

NORTIC
A7
2 0 2 5

» **NORMA PARA LA
ADMINISTRACIÓN DE
LA SEGURIDAD DE LA
INFORMACIÓN**

Santo Domingo, República Dominicana
Diciembre 2025.



CNCS ogtic 

NORTIC

A7

2 0 2 5

**NORMA PARA LA
ADMINISTRACIÓN DE
LA SEGURIDAD DE LA
INFORMACIÓN**

**SANTO DOMINGO, REPÚBLICA DOMINICANA
DICIEMBRE 2025.**

**NORTIC A7:2025 > NORMA PARA LA ADMINISTRACIÓN DE LA
SEGURIDAD DE LA INFORMACIÓN**

Edición: 2^{da}

**Oficina Gubernamental de Tecnologías de la Información y Comunicación
(OGTIC)**

Dirección de Transformación Digital Gubernamental
Departamento de Normas y Estándares

Centro Nacional de Ciberseguridad (CNCS)

Año de publicación: 2025

Versión 2.0

Diagramado y diseñado por la Dirección de Innovación, OGTIC.

CONTENIDO

PRÓLOGO.....	vii
INTRODUCCIÓN.....	ix
ANTECEDENTES.....	xi
MARCO LEGAL.....	xiii
CAPÍTULO I DIRECTRICES GENERALES.....	17
Sección 1.01. Objeto y ámbito de aplicación.....	17
Sección 1.02. Objetivos.....	18
Sección 1.03. Referencias normativas e informativas.....	19
Sección 1.04. Términos y definiciones	20
Sección 1.05. Reglas de interpretación y convenciones.....	24
CAPÍTULO II GOBERNANZA INSTITUCIONAL Y DE LA INFORMACIÓN....	27
Sección 2.01. Liderazgo y compromiso de la alta dirección (MAE).....	27
Sección 2.02. Estructura organizativa y roles de seguridad.....	28
Sección 2.03. Comité de implementación y gestión estándares TIC.....	29
Sección 2.04. Marco de políticas de seguridad de la información.....	32
CAPÍTULO III MODELO DE MADUREZ Y APLICABILIDAD.....	39
Sección 3.01. Definición de los niveles de madurez.....	39
Sección 3.02. Asignación del Nivel de Madurez Objetivo (MOO).....	44
Sección 3.03. Aplicabilidad de requisitos por nivel.....	45
CAPÍTULO IV PLANIFICACIÓN Y GESTIÓN DE LA SEGURIDAD.....	51
Sección 4.01. Contexto organizacional y partes interesadas.....	51
Sección 4.02. Marco de gestión de riesgos de seguridad.....	54
Sección 4.03. Declaración de Aplicabilidad (SoA).....	56
Sección 4.04. Seguridad en la cadena de suministro.....	59
Sección 4.05. Seguridad en la gestión de recursos humanos.....	62

CONT. CONTENIDO

CAPÍTULO V | EVALUACIÓN DEL DESEMPEÑO Y MEJORA DEL SISTEMA.....69

Sección 5.01. Monitoreo y medición del desempeño (KPIs).....69

Sección 5.02. Auditoría interna del SASI.....71

Sección 5.03. Revisión por la dirección.....73

Sección 5.04. Gestión de hallazgos y acciones de mejora.....75

BIBLIOGRAFÍA.....78

ABREVIATURAS Y ACRÓNIMOS.....79

ANEXOS.....80

Anexo A: Matriz de controles por nivel de madurez.....80

EQUIPO DE TRABAJO.....92

PRÓLOGO



En la era digital, la soberanía de la información y la confianza de los ciudadanos en sus instituciones dependen directamente de la capacidad del Estado para protegerla. Cada avance tecnológico es una oportunidad para servir mejor al país, pero también introduce riesgos que exigen un marco de gobierno claro, una gestión estructurada y una supervisión diligente de la seguridad.

Conscientes de esta realidad, la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC) y el Centro Nacional de Ciberseguridad (CNCS) presentamos de manera conjunta la NORTIC A7, la norma marco para la Administración del Sistema de Seguridad de la Información (SASI) en el sector público dominicano. Este es el pilar estratégico que dota a cada institución del Estado de una estructura de gobernanza para la seguridad.

Esta norma tiene un objetivo claro: establecer un sistema de gestión formal, alineado con estándares internacionales como la ISO 27001, que permita dirigir, supervisar y mejorar de forma continua la postura de seguridad de cada organismo. La NORTIC A7 define las políticas, los roles y responsabilidades, el marco de gestión de riesgos y los mecanismos de rendición de cuentas que son indispensables para una ciberdefensa eficaz.

Este estándar es el eje central del ecosistema normativo de seguridad. Establece los mandatos de alto nivel bajo los cuales operan las demás normas, y se materializa a través de los controles técnicos de la **NORTIC A8 - Norma General de Ciberseguridad** y las metodologías de la **NORTIC A9 - Norma para la Gestión de Riesgos Tecnológicos y Continuidad Operativa**. Juntas, aseguran que la estrategia de seguridad (A7) se traduzca en una defensa activa (A8) y una resiliencia operativa (A9).

La seguridad de la información es una responsabilidad indelegable de la alta dirección, no solo de la tecnología. Las autoridades deben garantizar el cumplimiento de esta norma, asumiendo el liderazgo del programa de seguridad como un objetivo estratégico de toda la administración pública.

Reafirmamos así nuestro compromiso unificado con una arquitectura digital gubernamental segura y gobernada. La NORTIC A7 es el instrumento rector del Estado para garantizar que la transformación digital de la República Dominicana se construya sobre cimientos de confianza y protección.

Edgar Batista Carrasco

Director general

*Oficina Gubernamental de
Tecnologías de la Información y
Comunicación (OGTIC)*

Carlos Leonardo

Director ejecutivo

*Centro Nacional de Ciberseguridad
(CNCS)*



NORTIC A7:2025

Norma para la Administración de
la Seguridad de la Información

INTRODUCCIÓN



La Norma para la Administración de la Seguridad de la Información, conocida como NORTIC A7, establece el Sistema de Administración de la Seguridad de la Información (SASI) y el marco de gobernanza que deben seguir los organismos gubernamentales. Su objetivo es asegurar que la seguridad sea una responsabilidad estratégica de la alta dirección, proporcionando la estructura formal para que los controles técnicos y las metodologías del ecosistema de seguridad del Estado se implementen de forma coherente, medible y adaptativa.

Esta normativa se articula en torno al ciclo de vida de un sistema de gestión. El primer pilar se enfoca en la **Gobernanza Institucional**, donde se establecen los requisitos de liderazgo y compromiso de la Máxima Autoridad Ejecutiva (MAE), la estructura de roles y responsabilidades de seguridad, y la obligación de contar con un conjunto de políticas formales que rijan la clasificación, el manejo, la retención y la disposición segura de la información.

El segundo y más innovador pilar de la norma introduce un **Modelo de Madurez**. Este define un marco escalonado que permite una implementación progresiva y adaptativa de los requisitos de seguridad, basándose en la capacidad y criticidad de cada organismo.



Este modelo funciona como el mecanismo de gobernanza central para la aplicación de todo el ecosistema de normas, estableciendo un Nivel de Madurez Objetivo (MOO) para cada institución y definiendo qué controles de las NORTIC A8 y A9 son aplicables en cada nivel.

Basado en el nivel de madurez asignado, la norma detalla la fase de **Planificación y Gestión de la Seguridad**. Aquí se exige que la planificación sea basada en los resultados del análisis de riesgos (conforme a la NORTIC A9), se formaliza la creación de la Declaración de Aplicabilidad (SoA) como entregable clave, y se establecen los requisitos de seguridad en la gestión de los recursos humanos.

