas en la Ley 53-07 contra Crímenes y Delitos de Alta Tecnología, estableciendo mecanismos de seguridad de los procesos, aplicaciones y equipos, de manera tal que se reduzcan los riesgos de intervenciones maliciosas que puedan afectar su funcionamiento.
- Las entidades públicas sujetas a la presente norma básica de segundo grado, además de las indicaciones anteriormente expuestas, deben asegurarse de observar cualquier disposición legal, normativa o procedimental relacionada con la calidad de los procesos diseñados para la gestión de la tecnología de la información y comunicación.

Las entidades públicas, en sus procesos de elaboración de las normas secundarias, al crear las políticas y procedimientos relacionadas con el control de la calidad de los procesos incorporados para la gestión de la tecnología de la información y comunicación, deben tener en cuenta una serie de disposiciones normativas, tales como leyes, decretos, políticas y procedimientos y marcos de referencia internacionales, incorporados como mejores prácticas para el aseguramiento del logro de los objetivos institucionales, siempre tomando en cuenta los avances y actualizaciones de las herramientas tecnológicas que mejor se adapten a las necesidades propias de su entorno y en relación con la misión y visión estratégica de las mismas.

CAPITULO 2.

2.1 Normas Generales de Control Interno de Segundo Grado para la gestión de la Tecnología de la Información y Comunicación (TIC) en las Entidades Públicas

Las normas básicas de control interno de segundo grado, como parte de la NOBACI 3 - Actividades de Control, son la base donde las entidades deben apoyarse para diseñar o adaptar, de acuerdo con sus fines, objetivos y operaciones, las normas secundarias de control interno, las cuales deben estar acorde a lo dispuesto en la Ley 10-07 y su reglamento de aplicación, con las NOBACI de primer grado, con las NOBACI de segundo grado, con las resoluciones, guías y pautas emitidas por la Contraloría General de la República (CGR) en su calidad de Órgano Rector del Control Interno.

Los titulares de las entidades y los servidores públicos que están bajo el ámbito de aplicación de la presente norma de segundo grado, en los diferentes niveles, como principales responsables del establecimiento y cumplimiento del control interno en las mismas, están en la obligación y el deber de dar seguimiento a las siguientes normas generales relacionadas a la gestión de la Tecnología de la Información y la Comunicación (TIC) en las entidades públicas sujetas a la Ley 10-07 y otras normativas relacionadas con las mismas.

La Oficina Gubernamental de Tecnologías de Información y Comunicación (OGTIC), es el principal órgano responsable de la emisión de las normas relacionadas con la gestión de la tecnología de información y comunicación en las entidades públicas, así como la evaluación de la calidad de los software y hardware que garanticen la calidad de los procesos y de la información que generan los sistemas. Otro órgano rector responsable directo de la gestión de la información y la comunicación es la Dirección General de Ética e Integridad Gubernamental (DIGEIG), así como los organismos responsables de la persecución de los crímenes y delitos de alta tecnología, entre otros.

Con el propósito de estandarizar el control interno en la gestión de las tecnologías de la información y comunicación de las entidades sujetas a la presente norma, se emiten las siguientes normas básicas de segundo grado relacionadas con la NOBACI General 3.2.a, Uso de la tecnología en los procesos internos y los controles generales sobre la tecnología, son las siguientes:

ADC-3-009.01. Principios del control interno en la gestión de las TIC. El titular y los demás servidores de las instituciones sujetas a la presente norma están en la obligación y el deber, en el marco de las atribuciones establecidas en las leyes que las regulan, de ajustar sus normas, políticas, procedimientos y resoluciones a los principios contenidos en el artículo 7 del Reglamento 491-07 de Aplicación de la Ley 10-07 que Instituye el Sistema Nacional de Control Interno y de la Contraloría General de la República, de manera que el uso de la tecnología informática en los diferentes procesos de la gestión institucional este armonizada con dichos principios.

ADC-3-009.01.1. Declaración Técnica. Con el propósito de mejorar los procesos, el uso de los recursos, el tiempo, así como la definición de roles y responsabilidades en las organizaciones, se han diseñado diferentes herramientas que hacen la gestión más eficiente, eficaz y económica.

La calidad de la gestión pública institucional, la cual constituye el primer objetivo del Sistema Nacional de Control Interno, está garantizada siempre y cuando se integren en sus procesos

las directrices establecidas a través de estándares internacionales tales como las diferentes declaraciones de la ISO y asociaciones profesionales relacionadas con las TIC, pero de manera muy consensuada el Marco de Referencia COBIT2019, mediante el cual se trazan las pautas más socorridas para la gestión de las Tecnologías en las organizaciones.

ADC-3-009.01.1. El titular y de los demás servidores públicos están en la obligación y el deber de establecer un modelo de gestión de tecnología de la información y comunicación, en el cual descanse el diseño y establecimiento de los procesos para alcanzar los objetivos institucionales con los principios contenidos en el artículo 7 del Reglamento 491-07, además de los objetivos de transparencia, legalidad y confiabilidad de la información generada por los sistemas, establecido en el artículo 22, numeral 2, de la Ley 10-07.

ADC-3-009.01.2. El titular y de los demás servidores públicos deben cumplir las directrices establecidas por la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC), a través de la Norma de Tecnología de la Información y Comunicación (NORTIC).

ADC-3-009.01.2.2. Declaración Técnica. Además de ser obligatorio su cumplimiento, son un instrumento de mucha utilidad, ya que estas integran en su estructura, todos los referentes antes mencionados, que de ser aplicada de manera correcta, entran en armonía con los principios del control interno establecidos en la Ley 10-07 y su Reglamento de aplicación 491-07 y también con las directrices de otras normativas, entre las cuales se encuentra la Ley 200-04 de libre acceso a la información pública.

ADC-3-009.01.3. El titular y de los demás servidores públicos de las entidades, al diseñar procesos de gestión, en un entorno que favorezca el uso de tecnología, al momento de seleccionar las aplicaciones informáticas, deben asegurarse en todo momento de que las mismas reúnan los requisitos de calidad que permita que la información generada por los sistemas cumpla con los indicadores de calidad establecidos en la normativa vigente. Esto implica que se puedan alcanzar los objetivos utilizando la menor cantidad de recursos y en el menor tiempo posible.

Riesgos Inherentes:

1. Contingencias legales adversas.
2. Incumplimientos legales y normativos.
3. Sobrecoste del servicio.

ADC-3-009.02. Diseño, adquisición y desarrollo de plataforma tecnológica. El titular y los demás servidores responsables del desarrollo y establecimiento del control interno en las entidades sujetas a la presente norma básica de segundo grado, están en la obligación y el deber de asegurarse de que el mismo esté armonizado con el ordenamiento jurídico y técnico aplicable, siempre tomando como premisa su cumplimiento, de manera especial los principios de eficiencia, eficacia, economía, transparencia y legalidad[2] en los procesos y operaciones de diseño, adquisición y desarrollo de plataforma tecnológica, así como software y hardware que garantice de manera razonable la confiabilidad y oportunidad de la información generada por sus sistemas.

En el proceso de Diseño, adquisición y desarrollo de plataforma tecnológica El titular y los servidores públicos de cada entidad en los diferentes niveles de responsabilidad deben:

ADC-3-009.02.01. Verificar el análisis ponderado de las capacidades que dispone la institución versus el apoyo que se obtiene de asesorías externas en esta fase, siendo de utilidad para una gestión eficiente, económica y eficaz de la tecnología de la información en el diseño de los procesos y operaciones de la institución.

ADC-3-009.02.02. Realizar un análisis costo beneficios, el cual contribuirá, en esta etapa de gestión, a la toma de decisión sobre la inversión en tiempo y recursos financieros que deben aplicarse para lograr procesos y operaciones alineados con el logro de los objetivos institucionales.

ADC-3-009.02.03. Tener en cuenta las disposiciones de la Ley 340-06 y su reglamente de aplicación, así como las directrices dadas en la NORTIC A1-2014, sobre los aspectos

[2] Ley 10-07, Art.4.3 Objetivo del SINACI.

mencionados en la norma, al momento de decidir si se adquiere en el mercado aplicaciones y software para apoyar los procesos de gestión; de manera que se garantice no solo el cumplimiento regulatorio, sino que se tome en cuenta lo dicho anteriormente en cuanto a las capacidades de las cuales dispone la entidad para desarrollar programas informáticos requeridos en un momento determinado y las disponibilidades a partir de asesorías externas, para lo cual deben verificarse los mismos principios a partir de la evaluación de los factores que inciden en su precio y calidad.

ADC-3-009.02.04. Hacer un análisis profundo a través de los departamentos de gestión humana y de tecnología de información y comunicación principalmente, lo cual debe incluir un levantamiento de información para determinar las necesidades de capacitación, así como las disponibilidades con la que cuenta la institución para dar respuesta al requerimiento tecnológico de que se trate.

Riesgos Inherentes:

1. Vulnerabilidad en la seguridad.
2. Sobrecoste en adquisición y diseño de equipos tecnológicos.
3. Incumplimientos legales y normativos.
4. No disponibilidad de capital humano necesario.

ADC-3-009.03. Estándares aplicables a las tecnologías de la información y comunicación. El titular y los demás servidores responsables de la gestión de la TIC están en la obligación y el deber de diseñar o ajustar su plataforma tecnológica de acuerdo con estándares internacionales aplicables a las diferentes áreas que inciden en la misma, para lo cual deberá seguir las directrices establecidas en el capítulo IV de la NORTIC A1-2014 y los lineamientos particulares establecidos en el Marco de Referencia COBIT2019 en lo referente a los indicadores que deben incorporarse a los procesos de gestión de la infraestructura tecnológica.

ADC-3-009.03.3. Declaración Técnica. Hoy por hoy, el uso de la TIC es imprescindible para ejecutar los procesos de gestión institucional para lograr una gestión eficiente y competitiva en un entorno global.

Como se apunta en la introducción de este documento, en la actualidad, uno de los estándares más utilizado para orientar la gestión de las TIC en las organizaciones es el marco de referencia COBIT en su versión 2019, el cual ofrece las herramientas más idóneas para evaluar de manera rápida y permanente la finalización de un proyecto, objetivos o metas propuestas en una o varias áreas específicas de la organización, con lo cual se logra un mejor control en los sistemas de información y comunicación.

El marco de referencia COBIT se sostiene en una serie de componentes que sirven de impulso y orientación a la gestión de la TIC en las instituciones. En ese sentido, el uso de las tecnologías de la información y comunicación debe apoyarse en procesos, estructuras organizativas, políticas y procedimientos, flujos de información, cultura y comportamientos, habilidades e infraestructura, que son la base fundamental de la planificación de la gestión institucional.[3]

El titular y los servidores públicos de cada entidad en los diferentes niveles de responsabilidad, como responsables del establecimiento y debido funcionamiento del control interno en la misma, deben atender las siguientes normas generales relacionadas al proceso de Estándares aplicables a las tecnologías de la información y comunicación:

ADC-3-010.03.01. Ajustar sus sistemas de gestión para las normas secundarias de control interno relativas al proceso de las tecnologías de la información y comunicación a criterios o estándares de aceptación generalizada, de manera que les permita insertarse con éxito en el contexto internacional, las cuales deben ser consistentes con la normativa emitida por la

[3] El COBIT 2019 una forma de auditar la gestión e información (cynthus.com.mx)

Contraloría General de la República y el organismo rector de las tecnologías de la información y la comunicación.

ADC-3-009.03.02. Asumir las NORTIC A1:2014, como el referente legal e institucional que las entidades sujeta a la presente norma deben seguir, así como las demás disposiciones y normativas emitidas por la Oficina Gubernamental de Tecnología de la Información y Comunicación (OGTIC).

ADC-3-009.03.02.4 Declaración Técnica. Este marco de referencia oficial NORTIC A1:2014, ha sido diseñado tomando en cuenta los principales estándares internacionales relacionados con la gestión de las TIC, las cuales abarcan desde la infraestructura general hasta el diseño de la estructura o formato de la información que debe salir por los sistemas informáticos.

Para la elaboración de la NORTIC A1:2014, se tomó como referencia varios modelos internacionales con el propósito de asegurar la calidad de cada uno de los procesos diseñados para la gestión de la TIC, entre los cuales pueden consultarse la norma ISO12207, para la gestión y desarrollo de software, que permite realizar un desarrollo ágil; el estándar ANSI/TIA 942 del Instituto Nacional Estadounidense de Estándares y la Asociación de Industria de Telecomunicaciones (ANSI/TIA, por sus siglas en inglés), que trata sobre infraestructura y telecomunicaciones para el centro de datos, entre otros estándares mencionados en el contenido de la citada norma[4].

Riesgos Inherentes:

1. No existencia de una estructura para la TIC aprobada.
2. No existencia de diseño de procesos en las unidades TIC.
3. Retraso en la prestación de los servicios.

ADC-3-009.04. Proceso de gestión y desarrollo de software. El titular y los demás servidores públicos responsables de la gestión de la tecnología de la información y

[4] NORTIC A1:2014, sección 1.02, Referencia Normativa, pag.24

comunicación en las entidades públicas, deben establecer procesos que incluyan políticas y procedimientos para garantizar de manera razonable una gestión y desarrollo de software eficiente, eficaz y económico y alineado con los procesos de gestión para el logro de los objetivos y metas institucionales.[5]

ADC-3-009.04.5. Declaración Técnica. En la sección 5.01 de la citada norma se establecen las pautas a las cuales nos referimos más arriba, las cuales abarcan desde la instalación y reinstalación de software cuando se adquieren de fuentes externas, lo cual incluye la actualización y políticas de uso; desarrollo de software para uso gubernamental, como utilizarlos y su accesibilidad; así como la metodología que debe observarse para que las propias entidades desarrollen sus propios programas informáticos, incluyendo, además, como diseñar los procesos para planificar y gestionar los requerimientos para el desarrollo de software y aplicaciones informáticas.

Todo el proceso desarrollado para crear, adquirir y gestionar las mejores opciones relacionadas con estas tecnologías implica que se tomen en cuenta parámetros que aseguren la utilidad de los mismos en el logro de los objetivos y metas de la entidad. Se recomienda igualmente, que entre las opciones identificadas para el desarrollo o adquisición de software, con el propósito de reducir el costo de los mismos, se establezcan acuerdos con otras entidades especializadas en el estudio y desarrollo de tecnología, tales como el Instituto Tecnológico de Santo Domingo, entre otras entidades formativas tanto nacionales como internacionales.

ADC-3-009.04.01. Para la gestión y desarrollo de software se deben implementar una serie de indicadores que deben cumplirse para lograr que estos se ajusten a los propósitos para los cuales se desarrollan en las propias entidades o se obtienen de proveedores externos.

[5] En ese sentido, deben acogerse a los lineamientos establecidos en el Capítulo V, Secciones 5.01-5.05 de la NORTIC A1: 2014 y la NORTIC A6:2016

ADC-3-009.04.02. Previo al establecimiento de la necesidad de adquirir o desarrollar programas, aplicaciones o software para apoyar los procesos de gestión, los responsables de las TIC en las entidades públicas deben apegarse a las directrices establecidas en las NORTIC A1:2014 y la NORTIC A6:2016.

Riesgos Inherentes:

1. Ausencia de análisis FODA relacionado con las necesidades de programas para la TIC.
2. Sobrecoste en adquisición y diseño de equipos tecnológicos.
3. Incumplimientos legales y normativos.
4. No disponibilidad de capital humano necesario.

ADC-3-009.05. Seguridad de la información y la continuidad en la prestación de servicios. El titular y el resto del personal directivo de las entidades sujetas a las presentes normas básicas de segundo grado, están en la obligación y el deber de establecer controles internos, normas, políticas y procedimientos, de acuerdo con el Capítulo 6, desde la Sección 01 a la 05 de la NORTIC A1:2014 y la NORTIC A7:2016, para garantizar razonablemente la seguridad de la información y la continuidad en la prestación de servicios a los ciudadanos, así como de las operaciones en el interior de la entidad.[6]

ADC-3-009.05.6. Declaración Técnica. Es de vital importancia para las organizaciones, en especial las entidades públicas, una correcta administración de la información generada por los sistemas. Por esas razones es preciso e imperativo que las mismas establezcan políticas y procedimientos adecuados y oportunos que hagan posible la seguridad de la información, pues esta se constituye en el principal activo para la toma de decisiones en las instituciones.

Las secciones 6.01 hasta la 6.05 de la NORTIC A1:2014, establecen de manera detallada las principales directrices para que las entidades gubernamentales desarrollen políticas y

[6] Capítulo 6, desde la Sección 01 a la 05 de la NORTICA1:2014.

procedimientos apropiados que les permitan asegurar de manera razonable el reguardo de este activo.

En ese sentido, las entidades deben orientarse de las NORTIC, sobre las directrices establecidas en la sección 6.01, que trata sobre los diferentes aspectos que deben observarse para realizar una administración eficiente de la información. Así podemos ver como en las subsecciones 9.01.1 se establece que las entidades deben crear un Sistema de Administración de la Seguridad de la Información (SASI) y se describe como debe estar integrado ese sistema y la implicación del titular de la entidad y los demás servidores en el proceso de elaboración, cumplimiento y evaluación del mismo; la responsabilidad del empleado público establecida en la subsección 6.02.2.

Asimismo, en la Sección 6.02 se aborda el tratamiento seguro de la información, donde se considera la información pública, abierta, valiosa, sensitiva y confidencial, los medios mínimos requeridos para procesar la información tales como portal web, correo electrónico, etc.; entre otros aspectos de no menor importancia.

En las demás secciones de este capítulo se dan directrices sobre controles de acceso, Plan de disponibilidad y continuidad, recomendaciones específicas sobre seguridad de las TIC. En lo relativo a las instrucciones sobre el Plan de disponibilidad y continuidad de los servicios, las entidades deben prestar atención especial a la administración de los riesgos en la seguridad de la información para lo cual deben observar las directivas establecidas en la Sub-sección 6.04.3.

Además, se debe observar las directrices establecidas en la NORTIC A7:2016, que reúne de forma actualizada y detallada las actividades a tomar en cuenta en la seguridad de las tecnologías de la información.

Riesgos Inherentes:

1. Vulnerabilidad en la seguridad.
2. Retraso en la prestación de los servicios.

3. Sobrecoste del servicio.

ADC-3-009.06. Reducción en los costos de los procesos y el consumo de materiales en un entorno de TIC. El titular y el resto del personal directivo de las entidades sujetas a las presentes normas básicas de segundo grado, están en la obligación y el deber de establecer controles internos, normas, políticas y procedimientos adecuados que le permitan asegurar razonablemente una administración eficiente, mediante un entorno tecnológico que facilite la reducción del consumo y costo en los procesos, así como mejorar la capacidad de respuesta en la prestación de servicios que ofrecen a la población. En ese sentido, las instituciones deben tomar en cuenta las directrices contenidas en las NORTIC A1:2014, en las secciones 7.01 hasta la 7.05 y la NORTIC A5:2019.