Finalmente, este documento define los requisitos para la **Evaluación del Desempeño y la Mejora del Sistema**. Este pilar cierra el ciclo de gestión, detallando los procedimientos para el monitoreo de indicadores (KPIs), la realización de auditorías internas, la revisión formal por la dirección y la gestión de los hallazgos, asegurando que el SASI sea un sistema vivo que se mide, se revisa y se adapta continuamente al entorno.



ANTECEDENTES



La Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC) es el organismo del Estado dominicano responsable de la estandarización, fomento e implementación del uso de las tecnologías de la información y comunicación (TIC) en la administración pública. Su rol y funciones, establecidos originalmente en el decreto no. 1090-04 y actualizados mediante el decreto no. 54-21, le confieren el mandato de garantizar que la transformación digital del país se realice de manera eficiente, transparente y segura, promoviendo la compatibilidad, interoperabilidad y estandarización en materia tecnológica.

Para cumplir con dicha responsabilidad, la OGTIC, a través de su departamento de normas y estándares, desarrolla y mantiene el marco normativo de TIC y gobierno digital de la República Dominicana. El componente central de este marco son las normas de tecnologías de la información y comunicación (NORTIC), un conjunto de estándares de cumplimiento obligatorio creados desde el año 2013. El propósito fundamental de las NORTIC es sistematizar y auditar la correcta implementación de las TIC, estableciendo un ciclo de mejora continua en los procesos gubernamentales y asegurando la prestación de servicios de calidad y confianza para la ciudadanía.



En los inicios de este marco normativo, los lineamientos sobre la protección de los activos de información del Estado se consolidaron en una única y robusta norma: la Norma sobre la seguridad de las tecnologías de la información y comunicación en el Estado dominicano, conocida formalmente como NORTIC A7. Dicho estándar funcionó como el pilar fundamental de la seguridad, abarcando de forma integral desde los controles técnicos de ciberseguridad hasta la planificación estratégica de la continuidad y la gestión de riesgos. Durante años, fue la guía principal para que las instituciones construyeran sus bases en materia de seguridad.

Sin embargo, la evolución del entorno digital y la creciente complejidad de los riesgos tecnológicos motivaron una especialización estratégica del marco de seguridad. En consecuencia, la NORTIC A7 original fue reestructurada para dar paso a un ecosistema de normas interconectadas. La presente **NORTIC A7 – Norma para la Administración de la Seguridad de la Información**, nace de esta evolución para servir como la **norma marco o rectora**. Su propósito ya no es detallar controles, sino establecer el Sistema de Administración de la Seguridad de la Información (SASI), definiendo el marco de gobernanza, el liderazgo de la alta dirección y el modelo de madurez que regirá la implementación de todo el ecosistema de seguridad del Estado.



La presente normativa se sustenta en el siguiente conjunto de leyes y decretos que establecen los derechos fundamentales sobre la información, las responsabilidades de la administración pública y el mandato de la OGTIC como entidad normalizadora.

Fundamento constitucional y derechos fundamentales

- 1. Constitución de la República Dominicana (proclamada en 2015):** El artículo 44 establece el derecho a la intimidad y la protección de datos personales. La NORTIC A7 es el instrumento de gobernanza que establece el mandato y la responsabilidad de la alta dirección para crear el sistema de gestión y las políticas necesarias para cumplir con este mandato constitucional.
- 2. Ley 200-04 sobre Libre Acceso a la Información Pública y su Reglamento de Aplicación (Decreto 130-05):** Este marco legal define la existencia de información pública, pero también la clasificada y reservada. La NORTIC A7 responde directamente a esta ley al exigir el establecimiento de una Política de Clasificación y Manejo de la Información, un pilar fundamental de la gobernanza de datos.
- 3. Ley 172-13 sobre Protección Integral de los Datos Personales:** Regula el tratamiento de datos personales y exige la implementación de medidas de seguridad. La NORTIC A7 establece la obligación de



crear el marco de políticas, roles y responsabilidades para asegurar que esas medidas se implementen y supervisen de manera efectiva.

4. **Ley 107-13 sobre los Derechos de las Personas en sus Relaciones con la Administración Pública:** Establece el derecho a una buena administración. La NORTIC A7 contribuye a este derecho al asegurar que la seguridad de la información sea un componente integral de la gestión estratégica y la toma de decisiones de la administración.
5. **Decreto 130-05 que aprueba el reglamento de la ley general de libre acceso a la información pública:** Si bien promueve el acceso, también implica la responsabilidad de proteger la información y asegurar la disponibilidad de los sistemas que la entregan, un pilar de la continuidad.

Marco legal de estructura, seguridad y tecnología

6. **Ley 53-07 contra crímenes y delitos de alta tecnología:** Protege los sistemas de información contra actos ilícitos. La NORTIC A7 establece el marco de gobernanza y la responsabilidad de la dirección para asegurar que se implementen los controles técnicos necesarios (detallados en la NORTIC A8) para prevenir estos delitos.
7. **Decreto 313-22 (Estrategia Nacional de Ciberseguridad), Decreto 685-22 (Madurez Cibernética) y Decreto 612-24 (Competencias en Ciberseguridad):** Este conjunto de decretos define la ciberseguridad como un tema de interés nacional. La NORTIC A7 es el instrumento de gobernanza principal para que las instituciones cumplan con estos mandatos, traduciendo la estrategia nacional en un sistema de gestión de seguridad aplicable.
8. **Resolución núm. 342-2024 del Ministerio de Administración Pública (MAP):** Actualiza los Modelos de Estructura Organizativa para las Unidades de Ciberseguridad. La NORTIC A7 complementa y da cumplimiento a esta resolución al definir formalmente los roles de seguridad (como el CISO), establecer su línea de reporte directo

a la máxima autoridad y detallar sus responsabilidades dentro del marco de gobernanza institucional.

Mandatos de modernización y cumplimiento de las NORTIC

9. **Ley 1-12 sobre Estrategia Nacional de Desarrollo 2030:** Promueve el uso de las TIC para mejorar la gestión pública. La NORTIC A7 es fundamental para este objetivo, al proveer el marco de gobierno necesario para que la digitalización del Estado se realice de forma segura y gestionada.
10. **Ley 167-21 sobre Mejora Regulatoria y Simplificación de Trámites:** Obliga al uso de tecnologías seguras. La NORTIC A7 establece la responsabilidad de la alta dirección de asegurar que la seguridad sea un criterio de diseño en la simplificación de trámites.
11. **Decreto 1090-04 y Decreto 54-21:** Crean y transforman la OPTIC en OGTIC, otorgándole la responsabilidad de velar por la seguridad y privacidad de la información. La NORTIC A7 es la herramienta de gobernanza con la que la OGTIC ejerce este mandato de supervisión.
12. **Decreto 229-07 sobre la implementación del gobierno electrónico:** Refuerza la obligación de las instituciones de adoptar las NORTIC para garantizar la seguridad en la digitalización de los procesos.
13. **Decreto 92-22 que establece el Marco Nacional de Interoperabilidad Gubernamental:** Define la interoperabilidad, la cual debe ser segura. La NORTIC A7 exige las políticas y el marco de supervisión para garantizar que el intercambio de información entre sistemas sea seguro.
14. **Decreto 709-07 y Decreto 707-22 (Programa Gobierno Eficiente - Burocracia Cero):** Instruyen de forma explícita a toda la administración pública a adoptar y cumplir las NORTIC. Estos decretos constituyen la base jurídica de la obligatoriedad de la presente norma como el estándar rector para la administración de la seguridad.