ADC-3-009.06.7. Declaración Técnica. Existe una relación entre el tiempo que se emplea para dar respuesta a las necesidades o requerimiento de un servicio, los recursos físicos empleados en el mismo y el nivel de satisfacción de los usuarios de los mismos. La aplicación de herramientas tecnológica en los diferentes procesos que diseñan las entidades públicas debe integrar unas series de directivas para asegurar la calidad de la información que deben generar los sistemas al menor costo y en el menor tiempo posible.

ADC-3-009.06.1. Para lograr una gestión eficiente, las entidades están en el deber de seguir los lineamientos contenidos en el capítulo VII de la NORTIC A1:2014, las cuales en las secciones 7.01 hasta la 7.05 describen los principales indicadores para alcanzar los estándares de calidad en la administración

ADC-3-009.06.01.8. Declaración Técnica. Entre los lineamientos planteados en la norma anterior, se encuentran entre otros, la digitalización de documentos, se establecen los requerimientos técnicos de los documentos para la digitalización; requerimientos para la creación de la Intranet, estructura de contenido de la Intranet, directrices relacionadas con la tecnología verde, canales de acceso, disposiciones sobre el portal de transparencia, entre otros aspectos relacionados con la creación de portales y sub portales en las entidades públicas, así como recomendaciones sobre el uso de papel, para la implementación de las

tecnologías verde y para la gestión de canales de acceso más apropiados, tales como el uso de las redes sociales de manera que se pueda llegar a más ciudadanos. Así como también lo establecido en la NORTIC A5:2019.

Riesgos Inherentes:

1. Sobrecoste en adquisición y diseño de equipos tecnológicos.
2. Incumplimientos legales y normativos.
3. Sobrecoste del servicio.

ADC-3-009.07. Gestión de Medios Web (CAMWEB). El titular de las entidades sujetas a las presentes normas básicas de segundo grado, debe asegurarse de que se constituya un Comité de Administración de Medios Web (CAMWEB), de acuerdo con lo establecido en la sección 1.05.1.c del Capítulo I de la NORTIC A-1:2014 y el Marco COBIT2019.

ADC-3-009.07.9. Declaración Técnica. Las entidades públicas, de acuerdo con las directrices establecidas en la Sub-sección 1.05.1.c, de la NORTIC A1:2014, las NORTIC A2:2016, A2:2021, A3:2014 y la B2:2018, están en el deber de constituir un comité que se encargue, entre otras funciones, de la administración de medios Web.

ADC-3-009.07.1. Este comité conocido por sus siglas en inglés CAMWEB debe estar integrado por la Oficina de Acceso a la Información (OAI), Tecnología de la Información y Comunicación (TIC), Legal, Comunicaciones, Prensa y Relaciones Públicas, entre otros.

ADC-3-009.07.2. El Comité de Administración de Medios Web, según lo establece la NORTIC A3:2014, debe ser el responsable principal del levantamiento de la información reutilizable o sea que el CAMWEB, debe ser el responsable del proceso de apertura de los datos de cada organismo y de que estos estén publicados en el portal web www.datos.gob.do con la periodicidad establecida.[7]

[7] Capítulo II. Levantamiento de la información sección 2.01 Responsables de la información, NORTIC A:3

Riesgos Inherentes:

1. No existencia del comité encargado de la gestión del portal web
2. Contingencias legales adversas.
3. Vulnerabilidad en la seguridad.
4. No disponibilidad de capital humano necesario.
5. Dificultad de acceso al portal web institucional.

2.2 Normas Específicas de Segundo Grado de Control Interno para la Gestión de las Tecnologías de la Información y Comunicación en Entidades Públicas.

El desarrollo y cumplimiento de las disposiciones generales contenidas en la Estrategia Nacional de Desarrollo establecida a través de la Ley 1-12 y las políticas y disposiciones del Poder Ejecutivo mediante decretos, con el propósito de hacer más eficiente la ejecución de los diferentes procesos de la administración pública, han hecho imprescindible paras las entidades públicas el desarrollo e implementación de tecnologías apropiadas para asegurar la eficiencia, efectividad, confiabilidad y oportunidad de la información generada por los sistemas.

De ahí que las instituciones públicas deben adaptar sus procesos para que los mismos se ajusten a una estructura tecnológica de acuerdo con las disposiciones establecidas en las Normas para el uso de la Tecnología de la Información y la Comunicación (NORTIC) emitidas por la OGTIC.

En ese sentido, la Contraloría General de la República, en su calidad de órgano rector del control interno institucional, con el propósito más bien de reforzar el compromiso de las entidades en el cumplimiento de las NORTIC, emite las siguientes Normas Básicas Específicas de Segundo Grado relacionada con los diferentes aspectos que deben tomarse en cuenta para el buen uso de las TIC.

El titular de la institución y los servidores públicos de cada entidad en sus diferentes niveles, son responsables del establecimiento y debido funcionamiento del control interno relacionadas con la Gestión de las Tecnologías de la Información y Comunicación en Entidades Públicas. Deben atender las siguientes normas específicas:

2.2.1 Normas Específicas sobre la Organización de TIC

ADC-3-009.08. Organización de Estructura de TIC. El titular y el resto del personal de las entidades públicas, tienen el deber de organizar sus Unidades de Gestión de Tecnología de la Información y Comunicación, de acuerdo con los lineamientos establecidos en la Resolución No.51-13 emitida por el Ministerio de Administración Pública y por la Oficina Gubernamental de la Tecnología de la Información y Comunicación, poniendo énfasis en los criterios que mejor se ajusten al modelo propuesto que aplique a la entidad.

ADC-3-009.08.01. Las entidades públicas deben tomar en cuenta para sus políticas y procedimientos y para adecuar sus unidades de TIC, los modelos propuestos en la Resolución No.51-2013, los cuales establecen una serie de criterios que las entidades deben tomar en cuenta para adecuar sus unidades de TIC, de manera que las mismas respondan a las necesidades definidas en sus procesos.

ADC-3-009.08.02. La entidad pública de que se trate debe asignar la responsabilidad de la gestión Tecnología de la Información (TI) a una unidad específica, con el propósito de alcanzar la homogeneidad de criterios para el logro de los objetivos de la entidad en materia de tecnología de información y comunicación.[8]

ADC-3-009.08.03. Las entidades deben elaborar las descripciones de los puestos de trabajo que conforman la unidad de TI, en las mismas deben contemplar tanto la autoridad como la responsabilidad. Estas descripciones deben estar documentadas y aprobadas, así como, deben dar a conocer personal de TI de sus deberes y responsabilidades.

[8] Normas de Control Interno para la Tecnología de Información Argentina.

ADC-3-009.08.04. La Oficina Gubernamental de la Tecnología de la Información y Comunicación (OGTIC) debe implementar un proceso de asistencia y capacitación al personal responsable de las TIC en las entidades públicas, de conformidad con lo establecido en el Decreto 1090-04.

ADC-3-009.08.05. El titular y demás servidores públicos de las entidades, en concordancia con el plan estratégico de las mismas, deben establecer y mantener políticas y procedimientos para identificar y documentar las necesidades de capacitación de todo el personal que utiliza los servicios de información.

ADC-3-009.08.06. Se debe establecer un plan de capacitación para cada grupo de empleados, tanto los usuarios finales como el personal técnico informático. Deben contemplarse medidas de concientización sobre la seguridad informática para todo el personal y para los usuarios de los servicios que brinda el organismo.

ADC-3-009.08.07. La institución debe realizar sus asignaciones de responsabilidades considerando una adecuada separación de funciones, que promueva el control por oposición de intereses, y propiciar rotaciones periódicas de personal con asignaciones de tareas críticas.

ADC-3-009.08.08. Es recomendable que además del cumplimiento de las disposiciones de la Resolución 51-2013 sobre la Estructura TIC, las entidades organicen su gestión sobre la base de los Principios de Gobierno establecidos en el Marco de Referencia COBIT, versión 2019: 1. Basado en un modelo conceptual; 2. Abierto y Flexible y, 3. Alineado con los principales estándares.

Riesgos inherentes:

1. Administración de prioridades no alineada con las necesidades y estrategia organizacional.
2. Atención priorizada del área de TI a la gerencia usuaria de la cual depende.
3. Dificultades para exigir rendiciones de cuentas.

4. Dificultades para el planeamiento, la ejecución y el control de las tareas.
5. Dilución de responsabilidades

2.2.2 Normas Específicas para Plan Estratégico de TI

ADC-3-009.09. Planificación estratégica en las unidades TIC. Las entidades y organismos públicos deben implementar políticas y procedimientos, atendiendo a las propuestas formuladas por las unidades o departamentos responsables de las TIC para la planificación, definición de estrategias y dirección de la estructura TIC en consonancia con los fines y propósitos de la entidad y con las Normativas emitidas por la OGTIC.

ADC-3-009.09.10. Declaración Técnica. La planificación estratégica es un instrumento de vital importancia en la Gestión de las Tecnologías de la Información y Comunicación, la cual debe estar alineada o más bien integrada, en el caso de las entidades públicas dominicanas, con los objetivos institucionales.

Es imperativo que exista una conexión entre la planificación estratégica de las TIC y la planificación estratégica de la organización. Los objetivos incluidos en la planificación estratégica TIC pueden prolongarse por hasta cinco años, igual puede ocurrir con los objetivos de la organización, aunque es bueno señalar que en el caso de las entidades públicas, generalmente se programan inicialmente por tres años.