DIRECTRICES GENERALES

Este capítulo establece el propósito, alcance y marco de referencia de la presente normativa. Define los objetivos, los términos clave y las reglas de interpretación que se aplicarán a lo largo de todo el documento para asegurar su correcta comprensión y aplicación.

Sección 1.01.

Objeto, ámbito de aplicación

Esta sección define el propósito fundamental de la norma, estableciendo su razón de ser y los resultados que persigue. Asimismo, delimita de manera precisa el universo de entidades que están sujetas a su cumplimiento obligatorio, así como aquellas para las cuales su adopción constituye una buena práctica recomendada.

Subsección 1.01.1.

Objeto

El objeto de esta norma es establecer el Sistema de Administración de la Seguridad de la Información (SASI) y el marco de gobernanza obligatorio que deben seguir los organismos del Estado Dominicano. Su propósito es asegurar que la seguridad sea una responsabilidad estratégica de la alta dirección y proporcionar la estructura formal para la implementación coherente y medible de todo el ecosistema de seguridad del Estado.

- (a) Las directrices de esta norma son de aplicación obligatoria para todos los organismos pertenecientes al Poder Ejecutivo, ya sean centralizados o descentralizados, así como las embajadas, consulados, misiones en el extranjero y municipios.
- (i) Entre los organismos centralizados se encuentran los Ministerios y sus dependencias, viceministerios, organismos adscritos a la Presidencia de la República, consejos y organismos asesores, direcciones generales, oficinas nacionales, procuradurías fiscales, escuelas públicas, hospitales públicos, bibliotecas y museos.
 - (ii) Entre los organismos descentralizados se encuentran las instituciones financieras y no financieras, organismos reguladores, instituciones de la seguridad social y empresas públicas.
- (b) Los organismos pertenecientes al Poder Legislativo, al Poder Judicial y los clasificados como “Organismos Especiales” por el Ministerio de Administración Pública (MAP), podrán adoptar los estándares de esta norma como un modelo de buenas prácticas.

Sección 1.02.**Objetivos**

La implementación de esta norma persigue los siguientes objetivos principales para todos los organismos del Estado:

- **Establecer la Gobernanza de la Seguridad:** Definir la estructura de roles, responsabilidades y comités, asegurando que la Máxima Autoridad Ejecutiva (MAE) lidere y supervise el programa de seguridad.
- **Implementar un Sistema de Gestión basado en Riesgos:** Exigir la adopción de una metodología formal para la gestión

de riesgos que guíe todas las decisiones de seguridad y la creación de un marco de políticas.

- **Dirigir el Ecosistema de Controles:** Servir como la norma rectora que establece los mandatos para la implementación de los controles técnicos de la NORTIC A8 y las metodologías de la NORTIC A9.
- **Introducir un Modelo de Madurez Adaptativo:** Establecer un marco de implementación escalonada que permita a los organismos adoptar los requisitos de seguridad de forma progresiva, basándose en su capacidad, criticidad y el Nivel de Madurez Objetivo (MOO) asignado.
- **Fomentar una Cultura de Seguridad:** Promover la responsabilidad y la concienciación en materia de seguridad en todos los niveles de la organización.
- **Asegurar la Mejora Continua:** Establecer un ciclo de vida para el sistema de gestión que incluya monitoreo, auditorías y revisiones por la dirección, garantizando su adaptación y eficacia a largo plazo.

Sección 1.03.

Referencias normativas e informativas

Esta norma se fundamenta y complementa con lo establecido en la Constitución de la República, así como en las leyes, decretos y resoluciones vigentes que regulan la seguridad de la información, la estructura de la administración pública y la protección de datos en el Estado.

Asimismo, esta norma funciona como el eje central del ecosistema de seguridad del Estado. Establece los mandatos de gobernanza que son implementados a través de las siguientes normas especializadas:

- **NORTIC A8 – Norma General de Ciberseguridad:** Contiene

el catálogo de controles técnicos y operativos para la ciberdefensa, cuya implementación es dirigida y supervisada por el sistema de gestión que establece esta norma (NORTIC A7).

- **NORTICA9 – Norma para la Gestión de Riesgos Tecnológicos y Continuidad Operativa:** Contiene las metodologías detalladas para la gestión de riesgos y la continuidad, las cuales deben ser adoptadas conforme a las políticas y el programa exigidos por esta norma (NORTIC A7).

Para su elaboración, se han tomado como referencia y guía las buenas prácticas de estándares internacionales de gobernanza y gestión de la seguridad, principalmente:

- **ISO/IEC27001-Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de la seguridad de la información:** Estándar internacional que define el modelo para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI/SASI).
- **COBIT (Control Objectives for Information and Related Technologies):** Marco de referencia para el gobierno y la gestión de la información y la tecnología de la empresa.
- **NIST Cybersecurity Framework (CSF) 2.0:** Específicamente su función de Gobernar, que establece los componentes para un programa de ciberseguridad estratégico y supervisado.

Sección 1.04.

Términos y definiciones

- **Acuerdo de Nivel servicio (SLA):** Es un contrato formal que plasma los acuerdos entre un proveedor de servicio y el cliente, en donde se estipulan los requisitos y parámetros

que el proveedor se compromete a cumplir para mantener unos niveles de calidad de servicio.

- **Amenaza:** Es cualquier evento, acción o circunstancia que tiene el potencial de causar un daño a los activos de información, comprometiéndola confidencialidad, integridad o disponibilidad de los sistemas, datos o infraestructuras tecnológicas. Las amenazas pueden ser de origen interno o externo, intencionales o accidentales, y pueden afectar la Gestión de Riesgos Tecnológicos y Continuidad Operativa a través de vulnerabilidades existentes en el entorno tecnológico.
- **Análisis de Impacto al Negocio (BIA):** Proceso de análisis que permite identificar y evaluar el impacto potencial de una interrupción de los procesos críticos de negocio de un organismo, como consecuencia de un desastre, accidente o emergencia. Este análisis es la base para establecer las estrategias de recuperación y los requisitos de continuidad.
- **Áreas no seguras:** Hace referencia a lugares o espacios dentro del Organismo, que presentan riesgos potenciales para la seguridad, ya sea por condiciones ambientales, falta de medidas de seguridad, presencia de sustancias peligrosas, o por ser propensas a accidentes o incidentes de cualquier tipo.
- **Áreas seguras:** Hacen referencia a los lugares seguros dentro del organismo que los colaboradores y visitantes pueden transitar sin correr ningún peligro.
- **Centro de Comando:** Es el lugar desde el cual se dirigen las actividades de recuperación de las actividades críticas de las operaciones de un organismo luego de sufrir una catástrofe.
- **Centro de datos:** Es un área donde se concentran y operan los equipos que conforman la infraestructura TIC que utilizan

los organismos para administrar sus actividades y servicios.

- **Continuidad Operativa:** Capacidad estratégica y táctica de un organismo para continuar operando sus funciones críticas a un nivel predefinido y aceptable después de un evento disruptivo.
- **Disponibilidad:** Asegurar que la información esté accesible y utilizable por los usuarios autorizados cuando sea necesario.
- **Evento:** Cualquier hecho u ocurrencia observable en un sistema, red o activo o dispositivo tecnológico.
- **Gestión de Riesgo:** La gestión de riesgos es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales.
- **Hardware:** Se refiere a todas las partes físicas o tangibles de un sistema de información.
- **Incidente:** Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de la calidad de dicho servicio.
- **Integridad:** Garantizar que la información es precisa y completa, y que no ha sido alterada de manera no autorizada.
- **Inventario:** Es un registro organizado de los activos pertenecientes o bajo la responsabilidad de un organismo determinado.
- **Máxima Autoridad Ejecutiva (MAE):** Es la persona con el mayor nivel de jerarquía dentro de una institución pública. Es quien tiene la responsabilidad final de dirigir, supervisar y

tomar decisiones en nombre de la entidad.