Estos objetivos se enfocan a la gestión de la infraestructura tecnológica, siempre en consonancia con los planes estratégicos de la entidad. Todo lo que ocurre en el departamento de TIC afecta a toda la institución, pues su propósito debe ser respaldar los objetivos de la organización, lo cuales se pueden ver impactados, ya sea la implantación satisfactoria de la conectividad remota o el fracaso en la contención del malware.[9]

---

[9] Ing. Rubén Bernardo Guzmán Mercado /**Planeación Estratégica de TI para el 2021/** https://www.rberny.com/2020/08/29/planeacion-estrategica-de-ti-para-el-2021

Es de vital importancia la planificación estratégica en las TIC por las siguientes razones:

a. Ayuda a tomar mejores decisiones.
b. Mayor eficiencia, efectividad y economía en las adquisiciones informáticas.
c. Facilita la evaluación temprana de las necesidades de ajuste o cambios en la infraestructura de TI en la organización.
d. Mejor adaptabilidad y flexibilidad a los cambios en el entorno informático.

ADC-3-009.09.1. Las entidades públicas deben alinear e integrar en la planificación estratégica de TIC, con los objetivos institucionales.

ADC-3-009.09.2. Los responsables de las unidades TIC en las entidades y organismos públicos, para la elaboración del plan de TIC, deben realizar la evaluación de los requerimientos de todas las áreas, para su priorización y deben hacer el análisis de los riesgos como elemento de gestión, así como deben considerarse las directrices estratégicas en TIC emanadas de la Estrategia Nacional de Desarrollo.

ADC-3-009.09.3. Los objetivos relacionados con las TIC deben surgir del análisis de la fortaleza y debilidades relacionadas con la tecnología a lo interno; así como las amenazas y oportunidades que surgen en el ambiente externo, que podrían afectar de manera positiva o negativa los objetivos de la entidad.

ADC-3-009.10. Plan de contingencia y continuidad en la prestación de servicios. El titular y demás servidores de las entidades públicas sujetas a la presente Norma Básica de Segundo Grado específicas, deben establecer políticas, procesos y procedimientos que permitan responder oportunamente a los requerimientos de asistencia técnica de las diferentes estaciones de trabajo en un ambiente basado en Tecnologías de la Información y Comunicación, de manera que se pueda garantizar la continuidad en los servicios de acuerdo con los estándares establecidos en las normativas y modelos aplicados.

ADC-3-009.10.11. Declaración Técnica. El propósito de Gestionar la Continuidad del Servicio es evitar que una interrupción imprevista de los servicios genere consecuencias catastróficas para la entidad de que se trate. Las complicaciones podrían ser causadas no solo de fallas en la infraestructura tecnológica o TI (ataques de denegación de servicio, virus, entre otros) sino también de desastres naturales (incendios, inundaciones, terremotos, entre otros).[10]

ADC-3-009.10.1. Las entidades deben establecer políticas y procedimientos para el aseguramiento de la continuidad en la prestación de los servicios en un entorno tecnológico. Las mismas deben contemplarse en la gestión de los riesgos a los que se exponen las instituciones ante posibles fallas en los procesos ejecutados a través de programas informáticos.

ADC-3-009.10.2. Las entidades públicas deben seguir las directrices establecidas en el capítulo VI, desde la sección 6.01 de la NORTIC A1:2014, las cuales les permiten crear los procedimientos y controles claves para asegurar la correcta implementación de la continuidad, tanto para la prestación de servicios al ciudadano como de las operaciones dentro de los organismos.

ADC-3-009.10.3. Entre las directrices establecidas por la OGTIC, las entidades deben acogerse, con el propósito de destacar la necesidad de las entidades de tener un plan de disponibilidad como se detalla en la Sub-sección 6.04.1 de la NORTIC A1:2014, debe seguir los siguientes lineamientos:

"(a) Los organismos gubernamentales deben tener un plan de disponibilidad. Este debe tener las siguientes informaciones:

(i) La situación actual de disponibilidad de los servicios TIC. Información que debe ser actualizada periódicamente.

(ii) Herramientas para la monitorización de la disponibilidad.

[10] Plan De Continuidad De Servicios De Ti Proceso De Tecnologías Y Sistemas De Información

(iii) Métodos y técnicas de análisis a utilizar.

(iv) Definiciones relevantes y precisas de las métricas a utilizar.

(v) Planes de mejora de la disponibilidad.

(vi) Expectativas futuras de disponibilidad.

Igualmente, refiriéndose a la continuidad de los servicios que presta el organismo, la Sub-sección 6.04.2 de la NORTIC A1:2014 en los literales de la ***a*** hasta la ***f*** se establecen las directrices que deben seguir los organismos gubernamentales, entre las cuales se citan las siguientes:

(a) Los organismos gubernamentales deben tener un Comité de Continuidad (CONTI).

(b) El CONTI debe estar compuesto por la Alta Gerencia, la máxima autoridad del departamento TIC y áreas claves del organismo gubernamental para la prestación de servicios.

(c) Los organismos gubernamentales deben tener un plan de continuidad para asegurar la no interrupción de sus operaciones vitales y sus servicios al ciudadano o demás organismos.

(d) Los organismos gubernamentales deben realizar un Análisis de Impacto del Negocio (BIA, por sus siglas en inglés) y este debe ser de insumo para la implementación del plan de continuidad."[11]

2.2.3. Normas Específicas de Procesamiento y Comunicación de la Información

ADC-3-009.11. Gestión de Información y Comunicación. Las entidades y organismos sujetos a las disposiciones contenidas en las presentes disposiciones normativas, deben establecer controles que garanticen la integridad y seguridad de la información que genera el sistema, así como la automatización de las operaciones y procesos de la entidad, de

[11] NORTIC A-1 .2014

manera que la comunicación tanto interna como externa se desarrolle de manera fluida y de acuerdo con los objetivos y metas de la organización.

ADC-3-009.11.12. Declaración Técnica. En las directrices establecidas en las NORTIC A7:2016 y la NORTIC A2:2023, se abordan de manera extensa los elementos mencionados más arriba y que aseguran la integridad de la información obtenida de los sistemas.[12]

La integridad implica mantener la consistencia, precisión y confiabilidad de los datos durante todo su ciclo de vida. Los datos no deben modificarse en tránsito, y deben tomarse medidas para garantizar que personas no autorizadas puedan alterar los datos (por ejemplo, en una violación de la confidencialidad). Estas medidas incluyen permisos de archivos y controles de acceso de usuarios.

ADC-3-009.11.1. Las entidades públicas, deben organizar los elementos esenciales (hardware, software, datos, procedimientos, usuarios y retroalimentación) de su sistema de información, los cuales deben integrarse de manera que puedan operar de manera conjunta.

ADC-3-009.11.2. Las entidades públicas que se encuentran bajo el ámbito de aplicación de la presente norma de control interno y las políticas dictadas por la OGTIC en su condición de órgano rector de las TIC, deben ajustar sus sistemas de información y comunicación de acuerdo a las directrices establecidas en las NORTIC A7:2016 y la NORTIC A2:2023, las cuales detallan todas las políticas y guías que deben observarse para la gestión de los portales WEB y la transparencia, así como la Norma para la seguridad de las tecnologías de la información y comunicación en el Estado dominicano, respectivamente.

Riesgos Inherentes:

1. No integridad de la información.
2. No consistencia en la información.
3. No. confiabilidad de la información generada por los sistemas.

[12] NORTIC A2:2023 NORMA PARA EL DESARROLLO Y GESTIÓN DE LOS PORTALES WEB Y LA TRANSPARENCIA DE LOS ORGANISMOS DEL ESTADO y NORTIC A7:2016 Norma para la seguridad de las tecnologías de las información y comunicación en el Estado dominicano.

4. Acceso de persona no autorizada a la información.

ADC-3-009.12. Acceso a la Información Pública. El titular y los demás servidores de las entidades públicas, principalmente los responsables de las TIC sujeto a las presentes normas, deben establecer políticas y procedimientos que garanticen a los usuarios de los portales WEB el acceso a la información de manera rápida, sencilla e intuitiva, ya sea en la versión de escritorio o móvil, para lo cual deben acogerse a las directrices establecidas en las secciones 2.01, 2.02 y 2.03 de la NORTIC A2 de la versión 2023.

ADC-3-009.12.13. Declaración Técnica. Para alcanzar esos propósitos en la sección 1.06 de la NORTIC A2:2023 se establecen políticas generales que las entidades deben seguir para asegurar que sus portales se organicen y se administren bajo criterios bien definidos y documentados para que se garantice la continuidad de las operaciones y responsabilidades designadas para tales fines.

ADC-3-009.12.1. Las entidades públicas deben tomar en consideración las políticas establecidas por la OGTIC, a través de la citada NORTIC se encuentra la obligación de las entidades de contar con una política de gestión de portales web, la cual debe contener, entre otros elementos, los siguientes:

- **Alcance**: donde se establezca que todos los portales desarrollados por la institución deben ser gestionados de acuerdo con los requerimientos de la política desarrollada.
- **Responsabilidades de gestión de los portales:** estableciendo claramente la estructura de responsabilidades para la gestión de los portales a lo interno de la institución, incluyendo:
    - ✓ Carga de Contenido.
    - ✓ Gestión de Servicios.
    - ✓ Desarrollo y Soporte.
    - ✓ Seguridad.
    - ✓ Procedimientos para actualizar y modificar el portal web, tanto en estructura como en contenido.

- **Gestión de las Contraseñas:** donde se indique la creación, almacenamiento y protección de las contraseñas utilizadas en la gestión de los portales web, como se indican en la sección 5.5 sobre seguridad, directriz. (Ver sección 1.06 completa) de la NORTIC A2:2023.[13]

ADC-3-009.12.2. Las entidades públicas, en lo que se refiere a las facilidades de acceso de los usuarios a los portales, deben dar seguimiento a las directrices generales de usabilidad establecidas en la Sección 2.01 de la NORTIC A2:2023, pues con estas los usuarios de la información podrán ubicar la información de su interés de manera sencilla e intuitiva, ya sea a través de sus computadoras de escritorio, teléfono móvil o computadora portátiles.