- **Plan de Continuidad de Negocio (BCP):** Conjunto documentado de procedimientos y recursos para guiar a un organismo en la respuesta, recuperación, reanudación y restauración de sus procesos de negocio a un nivel predefinido, tras una interrupción.
- **Plan de Recuperación ante Desastres (DRP):** Componente del plan de continuidad enfocado específicamente en la recuperación de la infraestructura tecnológica y los sistemas de información críticos de un organismo después de un desastre o interrupción mayor.
- **Recuperación:** Conjunto de actividades y procesos para restaurar las capacidades, servicios y operaciones de un organismo a un estado funcional predefinido después de una interrupción.
- **Riesgo residual:** Refiere al riesgo que queda tras tomar todas las medidas preventivas de reducción de riesgos.
- **Riesgo tecnológico:** Riesgo de pérdida o daño a un organismo causado por la falla, el mal uso o la interrupción de sus sistemas, infraestructura o procesos de tecnología de la información.
- **Resiliencia:** La capacidad de un organismo para absorber y adaptarse a un entorno cambiante o a eventos disruptivos, con el fin de continuar cumpliendo sus objetivos.
- **RPO (Objetivo de Punto de Recuperación / Recovery Point Objective):** El punto máximo en el tiempo hasta el cual se pueden perder datos de un servicio tras una interrupción. Determina la frecuencia mínima de las copias de seguridad.
- **RTO (Objetivo de Tiempo de Recuperación / Recovery Time Objective):** El período de tiempo máximo tolerable

dentro del cual un proceso de negocio o servicio debe ser restaurado después de un desastre o interrupción para evitar consecuencias inaceptables.

- **Servicio esencial:** Todo servicio que resulte ser necesario para la seguridad nacional, defensa, relaciones exteriores, economía, salud, seguridad u orden público de República Dominicana.
- **Software:** Se conoce como software al equipo o soportes lógicos de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.
- **Vulnerabilidad:** Cualquier debilidad en un sistema de información, sus procedimientos de seguridad, su implementación o en sus controles internos, que podrían permitir la materialización de una amenaza.

Sección 1.05.

Reglas de interpretación y convenciones

- Toda directriz en este documento indicada con las palabras “debe” o “no debe” representa un requisito de cumplimiento obligatorio.
- Para los fines de esta norma, el término “organismo gubernamental” se utilizará indistintamente como “organismo” y se refiere a toda entidad descrita en el ámbito de aplicación.
- Para mantener la coherencia terminológica, esta Norma utilizará el término “Gestión de Riesgos” (en plural) para referirse a la disciplina y al proceso general.

- Para los fines de esta norma, los términos “Máxima Autoridad Ejecutiva (MAE)” y “Alta Dirección” se utilizarán para referirse al individuo o grupo de individuos con la máxima responsabilidad ejecutiva y de supervisión del organismo.
- Cuando en la normativa aparezca el término “activos”, este se refiere tanto a los activos de información como a los activos tecnológicos que los soportan.



GOBERNANZA INSTITUCIONAL Y DE LA INFORMACIÓN

Este capítulo establece los requisitos de liderazgo, estructura y políticas marco que la Máxima Autoridad Ejecutiva (MAE) debe implementar para gobernar la seguridad de la información como una función estratégica. Su propósito es asegurar un compromiso auditable desde el más alto nivel y sentar las bases para la protección de la información en todas sus formas a lo largo de su ciclo de vida.

Sección 2.01.

Liderazgo y compromiso de la alta dirección (MAE)

Esta sección norma la responsabilidad y participación de la Máxima Autoridad Ejecutiva (MAE) en el Sistema de Administración de Seguridad de la Información (SASI).

Subsección 2.01.1.

Asunción de la responsabilidad estratégica

- a) El organismo debe contar con una Política General de Seguridad de la Información, según lo establecido en la Sección 2.03.
- b) La MAE debe aprobar formalmente dicha política. La evidencia de esta aprobación será la firma del documento, constituyendo el mandato principal que establece el apoyo de la alta dirección para todas las iniciativas de seguridad.

Subsección 2.01.2.**Asignación y provisión de recursos**

- a) La MAE debe asegurar la provisión de los recursos adecuados y suficientes (financieros, humanos y tecnológicos) para establecer, implementar, mantener y mejorar continuamente el SASI.
- b) La asignación de recursos para el programa de seguridad debe estar formalmente documentada y reflejada en los planes operativos anuales y en la asignación presupuestaria del organismo, como evidencia auditable del compromiso.

Subsección 2.01.3.**Promoción de la Cultura de Seguridad**

- a) La MAE debe liderar y participar activamente en la promoción de una cultura donde la seguridad de la información sea una responsabilidad compartida en todos los niveles de la institución.
- b) Esta participación debe evidenciarse a través de comunicaciones periódicas dirigidas al personal, el respaldo a programas de concientización y otras actividades que refuercen la importancia estratégica de la seguridad.

Sección 2.02.**Estructura organizativa y roles de seguridad**

Esta sección establece los requisitos para definir una estructura de mando clara y documentar las responsabilidades de seguridad en toda la organización.

Subsección 2.02.1.**Designación del responsable de seguridad**

- a) El organismo debe designar formalmente un responsable de seguridad de la información (CISO o rol equivalente).
- b) Este rol debe poseer la autoridad y la independencia necesarias

para supervisar el programa de seguridad y debe tener una línea de reporte definida que le permita comunicarse directamente con la alta dirección.

- c) Las responsabilidades, autoridad y competencias para este rol deben estar documentadas en una descripción de puesto oficial.

Subsección 2.02.2. Definición de responsabilidades de seguridad

- a) El organismo debe definir, documentar y comunicar los roles y responsabilidades de seguridad de la información para todo el personal, incluyendo a la alta dirección, los gerentes de áreas, el personal técnico y los usuarios finales.
- b) Estas responsabilidades deben ser integradas en las descripciones de puestos y en los procesos de evaluación de desempeño.

Sección 2.03. Comité de implementación y gestión estándares TIC

El Comité de Implementación y Gestión de Estándares TIC (CIGETIC) se forma dentro de los organismos para establecer una instancia responsable de la planificación, seguimiento, escalamiento y gestión de recursos para implementar estándares NORTIC, y el seguimiento y reporte de los resultados derivados e indicadores afectados. Para la conformación del CIGETIC, el organismo debe cumplir con lo establecido a continuación:

- (a) El organismo debe conformar un Comité de Implementación y Gestión de Estándares TIC (CIGETIC) mediante una resolución administrativa interna. Este comité es la instancia de gobernanza responsable de la planificación, supervisión y gestión de recursos para la implementación de todo el ecosistema de normas de seguridad.