ADC-3-009.12.3. Las entidades públicas deben ajustarse a las directrices del órgano rector de las TIC, específicamente las establecidas en la NORTIC A2:2023 de manera que sus portales se desarrollen, se desplieguen y se administren bajo lineamientos claros y documentados que faciliten a los ciudadanos el acceso a la información de manera ágil, rápida y fluida.

Riesgos Inherentes:

1. Ausencia de políticas para el acceso a la información.
2. Que los usuarios no puedan acceder de manera rápida y oportuna a la información.
3. Que la entidad no se acoja a la normativa vigente.

ADC-3-009.13. Disposición de los elementos en los portales. El titular y los demás servidores públicos de las instituciones responsables de la gestión de la tecnología de la información y comunicación, deben diseñar políticas y procedimientos que les permitan asegurarse de que la disposición de los elementos que deben contener los portales se haga de la manera correcta, para lo cual deben seguir las directrices dadas en las secciones 3.01 hasta la 3.04 de la NORTIC A2 de la versión 2023 que se refiere a la disposición en la

[13] NORTIC A-2.2023, sección 1.06

versión de escritorio, móvil y equipos portátiles y como deben disponerse para portales de iniciativas y proyectos.

ADC-3-009.13.14. Declaración Técnica. Las directrices de la NORTIC están armonizadas con lo dispuesto en el Sistema de Diseño Dominicano con el propósito de que se mantenga la identidad, de forma que los usuarios puedan identificar cualquier portal que pertenezca al Estado dominicano que le permita navegar en un entorno propicio y bien estructurado.

Un aspecto muy importante a destacar es que al crear el portal, las instituciones adopten un diseño que se adapte a cualquier dispositivo. En ese sentido, la sección 3.01 de la NORTIC A2:2023 establece el conjunto de directrices que deben respetarse y aplicarse en todos los medios web de la Administración Pública, lo cual incluye todo tipo de organismo, entre las cuales se destacan las siguientes:

- El portal debe tener un diseño responsivo. [14]

  Las herramientas o técnicas utilizadas deben ser flexibles para cambios, de manera que puedan responder correctamente a las diferentes dimensiones de los dispositivos por el cual se acceda, manteniendo la estructura establecida.

- El portal del organismo, ayuntamiento y embajada, independientemente del dispositivo por el cual se acceda, debe cumplir con los siguientes requerimientos:
  - ✓ Debe soportar tres grandes divisiones: cabecera, contenido y pie de página.
  - ✓ La estructura para la cabecera y pie de página debe tener una alineación al centro de la pantalla y mantenerse igual en todas las secciones y subsecciones.

ADC-3-009.13.1. Las entidades públicas sujeta a la presente norma están en el deber de cumplir las directrices contenidas en la sección 3.01 NORTIC A2:2023 que indican como

[14] **Diseño responsivo es crear un solo sitio web que se adapte a dispositivos diferentes, manteniendo su estructura y orden.** Así, cada elemento de la web se adapta a las proporciones de cualquier pantalla, permitiendo una correcta visualización y navegación. https://rockcontent.com/es/blog/diseno-responsivo/

deben dividirse los espacios en un portal web y como ubicar los componentes que se vayan a utilizar en el mismo.

ADC-3-009.13.2. Las demás secciones y todas las directrices contenidas en las NORTIC A2:2023 deben ser acatadas por los organismos públicos sujetos al ámbito de aplicación de la presente Norma Básica Específica de Segundo Grado sobre las TIC para asegurar la eficiencia y eficacia en la disposición de los elementos en los portales web.

Riesgos Inherentes:

1. Que los espacios no estén bien distribuidos,
2. Que los títulos y subtítulos no estén de acuerdo con la normativa vigente.
3. Que no haya armonía en el diseño del portal con el Sistema de Diseño Dominicano.
4. Que el diseño no sea adaptable a cualquier dispositivo.
5. Que el diseño del portal no sea responsivo.

ADC-3-009.14. Contenidos de los portales web. El titular y los demás servidores responsables de la gestión de la Tecnología de la Información y Comunicación en las entidades públicas sujetas a las presentes normas específicas de segundo grado, deben asegurarse de manera razonable de que el contenido de los portales web es el adecuado, en cuanto a cantidad, calidad y legalidad y que el mismo obedece a las directrices contenidas en las secciones 4.01- 4.08 de la NORTIC A2:2023 y las establecidas en la Ley 200-04 y su reglamento de aplicación No.130-05.

ADC-3-009.14.15. Declaración Técnica. Es importante tomar en cuenta que la información subida a los portales web debe ser significativa y útil para el público, en la mayoría de los casos, teniendo en cuenta lo que a ellos les interesa y no lo que le interesa al autor.

Es conviene tener cuidado en no abusar de la información textual, ya que son muy pocos visitantes que se leen completamente una página web. Sin embargo, como apuntamos en el primer párrafo de esta declaración, la información subida por las entidades públicas esta

normada en cuanto a su forma, calidad, cantidad, pertinencia, oportunidad y utilidad, pues debe cumplir los atributos que favorezcan la transparencia.

La sección 4.01 de la NORTIC A2:2023 establece las directrices generales que deben tomar en cuenta las entidades públicas al trabajar los contenidos de sus portales web. En estas pautas se establece las informaciones básicas obligatorias que debe ser integrada en la estructura de dichos sitios, entre los cuales se destacan los siguientes:

- Las estructuras de contenido especificadas en este capítulo no deben ser cambiadas de orden ni sustituir sus nombres.
- El portal web debe contar con el Identificador Oficial del Estado Dominicano.
- Bandera de la República Dominicana.
- Opción desplegable hacia abajo que muestre como identificar la veracidad del portal.
- Mensaje que indica que es un portal oficial del Gobierno de la República Dominicana, entre otras disposiciones.

Igualmente se presenta un apartado para los contenidos de los portales en los ayuntamientos y las embajadas. Finalmente, se presentan unas recomendaciones que permiten ayudar con la calidad, suficiencia y extensión de los textos en los sitios web institucionales.

ADC-3-009.14.1. Las entidades públicas, al momento de elaborar los contenidos dispuestos en el sitio web, deben tener especial cuidado en el cumplimiento regulatorio, ya que las leyes, procedimientos y normas que regulan el libre acceso a la información pública son las que establecen las características que debe reunir la información subida a la página web.

ADC-3-009.14.2. Las entidades y los responsables de las TIC, especialmente los encargados de la administración del sitio web, deben cumplir las disposiciones establecidas en las secciones 4.02 hasta la 4.07 para la disposición de los contenidos en la página web. En dicha sección se detallan como debe estructurarse el contenido institucional, lo relativo a la transparencia y contenidos para dispositivos móviles.

Riesgos Inherentes:

1. Que el contenido de la información no sea ni suficiente ni adecuada.
2. Que la información cargada en los portales no cumpla el criterio de legalidad.
3. Que los contenidos no estén debidamente ordenados.
4. Que la información cargada no cumpla con los criterios de utilidad, oportunidad, pertinencia, entre otros.
5. Que no se mantenga la estructura de contenido establecida en la normativa.

ADC-3-009.15. Seguridad en la gestión de los medios web. El titular y los responsables de la gestión de las TIC en las entidades públicas sujetas al ámbito de aplicación de la presente Norma Básica Específica de Segundo Grado deben asegurarse de crear las condiciones que permitan una gestión eficiente, segura y confiable de los portales web, especialmente el nombre de dominio, en cuanto al uso de las jerarquías que corresponda, y la creación mediante resolución del Comité de Implementación y Gestión de Estándares TIC (CIGETIC). En ese sentido deben acogerse a las disposiciones contenidas en las secciones 5.01 hasta la 5.04 de la NORTIC A2:2023.

ADC-3-009.15.16. Declaración Técnica. Las directrices contenidas en las secciones de 5.01 hasta la 5.05 abordan las pautas que deben seguirse para gestionar de manera correcta los elementos relacionados con la seguridad de los portales, tales como los nombres de dominio, la administración de contenido, estadísticas y seguridad, los cuales representan componentes fundamentales para el funcionamiento de los medios web.

La continuidad en la prestación de los servicios y la protección de la imagen de las entidades públicas frente a los usuarios de la información debe ser un objetivo de las entidades y los riesgos que pueden afectar su consecución deben ser gestionados adecuadamente, a través de respuestas que podrían consistir en mecanismos de control de acceso que aseguren la confidencialidad de las informaciones.

ADC-3-009.15.1. Las entidades públicas deben asegurarse de que el sistema de seguridad en un ambiente basado en tecnología de la información y la comunicación debe establecerse tomando en consideración los objetivos siguientes:

- **Confidencialidad**, que implica la generación de respuesta a las amenazas de divulgación no autorizada de información sensible de la institución.
- **La integridad**, se refiere a la seguridad razonable de que la información pueda conservarse sin alteraciones ante la ocurrencia de hechos fortuitos e intentos maliciosos. Es decir, que la información sólo pueda ser modificada mediante mecanismos de autorización previamente establecidos.
- **La disponibilidad**, se entiende el mantenimiento de la página web activa sin sufrir ninguna interrupción que pueda afectar el acceso de los usuarios a la información. Es necesario que se ofrezcan los recursos que requieran los usuarios autorizados cuando se necesiten. La información pública o de código abierto debe permanecer accesible.