- (b) El CIGETIC debe estar conformado, como mínimo, por los responsables de las áreas listadas a continuación:
 - (i) **Comunicaciones:** Responsable de la comunicación de crisis y la gestión de la reputación institucional.
 - (ii) **Oficina de Acceso a la Información (OAI):** Responsable de la clasificación y protección de la información pública.
 - (iii) **Jurídica:** Responsable de asegurar el cumplimiento del marco legal y regulatorio.
 - (iv) **Tecnologías de la Información y Comunicación (TIC):** Responsable de la implementación y operación de la infraestructura tecnológica.
 - (v) **Planificación y desarrollo:** Responsable de alinear la implementación de las normas con la estrategia institucional.
 - (vi) **Seguridad de la información:** El responsable de seguridad (CISO o rol equivalente), quien actuará como asesor principal del comité en materia de seguridad y riesgo.
- (c) La MAE del organismo debe designar un coordinador y un secretario para el comité.
- (d) La resolución de conformación debe detallar las responsabilidades y atribuciones del CIGETIC, incluyendo, como mínimo:
 - (i) Planificación y seguimiento de la implementación de estándares NORTIC.
 - (ii) Monitorear el mantenimiento de los estándares NORTIC implementados.
 - (iii) Realizar reuniones periódicas para la gestión correspondiente para cumplir los objetivos planificados, como avanzar en las implementaciones y mantener los

estándares.

- (iv) Poner en conocimiento a la MAE, a través de informes periódicos, sobre el estado de las implementaciones NORTIC y sus derivados.
 - (v) Funcionar como primera instancia para la resolución de conflictos que pudieran surgir durante la implementación de los estándares NORTIC.
 - (vi) Escalar a la MAE, a través del coordinador, situaciones que requieran la intervención de ésta, como la necesidad de recursos o la resolución de conflictos que no puedan solucionarse a nivel del comité.
 - (vii) Velar por la capacitación de los integrantes del comité, el personal bajo su cargo y demás involucrados, en las Normas de Tecnologías de la Información y Comunicación (NORTIC).
 - (viii) Asumir las funciones de gobierno del programa de continuidad operativa: El CIGETIC asume todas las responsabilidades de supervisión, aprobación de planes y estrategias que anteriormente correspondían al Comité de Continuidad (CONTI). El CONTI queda, por tanto, discontinuado y sus funciones se integran en el CIGETIC para asegurar una gobernanza unificada de la seguridad y la resiliencia.
 - (ix) Otras responsabilidades que la MAE delegue.
- (e) La MAE del organismo debe concretar, mediante un artículo de la resolución de conformación, las atribuciones que concede al Comité, en las que se incluya la potestad de:
- (i) Convocar a reunión, a colaboradores de la institución que no sean miembros del comité.

- (i) Asignar responsabilidades y tareas a los miembros (y no miembros) del Comité y personal bajo su cargo, si son necesarias para la implementación de estándares NORTIC.
 - (ii) Otras atribuciones que la MAE considere necesarias.
- (f) La resolución debe establecer, de forma separada a las responsabilidades, las directrices para la entrega de los informes a la MAE, indicando:
- (ii) La periodicidad de entrega.
 - (iii) La estructura de contenido de los informes.
 - (iv) Otras directrices que la MAE entienda necesarias.

Sección 2.04.

Marco de políticas de seguridad de la información

Esta sección establece los requisitos para la creación y mantenimiento del conjunto de políticas documentadas que forman la base del Sistema de Administración de la Seguridad de la Información (SASI). Define los mandatos de alto nivel que deben existir para gobernar los dominios clave de la seguridad.

NOTA: Los mandatos de política definidos en las siguientes subsecciones pueden ser documentados en políticas individuales o pueden ser agrupados en un número menor de documentos de política consolidados, siempre y cuando todo el contenido requerido esté claramente abordado y documentado.

Subsección 2.04.1.

Política general de seguridad de la información

- a) El organismo debe elaborar, documentar y mantener una Política General de Seguridad de la Información, aprobada por

la MAE.

- b) Dicha política debe, como mínimo:
 - (i) Establecer la dirección estratégica y los principios fundamentales de la seguridad para el organismo.
 - (ii) Declarar el compromiso de la MAE con la protección de la información.
 - (iii) Hacer referencia al marco legal y regulatorio que el organismo debe cumplir.
 - (iv) Asignar las responsabilidades generales para la gestión de la seguridad.
 - (v) Establecer el marco para la definición de objetivos de seguridad y la gestión de riesgos.
- c) Esta política debe ser comunicada a todo el personal y partes interesadas relevantes.

Subsección 2.04.2.

Política de clasificación y manejo de la información

- a) El organismo debe definir, documentar e implementar un esquema de clasificación de la información que abarque todos los activos de información del organismo (digitales y físicos).
- b) Dicho esquema debe estar fundamentado, como mínimo, en las categorías definidas en la [Ley 200-04 sobre Libre Acceso a la Información Pública](#), distinguiendo claramente entre la información de carácter público, reservado o confidencial.
- c) Adicionalmente a la clasificación legal, el esquema debe incluir, como mínimo, tres niveles de clasificación para regular el manejo interno de la información, basados en su sensibilidad y criticidad. Estos niveles deben definir, al menos, la información de Uso Público, de Uso Interno del organismo y de Uso

Restringido o confidencial.

- d) El organismo debe establecer y documentar reglas formales para el manejo, etiquetado, almacenamiento, transporte y comunicación de la información, que sean proporcionales a su nivel de clasificación.

Subsección 2.04.3. Política de retención y disposición segura

- a) El organismo debe definir y documentar los períodos de retención para los diferentes tipos de información, en cumplimiento con los requisitos legales, regulatorios y de negocio.
- b) El organismo debe implementar y documentar procedimientos formales y auditables para la destrucción segura de la información y de los activos físicos que la contienen, como papel, discos duros, cintas, entre otros, una vez que su período de retención haya concluido.

Subsección 2.04.4. Política de control de acceso

- a) La política debe establecer el mandato de que el acceso a los activos de información y sistemas tecnológicos sea controlado y restringido únicamente a usuarios, procesos y dispositivos autorizados.
- b) La política debe exigir la implementación de mecanismos de autenticación que se ajusten al nivel de riesgo de cada transacción o acceso, garantizando un equilibrio entre seguridad y usabilidad.
- c) La política debe ordenar la aplicación de medidas reforzadas de autenticación, como la autenticación multifactor (MFA), para el acceso a recursos tecnológicos críticos, información sensible o para usuarios con privilegios elevados.
- d) La política debe formalizar que todo acceso a sistemas, datos y recursos se otorgue exclusivamente conforme al principio

de mínimo privilegio, garantizando que cada usuario tenga únicamente los permisos necesarios para desempeñar sus funciones asignadas.

- e) La política debe exigir el establecimiento de mecanismos de separación de funciones para las tareas críticas, con el fin de prevenir fraudes, abusos o errores.
- f) Se debe establecer en la política la responsabilidad de implementar y mantener controles de acceso físico para proteger las áreas críticas de la institución, como los centros de datos y las salas de comunicaciones.

Subsección 2.04.5. Política de protección de datos y criptografía

- a) La política debe establecer el mandato de proteger la información del organismo en todos sus estados (en reposo, en tránsito y en uso), exigiendo, como mínimo:
 - (i) La implementación de mecanismos de cifrado para los datos almacenados, tanto en sistemas de producción como en soportes de respaldo.
 - (ii) El establecimiento de procedimientos seguros para la gestión del ciclo de vida de las claves criptográficas.
 - (iii) La implementación de mecanismos técnicos para proteger la confidencialidad, integridad y autenticidad de los datos durante su transmisión, mediante el uso de cifrado robusto y protocolos seguros.

Subsección 2.04.6. Política de seguridad de redes

- a) La política debe establecer el mandato de implementar mecanismos técnicos y organizativos para asegurar la protección y resiliencia de las redes de control, las comunicaciones críticas y los sistemas de tecnología de operación, exigiendo, como mínimo, la aplicación de los principios de defensa en

profundidad y segmentación de red.