ADC-3-009.15.2. Las entidades sujetas a la presente norma deben orientar la gestión de los medios web de manera eficiente, eficaz y segura para lo cual disponen de las directrices establecidas en las secciones de 5.01 hasta la 5.05.

ADC-3-009.15.3. Las entidades están en el deber de acogerse a las directrices establecidas en la NORTIC A2:2023 en la sección 5.05 que aborda todos los temas relacionados con la seguridad web.

Riesgos Inherentes:

1. nombres de dominio, la administración de contenido, estadísticas y seguridad,
2. Divulgación no autorizada de información sensible.
3. Que no información no este protegida ante la ocurrencia de hechos fortuitos.
4. No acceso a la información por falta de mantenimiento de la página web.

ADC-3-009.16. Accesibilidad a la información pública. El titular de cada entidad y organismo público, así como los demás servidores responsables de la administración de las TIC, deben establecer políticas y procedimientos claros que faciliten la accesibilidad, de manera que estos medios puedan ser utilizados por cualquier persona, sin importar su condición o capacidades personales, independientemente de sus conocimientos de las características técnicas del equipo utilizado para acceder a la web, reduciendo las barreras que puedan dificultar su uso.

ADC-3-009.16.17. Declaración Técnica. Desde su creación, la web tiene su fundamento en facilitar los medios para que más personas puedan acceder a la información. Así que el objetivo fundamental de las páginas es que la misma sea utilizada por la mayor cantidad de personas sin importar sus conocimientos o capacidades personales, independientemente de sus limitaciones en cuanto al conocimiento técnico del equipo utilizado para acceder a la web.[15]

A nivel general se ha trabajado de manera consistente para lograr una mayor accesibilidad a la web, de manera que se alcancen los objetivos relacionados con la inclusión.
Para lograr ese propósito se han desarrollado políticas, directrices y pautas que orientan como se crean las páginas web. De igual manera se han creado aplicaciones que facilitan el acceso de persona con discapacidades, tales como dificultades para leer, escuchar, escribir, entre otras.

Para facilitar el acceso a la información en la página web, se puede utilizar la tecnología Text-to-Speech (TTS), este convierte un texto digital en palabras habladas, el cual es de utilidad para aquellas personas con aprendizaje o dificultades para poder leer. Ejemplo de estas aplicaciones incluyen: Natural Reader, Speechify y Speechelo. Entre las aplicaciones más utilizadas encontramos: Microsoft Speech API, Nuance Dragon (anteriormente Dragon NaturallySpeakin), entre otros.[16]

[15] Accesibilidad web. Universidad de Alicante
https://accesibilidadweb.dlsi.ua.es/
[16] https://blogs.iadb.org/conocimiento-abierto/es/accesibilidad-web/

Otra tecnología de asistencia para facilitar la accesibilidad son los lectores de pantalla. Estas aplicaciones facilitan a las personas con discapacidad visual leer el texto que se muestra en la pantalla de la computadora con un sintetizador de voz o una pantalla braille. Algunos ejemplos incluyen: JAWS, NVDA y VoiceOver.[17]

ADC-3-009.16.1. Las entidades públicas están en el deber de establecer políticas y procedimientos y controles claves en los diseños de la estructura de la información que facilite el acceso universal a la información de acuerdo con lo establecido en la Ley 200-04 y su reglamento de aplicación No.130-05 y de manera específica las directrices de la NORTIC A2:2023 en las secciones 7.01 y 7.02., también las directrices dadas en la NORTIC A1:2014.

ADC-3-009.16.2. Se debe tener en cuenta el diseño, de manera que el sitio pueda ser accesible por cualquier persona que tenga una determinada discapacidad, sea esta temporal o permanente. Debe atenderse en su diseño a las necesidades no solo de los usuarios en cuanto a las limitaciones personales, sino también a los intereses de la entidad pública. En ese sentido, también se debe prestar atención a la tecnología que sirve para ayudar a mejorar la experiencia en la web.

Riesgos Inherentes:

1. No existencia de políticas que faciliten el acceso a personas con discapacidad.
2. No observancia de la normativa que protege los derechos de las personas con discapacidad.

ADC-3-009.17. Levantamiento, identificación, estructuración y publicación de la información reutilizable. El titular de cada entidad y organismo público, así como los demás servidores encargados de la gestión de los portales Institucionales (CAMWEB) deben establecer y aplicar políticas y procedimientos para garantizar razonablemente que el proceso de levantamiento de la información que debe ser publicada dentro de la categoría de "Datos Abiertos" respondan a las necesidades de los diferentes usuarios, de acuerdo

[17] https://blogs.iadb.org/conocimiento-abierto/es/accesibilidad-web/

con la normativa vigente, para lo cual es preciso observar las directrices trazadas por la DIGEIG y la OGTIC, en el Capítulo II, sección 2.01 de la NORTIC A3:2014.

ADC-3-009.17.18. Declaración Técnica. En cuanto a la información relevante se entiende por aquella que puede ser reutilizable, tales como el presupuesto, nómina, planes y proyectos de la entidad, listado de funcionarios, entre otras.

ADC-3-009.17.1. Las entidades y los servidores públicos responsables de la gestión de los portales web, en el proceso de levantamiento de la información que debe ponerse a disposición de los diferentes grupos de interés, deben tomar en cuenta una serie de directivas que van encaminadas a asegurar que la información que ha de ser reutilizable, sea validada por parte del público.

ADC-3-009.17.2.[18]Las entidades deben crear políticas y procedimientos que le permitan asegurarse del cumplimiento de los aspectos legales que deben observarse para el tratamiento de la información considerada sensible, así como los criterios establecidos para disponer de información relevante.

ADC-3-009.17.3. En cuanto a la información sensible, las entidades deben tomar en consideración los aspectos legales relacionados con la información que pueda afectar la seguridad del Estado. Para esos fines es preciso consultar la ley que regulan el acceso a la información pública, la ley de archivos y entre otras.

ADC-3-009.17.4. Las entidades públicas deben tomar en cuenta el debido cuidado al gestionar la información reutilizable, es el debido cuidado de que no se publique información de carácter personal o que esté relacionada con la vida privada de la persona física. Igualmente se debe poner atención al orden en que deben presentarse los datos.[19]

[18] Ver secciones 2.02, Selección de la Información y 2.02.1, Información Relevante, 2.02.2 Restricción a la Publicación de la Información, NORTIC3:2014

[19] Ver secciones 2.03 y 2.04 sobre Datos Personales y Ordenamiento de Datos, NORTIC a3:2014.

Riesgos Inherentes:

1. Que no se publique la información requerida.
2. Que se publique información de las personas físicas.
3. Que no se tenga cuidado de la información sensible.

ADC-3-009.18. Información reutilizable. El titular de cada entidad y los demás servidores públicos encargados de la gestión de la TIC deben elaborar políticas y procedimientos que le permitan asociar la información reutilizable, de acuerdo con la categoría que corresponda y siguiendo las directrices trazadas por la OGTIC en el Capítulo III, sección 3.01 de la NORTIC A3:2014.

ADC-3-009.18.19. Declaración Técnica. La información gestionada por las entidades públicas, hasta hace poco tiempo la acumulaba para su uso exclusivo, ahora la produce con el fin de ponerla a disposición de los ciudadanos. Las entidades públicas han pasado por una transformación en cuanto a la forma de manejar la información como resultado del uso de las Tecnologías de la Información y de las Comunicaciones, lo cual se ha visto favorecido por la creciente demanda de información confiable por parte de los ciudadanos y la obligación ética/legal de mayor transparencia en la gestión de los recursos públicos.

La obligación ética/legal, más que la posibilidad de ofrecer los datos públicos abiertos, convierte esa información en un activo abundante y económico. Esa versatilidad de la información supone una modificación de la definición tradicional de documento y dibuja una clara diferencia entre los conceptos de documentación e información.[20]

Ejemplo de las categorías a utilizarse para clasificar la información se refiere a Economía, Historias, Ciencia y Tecnología, entre otras.

---

[20] https://redc.revistas.csic.es/index.php/redc/article/view/805/968
DEL ACCESO A LA REUTILIZACIÓN, DEL DATO AL DOCUMENTO: UNA VISIÓN CONCEPTUAL DE LA INFORMACIÓN PÚBLICA.

Concepción Mendo*, L. Fernando Ramos*, Rosario Arquero*, Félix Del Valle-Gastaminza*, Iuliana Botezán*, Rodrigo Sánchez*, Carlos Tejada*, Jaime L. Peón*, Silvia Cobo*, Andrea Sala*

* Facultad de Ciencias de la Documentación, Universidad Complutense de Madrid. España.

ADC-3-009.18.1. Es deber del titular de cada entidad u organismo público sujeto a la presente Norma Básica de Control Interno establecer un Comité de Administración de Medios Web (CAMWEB) de acuerdo con las directrices establecidas en las NORTIC A2 y A3 de manera que la responsabilidad por la gestión de los distintos tipos de información se realice de acuerdo con los estándares establecidos.

ADC-3-009.18.2. las entidades públicas deben acogerse a las directrices estipuladas en la sección 3.01 de la NORTIC A3:2014, que se refiere a la información reutilizable, la cual debe identificarse de acuerdo con las categorías establecidas, de manera que facilite su localización en la web.

ADC-3-009.18.3. Las entidades públicas deben seleccionar cuidadosamente las informaciones que han de subir en los portales de acuerdo con las leyes y normas que rigen este proceso, tomando como base las directrices contenidas en la sección 3.02 de la NORTIC A3:2014 se trazan las pautas sobre el proceso de selección de la información que debe subirse a los portales de acuerdo con las leyes y normas que rigen este proceso.

ADC-3-009.18.3.20. Declaración Técnica. Un Ejemplo de esas directivas es la que establece: "Una vez determinada la información apta para la reutilización, entonces debe publicarse los documentos primarios de dichas informaciones, a fin de mantener la integridad de lo que se quiere mostrar".

Riesgos Inherentes:

1. Desconexión de la estructura TIC del plan estratégico institucional
2. Estructura de gestión TIC desactualizada.
3. Retraso en la respuesta requerida de asistencia técnica.
4. Accesos no autorizados a las TIC.
5. Deficiente protección de equipos y software.
6. Retraso en el acceso de la información en el sistema.

7. Interrupción en la continuidad del servicio y afectación de la integridad de la información.
8. Información desactualizada.
9. Incumplimiento regulatorio en cuanto a la transparencia.
10. Limitación de acceso a personas con discapacidad.
11. Insuficiencia de la información de datos abiertos.
12. Falta de calidad de la información.

CAPITULO 3.

3.1 Procedimientos Específicos de Control Interno para la Gestión de las TIC

ADC-3-009.19. Controles de datos fuente, de operación y de salida. El titular y los responsables de las unidades de las TIC, deben establecer controles para la protección de los datos fuente de origen, operaciones de proceso y salida de información, con el propósito de resguardar la integridad de la información procesada por la entidad.

ADC-3-009.19.1. Las entidades públicas deben designar a los usuarios responsables de la protección de los datos fuentes. Asimismo, se deben establecer políticas claras para la creación de las claves de acceso para los niveles de usuarios: a) el primer nivel solo tiene acceso a la opción de consulta de datos, b) el segundo nivel puede hacer captura, modificar y consultar datos, y c) el tercer nivel puede capturar, modifica, consulta y además puede suprimir los datos.

ADC-3-009.19.2. Las entidades públicas deben establecer controles para la operación de los equipos de cómputo, los cuales deben hacerse a través de procedimientos estandarizados y formales, los cuales deben describir de manera detallada las actividades a realizar, deben actualizarse periódicamente e incluir los niveles efectivos de utilización de los equipos. Esas políticas deben incluir controles tales como:

a) Una supervisión directa sobre todo el personal del centro de cómputo, especialmente los operadores;
b) Los supervisores deben ser los responsables de establecer las prioridades y abrir el programa de trabajo diario;
c) Cada operador debe firmar la bitácora de operación de la computadora cuando se inicia y cuando termina cada turno y el supervisor debe pedir los reportes de las operaciones realizadas en su área cada día;
d) El operador debe de ser el único que pueda operar la computadora;
e) Se debe tener un control sobre los operadores cuando estos tengan accesos a cintas, discos, programas o documentos importantes;
f) El acceso al área de computadoras deberá estar restringido.[21]
g) El auditor debe revisar los reportes periódicamente;

ADC-3-009.19.3. Las entidades públicas y los responsables de las TIC, con el propósito de asegurar la integridad de la información, deben tener especial cuidado en los aspectos, tales como: Copias de la información en otras locaciones, designación de las personas responsables de entregar el documento de salida y las personas que reciben la información.

ADC-3-009.19.4. Es responsabilidad del titular de la entidad en coordinación con el/la responsable de la TIC, establecer los controles de datos fuente, los controles de operación y los controles de seguridad que garanticen la integridad y adecuado uso de la información generada por los sistemas que apoyan las operaciones de la entidad.

Riesgos inherentes:

1. Ausencia de políticas y procedimiento (controles) de protección de datos fuentes.
2. Ausencia de políticas y procedimiento (controles) sobre la responsabilidad de la operación en los equipos de cómputo.
3. Ausencia de políticas y procedimiento (controles) relacionada con los responsables de la salida de salida de la información.

[21] https://tareasuniversitarias.com/controles-de-operacion-de-la-computadora-en-auditoria-informatica.html

ADC-3-009.20. Mantenimiento de equipos de computación. El titular de cada entidad u organismo público y los responsables directos de la gestión de la Tecnología de Información y Comunicación deben establecer controles para el mantenimiento preventivo y correctivo para los dispositivos y equipos de computación, abordando los aspectos relacionado con la seguridad tanto lógica como física que permitan optimizar su rendimiento y la seguridad de la información.

ADC-3-009.20.21. Declaración Técnica. El objetivo del mantenimiento que debe darse a los dispositivos es el de optimizar su funcionamiento y dar respuesta a los riesgos de obsolescencia de los mismos, proteger la información que en ellos reside y asegurar la continuidad en los servicios que ofrece la entidad a los ciudadanos.

El mantenimiento correctivo es el que da respuesta a situaciones o fallas en los equipos por circunstancias no previstas. Se refiere a fallas en los equipos que requieren de solución inmediata. De no disponerse de equipos de respuesta a lo interno de la entidad, se debe contar con un directorio de especialistas que pueda resolver la emergencia en el menor tiempo posible.

ADC-3-009.20.1. Las entidades y responsables de las TIC, deben establecer políticas y procedimientos para el mantenimiento, que integren controles preventivos y controles correctivos, para garantizar razonablemente la seguridad, tanto de los software como de los equipos y la información que generan los sistemas.

ADC-3-009.20.2. El titular de la entidad en coordinación con el responsable de la TIC, deben establecer políticas y los controles internos sobre el mantenimiento de los equipos de computación, debido a que una apropiada implementación asegura el funcionamiento general y rendimiento de los mismos.

ADC-3-009.20.3. La entidad, principalmente los responsables de las TIC, deben elaborar y ejecutar un plan de mantenimiento que debe involucrar la observación de tres elementos: a) Un programa de limpieza con la frecuencia o período en que se debe ejecutar (semanal, quincenal o mensual) de la sala de máquinas y demás equipos que requieren mantenimiento

preventivo; b) El acceso inmediato al mantenimiento correctivo; y, c) la protección de los dispositivos de almacenamiento.

ADC-3-009.20.4. Las entidades públicas deben llevar estadísticas para registrar los eventos que se generan para ajustar lo mejor posible el mantenimiento preventivo. [22]

ADC-3-009.20.4.22. Declaración Técnica. El mantenimiento preventivo por lo general es parte de las actividades de control para minimizar las consecuencias que obligan a dar mantenimiento correctivo. Las actividades de prevención se programan para ser ejecutadas en períodos cortos.

Riesgos Inherentes:

1. No disponer de equipos de respuesta a lo interno de la entidad para mantenimiento de los equipos.
2. no disponer de equipos de respuesta a lo externo de la entidad para mantenimiento de los equipos.
3. Falta de controles sobre el cuidado de los equipos.
4. Ausencia de políticas y procedimientos para el mantenimiento preventivo de los equipos de cómputo.

ADC-3-009.21. Seguridad en los programas y datos. El titular de la entidad u organismo público y el responsable de la gestión de las TIC deben establecer políticas y procedimientos, así como controles claves que garanticen la seguridad en los programas y datos del sistema basado en TIC de manera que se conserve la integridad y exactitud de la información procesada por la entidad, así como la protección de los dispositivos de computación.

ADC-3-009.21.23. Declaración Técnica. Las entidades tanto públicas como privadas se empeñan en tomar las medidas más adecuadas que les permitan garantizar la protección de sus Sistemas de Información y Comunicación; esto se hace partiendo desde el proceso de desarrollo y adquisición de las aplicaciones o programas (software) hasta el proceso mismo

[22] Normas de Control Interno de la República de Panamá.

de la instalación de los equipos (hardware) que se utilizan para el procesamiento de la información.

La seguridad en sistemas informáticos se refiere a la capacidad de un sistema para proteger sus recursos, datos y funcionalidades contra amenazas internas y externas, y garantizar la integridad, disponibilidad y confidencialidad de la información.

Desde el punto de vista operativo, la implementación del sistema de seguridad se desarrolla entendiendo dos tipos: Seguridad Lógica y Seguridad Física, respectivamente.[23]

La seguridad lógica incluye los controles orientados a la protección del sistema, su instalación y operatividad.

El tipo de seguridad física se refiere a las actividades de control y medidas adoptadas para gestionar los riesgos de interrupciones prolongadas del servicio de procesamiento de datos por causa de daños o desperfectos en los equipos, accidentes, incendios y toda serie de circunstancias que haga peligrar el funcionamiento del sistema. Este tipo de seguridad se puede establecer asignando un personal de vigilancia, colocación de alarmas, extintores y cualquier otro equipo que pueda evitar un imprevisto, así como la adquisición de equipos para la protección del computador principal ante la ausencia o falla en la energía eléctrica.

ADC-3-009.21.1. Las entidades públicas deben establecer controles integrados relacionados con los siguientes aspectos:

a) restricciones de acceso a los archivos y programas para los programadores, analistas u operadores;

b) claves de acceso (password) por usuario para evitar la violación a la confidencialidad de la información;

c) copias de respaldo de los datos procesados en forma diaria, semanal o mensual (backups), y descentralizar su ubicación para evitar pérdida de la información;

[23] Normas de Control Interno de la República de Panamá.

d) crear un sistema de monitoreo a través de un programa de computación (software), desde el cual se pueda tener control de todas las actividades; y

e) mantener programas antivirus actualizados para evitar el deterioro de la información, entre otros controles.

ADC-3-009.21.2. Es responsabilidad de las unidades encargadas de las TIC junto con el titular de la entidad, seleccionar los mecanismos y las actividades de control de seguridad de los programas y datos del sistema, de manera que se garantice la integridad, veracidad y acceso a las informaciones que se procesan internamente.

Riesgos Inherentes:

1. Ausencia de políticas y procedimientos para la protección de software y programas.
2. Ausencia de políticas y procedimientos para la protección y mantenimiento de los equipos.