Subsección 2.04.7.**Política de gestión de cambios**

- a) La política debe establecer la obligación de implementar un proceso estructurado para la gestión de cambios en la configuración de sistemas, plataformas y componentes tecnológicos, garantizando que tales cambios sean controlados, autorizados y evaluados en cuanto a su impacto en la seguridad.

Subsección 2.04.8.**Política de desarrollo seguro (SDLC)**

- a) La política debe establecer la obligación de implementar un Ciclo de Vida de Desarrollo Seguro (SDLC, por sus siglas en inglés), que incorpore prácticas de seguridad en cada una de sus fases, desde la planificación hasta el mantenimiento, asegurando que los sistemas y aplicaciones mantengan un nivel de protección acorde con los riesgos.

Subsección 2.04.9.**Política de monitoreo y detección de amenazas**

- a) La política debe establecer el mandato de implementar capacidades de monitoreo continuo y detección de amenazas para identificar actividades maliciosas y eventos de seguridad de manera oportuna. Debe exigir, como mínimo:
 - (i) El establecimiento de líneas base de comportamiento normal para los sistemas y redes críticas.
 - (ii) La implementación de capacidades técnicas y operativas para la integración, correlación y análisis de eventos de seguridad provenientes de diversas fuentes.
 - (iii) El uso de herramientas de monitoreo para la supervisión constante de la infraestructura tecnológica, incluyendo redes, sistemas, actividad del personal y proveedores.

Subsección 2.04.10.**Política de gestión de incidentes de ciberseguridad**

- a) La política debe establecer el mandato de contar con un programa formal para la gestión de incidentes de ciberseguridad, con el fin de asegurar una respuesta estructurada, coordinada y eficaz ante cualquier evento que comprometa la seguridad del organismo. Debe exigir, como mínimo:
 - (i) La creación y mantenimiento de un Plan de Respuesta a Incidentes.
 - (ii) Un esquema formal para la categorización y priorización de incidentes.
 - (iii) Un proceso definido para la notificación, comunicación y escalada de incidentes a las partes interesadas internas y externas, incluyendo a las autoridades nacionales competentes.
 - (iv) El establecimiento y mantenimiento de un Plan de Comunicación de Crisis para asegurar una comunicación estructurada, oportuna y precisa durante y después de un incidente de alto impacto.

Subsección 2.04.11.**Política de seguridad en la recuperación**

- a) La política debe establecer la obligación de integrar controles de seguridad en la fase de recuperación de un incidente, asegurando que la restauración de los servicios no reintroduzca amenazas y fortalezca la postura de seguridad del organismo. Adicionalmente, debe exigir:
 - (i) Un proceso formal para la activación oportuna y eficaz de los planes de recuperación.
 - (ii) Un mecanismo para la selección, ajuste y priorización de las acciones de recuperación, basado en la criticidad de las

funciones y los resultados del BIA.

- (iii) Criterios objetivos para determinar y declarar formalmente el final del proceso de recuperación.



MODELO DE MADUREZ Y APLICABILIDAD

Este capítulo establece el marco de madurez que permite una implementación escalonada y adaptativa de los requisitos de seguridad y resiliencia, basándose en la capacidad y criticidad de cada organismo. Funciona como el mecanismo de gobernanza para la aplicación de todo el ecosistema de normas.

Sección 3.01.

Definición de los niveles de madurez

El Modelo de Madurez del Sistema de Administración de la Seguridad de la Información (SASI) se estructura en tres niveles progresivos. Cada nivel representa un grado mayor de madurez en las capacidades de seguridad de un organismo, desde las prácticas esenciales hasta la optimización continua.

a) Nivel 1: Fundamental (MIL 1)

Representa el conjunto de prácticas de seguridad esenciales y obligatorias para cualquier organismo del Estado, sin importar su tamaño o complejidad. Este nivel se enfoca en establecer los controles de “higiene cibernética” indispensables para mitigar los riesgos más comunes y en formalizar los procesos de gestión básicos requeridos por la normativa transversal. El objetivo

principal es garantizar una base de cumplimiento y protección mínima para los activos y servicios.

b) Nivel 2: Gestionado (MIL 2)

Representa un avance hacia un programa de seguridad proactivo y con procesos definidos. En este nivel, las prácticas ya no se enfocan únicamente en el cumplimiento básico, sino que se gestionan a través de políticas y procedimientos diseñados para estandarizar la operación y mejorar la consistencia. Se establecen roles especializados, se implementan metodologías formales de gestión de riesgos y se realizan evaluaciones periódicas para asegurar que las actividades sean planificadas, implementadas y supervisadas de forma coherente.

c) Nivel 3: Optimizado (MIL 3)

Representa el nivel más alto de madurez, donde el programa de seguridad está plenamente integrado en la cultura y los procesos estratégicos del organismo. En este nivel, la gestión de la seguridad es predictiva y se basa en un ciclo de mejora continua impulsado por datos. El organismo no solo gestiona sus procesos, sino que utiliza métricas (KPIs) y análisis de tendencias para anticipar amenazas, adaptar sus defensas y optimizar la asignación de recursos. La seguridad se consolida como un habilitador de la misión institucional y se busca la innovación continua en los procesos de defensa y resiliencia.

Subsección 3.01.1.

Estructura y componentes del modelo de madurez

El Modelo de Madurez se articula en una estructura jerárquica de bloques, dominios y capacidades para asegurar una cobertura integral de la seguridad y la resiliencia.

El modelo agrupa las capacidades en tres (3) bloques temáticos que representan el ciclo de vida de la gestión de la seguridad:

- **Bloque 1: Gobernanza y Fundamentos Estratégicos:** Establece las bases de liderazgo, políticas y planificación.
- **Bloque 2: Gestión de Riesgos y Defensa Proactiva:** Se enfoca en la identificación de riesgos y la construcción de las defensas para prevenirlos.
- **Bloque 3: Operaciones de Seguridad, Resiliencia y Mejora:** Cubre las capacidades para detectar, responder, recuperarse y aprender de los incidentes.

Los bloques temáticos se desglosan en siete (7) dominios funcionales que agrupan las prácticas de seguridad. Estos dominios son:

1. Gobernanza (GOB)
2. Gestión de Riesgos (RIS)
3. Gestión de Activos y Ciclo de Vida de la Información (ACT)
4. Defensa y Protección (DEF)
5. Seguridad en el Factor Humano (HUM)
6. Gestión de Incidentes (INC)
7. Resiliencia y Continuidad Operativa (CON)

Dentro de cada dominio, se definen un total de diecinueve (19) capacidades específicas, las cuales representan un conjunto de prácticas orientadas a un objetivo concreto y son la base para la evaluación de la madurez. A continuación, se describen las capacidades agrupadas por su bloque temático:

Bloque 1: Gobernanza y fundamentos estratégicos

- **Capacidad 1:** Liderazgo y Compromiso Institucional. Cubre el rol de la MAE, la asignación de recursos y la promoción de la cultura.

- **Capacidad 2:** Estructura Organizativa y Roles de Seguridad. Cubre la designación del CISO y la definición de responsabilidades en toda la organización.
- **Capacidad 3:** Marco Normativo y Político de Seguridad. Cubre la Política General de Seguridad y el ecosistema de políticas específicas.
- **Capacidad 4:** Gestión de Activos y Clasificación de la Información. Cubre el inventario de activos, la asignación de propietarios y el esquema de clasificación.