ADC-3-009.22. Plan de contingencias. El titular y el responsable de las TIC en las entidades públicas, deben elaborar el Plan de Contingencias, que establezca las políticas y procedimientos a utilizarse para evitar interrupciones en la operación del sistema de cómputo.

ADC-3-009.22.1. Las entidades públicas, para responder a las situaciones imprevistas, deben establecer políticas y procedimientos que han de cumplir las unidades responsables de las TIC a la hora de responder ante un evento causado por hecho fortuito o de fuerza mayor.

ADC-3-009.22.2. Las políticas deben estar integradas en un documento de carácter confidencial, para evitar la interrupción del funcionamiento del sistema de cómputo. Al aplicar el plan, el sistema debe operar en un nivel aceptable, cuando las facilidades de procesamiento de información no están disponibles.

ADC-3-009.22.3. Las entidades deben asegurarse de que, además de que todos los elementos del plan, conforme a la necesidad de su aplicación, se consideren por separados, deben articularse para que pueda operar de forma integral como sistema.

ADC-3-009.22.4. Las entidades deben asegurarse en todo momento de que la documentación esté actualizada tanto como sea posible y de acuerdo con las necesidades detectadas en el proceso de seguimiento a la ejecución del mismo, incorporando las últimas modificaciones. Igualmente, se debe contemplar la necesidad, si fuere el caso, de suscribir acuerdo con otra institución que disponga de configuración informática similar a la de la entidad para poder utilizarla en caso de desastre total.[24]

ADC-3-009.22.5. La entidad debe tomar en consideración a la hora de poner en funcionamiento el plan, de que el mismo debe ejecutarse sobre la base de que la emergencia existe y tienen que utilizarse respaldos posiblemente de otras instituciones. Los supuestos que se utilicen para la simulación, deben referirse a los hechos que ocurrirían en caso de una emergencia real, tomando en cuenta todos sus detalles.

ADC-3-009.22.6. Aunque se haya guardado copia del plan de contingencias aprobado fuera de las instalaciones donde está el área de informática, la entidad y el responsable de la TIC, deben entregar copias al personal responsable de su operación.

ADC-3-009.22.7. Las entidades públicas y los responsables de las TIC, deben realizar revisiones del plan, siempre que se hayan efectuado cambios en el personal, en la configuración de los equipos, en los programas y en las redes y comunicaciones. El personal responsable de su operación debe estar en capacidad de ejecutar el plan de contingencia y conocer los cambios realizados.

ADC-3-009.22.8. El titular y demás servidores responsables son los responsables de elaborar, mantener y actualizar el Plan de Contingencias, de manera que se pueda asegurar

[24] Normas de Control Interno para las TIC de la República de Panamá.

la correcta operación de los sistemas de información que precisa la entidad para desarrollar sus planes y proyectos.

Riesgos Inherentes:

1. No contar con un plan de contingencia revisado y actualizado.
2. Que no se entregue copia del plan de contingencia al personal responsable.
3. Falta de competencia del personal responsable de ejecución del plan.
4. No contar con revisión del plan luego de cambios en el personal.

ADC-3-009.23. Aplicación de técnicas de intranet. De acuerdo con los planes, programas y necesidades propias de su misión, las entidades públicas deben implementar las técnicas de Intranet, siempre con el propósito de mejorar el control interno e incrementar la eficiencia de las comunicaciones internas, previa evaluación del costo-beneficio que reportaría su aplicación.

ADC-3-009.23.24. Declaración Técnica. La Intranet es un sitio lógico privado o un conjunto de sitios que se configuran para uso exclusivo de una organización. El internet es un espacio abierto, a través del cual un usuario puede conectarse con millones de personas. La Intranet viene siendo una versión cerrada que sólo conecta al usuario con dispositivos que han sido seleccionados de manera anticipada.

En el Internet la información circula abiertamente para todo público; mientras que en la Intranet la información está disponible solo a usuarios específicos y se retienen los derechos de propiedad privada y al mismo tiempo se establecen niveles de seguridad para proteger información específica que es compartida entre múltiples usuarios dentro de una entidad.

ADC-3-009.23.1. Las entidades públicas y los responsables de las TIC, al iniciar un proceso de desarrollo de la Intranet deben seguir una serie de pautas y estándares que le permitan asegurar su funcionalidad con el mayor nivel de eficiencia posible. Entre las pautas y estándares que deben seguir se encuentran, entre otras:

a) instalación del protocolo de comunicaciones TCP/IP;

b) seleccionar un servidor que ofrezca la facilidad de empaquetado, seguridad y enlaces a la base de datos corporativa;
c) realizar reuniones con los funcionarios de más alto nivel para determinar qué información debe entrar a la intranet;
d) tener conocimiento claro del programa (software) de manipulación de la información utilizado en Internet;
e) conexión a una base de datos, a fin de organizar mejor la documentación disponible en el Servidor Web.

ADC-3-009.23.2. Es responsabilidad del titular de la entidad autorizar la implementación de Intranet, previa evaluación del costo/beneficio que reportaría para su organización su puesta en funcionamiento.

ADC-3-009.24. Gestión optima de programas (software) adquirido a la medida por las entidades públicas. El titular de la entidad debe establecer políticas y procedimientos relacionados con los programas de computación (software) diseñado y desarrollado a la medida de la entidad, tanto los programas contratados con terceros como los programas diseñados por la propia entidad, con el propósito de que los mismos sean registrados a nombre de la entidad pública o del Estado dominicano.

ADC-3-009.24.1. Las entidades deben asegurarse cuando contratan los servicios de terceros para desarrollar e implementar programas (software) a la medida, para la ejecución de actividades y operaciones, que los derechos sobre tales programas o aplicaciones que le correspondan a esta, de manera que se pueda impedir que puedan ser re-utilizado indebidamente por el proveedor original.

ADC-3-009.24.2. Es deber del titular de la entidad, de acuerdo con las disposiciones establecidas por la OGTIC, en su condición de órgano rector de la TIC, aprobar las políticas y procedimientos que permitan compartir con otras entidades públicas, el uso del programa (software) adquirido a la medida para sus actividades, con el propósito de evitar que el Estado incurra en gastos mayores por la adquisición repetitiva de aplicaciones informáticas.

Riesgos Inherentes:

1. No contar con políticas para el registro de los programas desarrollados a la medida para la entidad de derecho de propiedad estatal de los sistemas y dispositivos.
2. No existencia de registro de propiedad de los programas existentes.
3. No existencia de políticas que permitan compartir programas con otras entidades públicas.

Bibliografía

1. NORTIC A1:2014, Norma General sobre el Uso e Implementación de las Tecnologías de la Información y Comunicación en el Estado Dominicano.

2. NORTIC A3:2014, Norma sobre Publicación de Datos Abiertos del Gobierno Dominicano.

3. NORTIC A6:2016 Norma sobre el Desarrollo y Gestión del Software en el Estado Dominicano.

4. NORTIC A7:2016 Norma para la Seguridad de las Tecnologías de la Información y Comunicación en el Estado Dominicano.

5. NORTIC A5:2019 Norma la Prestación y Automatización de los Servicios Públicos sobre del Estado Dominicano.

6. NORTIC A2:2021, Norma Para el Desarrollo y Gestión de los Portales Web y la Transparencia de los Organismos del Estado Dominicano.

7. NORTIC A2:2023 Norma Para el Desarrollo y Gestión de los Portales Web y la Transparencia de los Organismos del Estado Dominicano.

8. COBIT 5. A Business Framework for the Governance an Management of Enterprice IT. ISACA. (2012).

9. COBIT 2019. A Business Framework for the Governance an Management of Enterprice IT. ISACA. (2019).

10. Normas Generales de Control Interno para el Sector Público Nacional, Sindicatura General de la Nación. Noviembre 2014. República de Argentina.

11. Normas de Control Interno para Tecnología de la Información, Sindicatura General de la Nación. Noviembre 2021. República de Argentina.

12. Resolución de Contraloría General N° 320-2006-CG, Normas de Control Interno, Contraloría General de la República. República del Perú. Octubre 2006.

13. Normas de Control Interno Gubernamental para la República de Panamá.

14. Modelo de Gobierno y Gestión de TI, basado en COBIT 2019 e ITIL 4, para la Universidad Católica de Cuenca, República de Ecuador.

15. Marcos de control y estándares para el gobierno de tecnologías de información (TI). Francisco Arnaldo Vargas-Bermúdez, Grupo de Investigación Gisdytel Universidad de Boyacá, Colombia.

16. Gobierno de las TI para universidades, Antonio Fernández Martínez, Universidad de Almería Faraón Llorens Largo, Universidad de Alicante.

17. Gestión de Servicios de Tecnologías de la Información, Information Technology Services Management, Cristian Mera Macías y Daniela Vera Vélez.

18. Aplicación de las nuevas tecnologías en la Administración pública, LUIS PA RDO, Fecha recepción: 14/04/2011 Fecha aceptación: 12/10/2011, https://accid.org/wp-content/uploads/

19. El Decreto 615-07, que instruye a la OPTIC a coordinar el procedimiento para la elaboración de los inventarios respecto a los programas incorporados a las computadoras y su licenciamiento.

20. https://www.unibarranquilla.edu.co/docs/Plan-de-Continuidad-de-Servicios-de-TI-ITSA-v1.pdf/Plan de Continuidad de Servicios de TI Proceso de Tecnologías y Sistemas de Información.

21. https://www.freshworks.com/freshservice/es/a-roadmap-to-modernise-it-service-and-operations-management-blog/ FreshserviceBlog.

22. https://www.ninjaone.com/es/blog/planificacion-estrategica-ejemplos/