Bloque 2: Gestión de riesgos y defensa proactiva

- **Capacidad 5:** Gestión de Riesgos de Seguridad de la Información. Cubre la metodología de análisis, el Plan de Tratamiento y la Declaración de Aplicabilidad (SoA).
- **Capacidad 6:** Gestión de la Seguridad en Recursos Humanos. Cubre la concientización, la gestión del ciclo de vida del empleado (énfasis en el cese) y los acuerdos de confidencialidad.
- **Capacidad 7:** Seguridad Física y Ambiental. Cubre el control de acceso físico a áreas críticas, protección de equipos, etc.
- **Capacidad 8:** Gestión de Identidades y Control de Acceso Lógico. Cubre el ciclo de vida de las identidades (IAM), la autenticación (MFA) y la aplicación del principio de mínimo privilegio.
- **Capacidad 9:** Protección de Datos y Criptografía. Cubre el cifrado de datos en reposo y en tránsito, y la gestión de claves criptográficas.
- **Capacidad 10:** Gestión de Vulnerabilidades Técnicas. Cubre el escaneo, la priorización y la gestión de parches.

- **Capacidad 11:** Configuración Segura y Gestión de Cambios. Cubre el hardening de sistemas y el proceso formal de gestión de cambios.
- **Capacidad 12:** Seguridad de Redes y Perímetro. Cubre firewalls, segmentación, protección contra DDoS, etc.
- **Capacidad 13:** Seguridad en el Desarrollo de Aplicaciones (SDLC). Cubre la integración de la seguridad en el ciclo de vida del desarrollo de software.
- **Capacidad 14:** Gestión de Riesgos de la Cadena de Suministro. Cubre la seguridad en la relación con proveedores y terceros.

Bloque 3: Operaciones de seguridad, resiliencia y mejora

- **Capacidad 15:** Detección y Monitoreo de Eventos de Seguridad. Cubre la gestión de logs, la implementación de SIEM y el monitoreo de la actividad.
- **Capacidad 16:** Gestión de Incidentes de Seguridad. Cubre el plan de respuesta, la contención, el análisis forense y la comunicación de incidentes.
- **Capacidad 17:** Gestión de la Continuidad Operativa. Cubre el Análisis de Impacto al Negocio (BIA), y los planes (BCP, DRP).
- **Capacidad 18:** Pruebas, Validación y Resiliencia. Cubre las pruebas y simulacros de los planes de continuidad y respuesta.
- **Capacidad 19:** Evaluación del Desempeño y Mejora Continua. Cubre los KPIs, las auditorías internas del SASI y la Revisión por la Dirección.

Sección 3.02.

Asignación del Nivel de Madurez Objetivo (MOO)

Todo organismo del Poder Ejecutivo debe tener un Nivel de Madurez Objetivo (MOO) formalmente asignado, el cual determina el conjunto mínimo de requisitos que la institución está obligada a implementar.

Subsección 3.02.1.

Metodología de asignación del MOO

- a) El Nivel de Madurez Objetivo (MOO) debe determinarse de forma directa, basándose en el **Modelo de Estructura Organizativa (A, B o C)** que le haya sido asignado al organismo.
- b) La asignación del Modelo de Estructura Organizativa se rige por la metodología y los criterios de clasificación de complejidad institucional establecidos en la **Resolución núm. 342-2024 del Ministerio de Administración Pública (MAP)**, o la normativa que la sustituya.

Subsección 3.02.2.

Correspondencia entre modelo de estructura y MOO

- a) La correspondencia que debe aplicarse para determinar el MOO es la siguiente:
 - (iv) Los organismos clasificados con el Modelo A (alta complejidad) tendrán asignado un Nivel de Madurez Objetivo 3 (Optimizado).
 - (v) Los organismos clasificados con el Modelo B (complejidad media) tendrán asignado un Nivel de Madurez Objetivo 2 (Gestionado).
 - (vi) Los organismos clasificados con el Modelo C (baja complejidad) tendrán asignado un Nivel de Madurez Objetivo 1 (Fundamental).

Subsección 3.02.3.

Documentación y ciclo de vida del MOO

- a) El Nivel de Madurez Objetivo (MOO) resultante de esta clasificación debe ser documentado formalmente y comunicado al Comité de Implementación y Gestión de Estándares TIC (CIGETIC) y a la Máxima Autoridad Ejecutiva (MAE) para su conocimiento y supervisión.
- b) El MOO debe ser revisado y, si aplica, reajustado, siempre que el organismo sea sometido a una reevaluación de su Modelo de Estructura Organizativa por parte del MAP, para asegurar que el nivel de exigencia se mantenga alineado con el contexto y la criticidad de la institución.

Sección 3.03. Aplicabilidad de requisitos por nivel

El Nivel de Madurez Objetivo (MOO) asignado a un organismo determina el conjunto de requisitos de todo el ecosistema normativo (NORTIC A7, A8 y A9) que le son de cumplimiento obligatorio. Esta sección detalla el instrumento (la matriz) y el proceso (el cumplimiento progresivo) para la aplicación de este modelo.

Subsección 3.03.1.

Matriz de controles por nivel de madurez

- a) El Anexo A de esta norma contiene la **Matriz de Controles por Nivel de Madurez**. Esta matriz es el instrumento oficial que clasifica cada requisito individual de las NORTIC A7, A8 y A9 en su correspondiente nivel de madurez (Nivel 1, 2 o 3).
- b) La Matriz de Controles debe ser utilizada como la única fuente de referencia para identificar la aplicabilidad de los requisitos. Detalla, para cada control, el nivel de madurez en el que su implementación se vuelve obligatoria.

- c) La Matriz de Controles está organizada en función de las capacidades de seguridad definidas en las NORTIC A7, A8 y A9. Cada fila de la matriz representará una capacidad específica, mientras que las columnas indicarán en qué nivel de madurez se exige la implementación de los controles asociados a dicha capacidad, en lugar de ser una enumeración secuencial de los requisitos de cada norma.
- d) La OGTIC será responsable de mantener la Matriz de Controles actualizada, reflejando cualquier cambio o nueva versión en las normas del ecosistema de seguridad.
- e) La Matriz de Controles del Anexo A se organiza en las siguientes columnas: **ID** (identificador con prefijo de dominio), **Fuente** (norma de referencia, sección /subsección), **Práctica/Requisito** (la capacidad a implementar), y las columnas **MIL 1**, **MIL 2**, **MIL 3** que indican el nivel de obligatoriedad.

Subsección 3.03.2.

Cumplimiento progresivo y proceso de certificación

- a) La certificación bajo este marco normativo consistirá en la obtención de un Nivel de Madurez en Seguridad, el cual indicará el nivel alcanzado (Nivel 1, 2 o 3). Los organismos no obtendrán certificaciones independientes o parciales en la NORTIC A7, A8 o A9.
- b) Para obtener la certificación en un nivel de madurez específico, el organismo debe demostrar el cumplimiento de todos los requisitos y controles listados en la Matriz de Controles (Anexo A) que correspondan a ese nivel y a todos los niveles inferiores.
- c) El cumplimiento debe ser estrictamente progresivo. Un organismo no podrá ser certificado en un Nivel de Madurez superior (ej. Nivel 2) si presenta no conformidades mayores en cualquiera de los requisitos pertenecientes a un nivel inferior (ej. Nivel 1). La subsanación de las no conformidades de los niveles

básicos es un prerrequisito para aspirar a un nivel superior.

- d) La auditoría de certificación evaluará el grado de implementación y la efectividad de los controles aplicables al nivel de madurez al que aspira el organismo. El nivel final otorgado en el certificado será el nivel más alto en el que el organismo demuestre un cumplimiento completo y sin no conformidades mayores.
- e) En caso de que un organismo no alcance a cumplir con todos los requisitos de su Nivel de Madurez Objetivo (MOO) en una evaluación, se le otorgará la certificación en el nivel inferior que sí haya completado satisfactoriamente. A partir de la emisión del informe de auditoría, el organismo deberá elaborar y presentar a la OGTIC, en un plazo no mayor a treinta (30) días calendario, un plan de acción formal con un cronograma para cerrar las brechas identificadas y alcanzar su MOO. El cumplimiento de este plan será objeto de seguimiento.
- f) La auditoría para una certificación de Nivel de Madurez se realizará exclusivamente contra el conjunto de prácticas exigidas para dicho nivel y los inferiores, según lo establecido en la Matriz de Controles. La evidencia de cumplimiento para cada práctica se evaluará conforme a los requisitos detallados en la norma citada en la columna “Fuente”.

Subsección 3.03.3.

Requisitos de institucionalización por nivel de madurez

- a) Para alcanzar el Nivel 2 (Gestionado), el organismo debe evidenciar, como mínimo:
 - (i) La existencia de políticas y procedimientos formales, documentados y aprobados que rigen la implementación de las capacidades de seguridad.
 - (ii) La asignación formal de roles y responsabilidades para la ejecución de dichos procedimientos.

- (iii) La asignación de recursos (humanos y financieros) para sostener las prácticas de seguridad.
- b) Para alcanzar el Nivel 3 (Optimizado), el organismo debe evidenciar, adicionalmente a lo requerido en el Nivel 2:
 - (i) La existencia de un proceso formal de revisión y actualización periódica de las políticas y procedimientos, basado en lecciones aprendidas y cambios en el entorno.
 - (ii) El uso de métricas (KPIs) para medir la efectividad de las capacidades de seguridad y reportarlas a la alta dirección.
 - (iii) La implementación de un proceso de mejora continua documentado, que demuestre cómo la institución estandariza y optimiza sus prácticas de seguridad.

Subsección 3.03.4.**Aplicabilidad basada en el riesgo y contexto específico**

- a) El Nivel de Madurez Objetivo (MOO) establece el requisito mínimo de cumplimiento para el organismo en su totalidad. Sin embargo, esto no exime a la institución de su responsabilidad de gestionar sus riesgos específicos.
- b) El organismo, como resultado de su proceso de gestión de riesgos (definido en la NORTIC A9), debe identificar si existen sistemas, procesos o activos de información cuya criticidad o perfil de riesgo exijan la implementación de controles de un nivel de madurez superior al MOO asignado.
- c) La implementación de estos controles adicionales debe ser documentada en el Plan de Tratamiento de Riesgos y en la Declaración de Aplicabilidad (SoA), justificando la necesidad de superar el requisito mínimo establecido por el MOO.
- d) La correcta implementación de estos controles adicionales será verificada durante la auditoría, pero no afectará el Nivel de

Madurez general certificado del organismo, a menos que este decida aspirar formalmente a un nivel superior.

Subsección 3.03.5. Proceso de transición y evolución de nivel

- a) Un organismo que desee evolucionar hacia un Nivel de Madurez superior a su MOO actual o al nivel certificado debe formalizarlo a través de un plan de proyecto aprobado por su CIGETIC.
- b) Dicho plan debe incluir un análisis de brechas (gap analysis) contra los requisitos del nivel superior y un cronograma para la implementación de los controles y procesos faltantes.
- c) El organismo podrá solicitar a la OGTIC una nueva auditoría de certificación para validar el nuevo nivel una vez que considere que ha completado satisfactoriamente su plan de transición.



PLANIFICACIÓN Y GESTIÓN DE LA SEGURIDAD

Este capítulo establece los requisitos para la planificación del Sistema de Administración de la Seguridad de la Información (SASI), integrando la gestión del riesgo como el pilar fundamental para la toma de decisiones.

Sección 4.01. Contexto organizacional y partes interesadas

Esta sección establece los requisitos para que la organización defina su contexto interno y externo. Detalla los procedimientos para comprender la misión institucional, identificar a las partes interesadas relevantes y determinar sus expectativas y requisitos de seguridad, sentando así las bases para una gestión de riesgos alineada con los objetivos del negocio.

Subsección 4.01.1. Comprensión de la organización y su misión

- a) El organismo debe definir, documentar y comunicar formalmente su misión institucional, visión estratégica y prioridades organizacionales, ya que constituyen la base para la identificación de los riesgos de seguridad que pudieran afectar su cumplimiento.

- b) La misión y visión del organismo deben ser compartidas a través de canales formales, tales como el plan estratégico, las comunicaciones oficiales o los materiales de orientación institucional.
- c) Debe evidenciarse la elaboración de documentos estratégicos que definan de manera clara las prioridades de la organización, sus objetivos operativos y los mandatos legales que debe cumplir.
- d) Debe establecerse un mecanismo regular de comunicación organizacional (como reuniones internas o boletines informativos) para informar al personal y a la comunidad atendida sobre las prioridades institucionales y los aspectos estratégicos relacionados con la gestión de riesgos de seguridad.

Subsección 4.01.2.**Identificación de partes interesadas y sus requisitos**

- a) El organismo debe identificar de forma estructurada a sus partes interesadas internas y externas, y documentar sus requisitos y expectativas en materia de seguridad de la información.
- b) Para las partes interesadas internas (tales como la alta dirección, asesores, personal técnico y operativo), la documentación debe incluir, como mínimo, sus expectativas respecto a:
 - (i) Los niveles aceptables de riesgo.
 - (ii) El desempeño esperado de los servicios tecnológicos.
 - (iii) Las consideraciones culturales de la institución.
- c) Para las partes interesadas externas (tales como ciudadanos, otros organismos del Estado, proveedores y socios), la documentación debe incluir, como mínimo, sus expectativas respecto a:

- (i) La privacidad y protección de sus datos personales.
- (ii) El cumplimiento de los requerimientos regulatorios.
- (iii) Las obligaciones de seguridad establecidas en compromisos contractuales.

Subsección 4.01.3.

Gestión de requisitos legales y regulatorios

- a) El organismo debe establecer y mantener un proceso documentado para identificar, registrar y realizar el seguimiento de todos los requisitos legales, regulatorios y contractuales aplicables a la seguridad de la información.
- b) Este proceso debe asegurar que se identifiquen y se documenten los requisitos vigentes sobre la protección de la información personal, conforme a las leyes nacionales y los compromisos internacionales suscritos por el Estado Dominicano.
- c) El proceso debe incluir un mecanismo específico para rastrear y gestionar las obligaciones de seguridad establecidas en contratos con proveedores, clientes, socios o cualquier tercero con el que el organismo mantenga una relación operativa.
- d) La estrategia de seguridad del organismo, así como sus políticas y controles, deben estar alineadas con los requisitos legales, regulatorios y contractuales identificados.
- e) Debe designarse formalmente un rol o una función dentro del organismo (en coordinación con el área jurídica) que sea responsable de mantener actualizado el inventario de requisitos y de comunicar cualquier cambio al Responsable de Seguridad de la Información y al CIGETIC.
- f) Debe establecerse un proceso de revisión y actualización periódica de las políticas y procedimientos del SASI, para garantizar su conformidad continua con los requisitos aplicables.

Sección 4.02.

Marco de gestión de riesgos de seguridad

Esta sección establece los requisitos para la implementación de un proceso formal de gestión de riesgos. Define la obligación de adoptar la metodología estandarizada para todo el Estado y asegura que la gestión del riesgo sea un componente central en la toma de decisiones estratégicas.

Subsección 4.02.1.

Proceso de gestión de riesgos

- a) El organismo debe establecer y mantener un proceso formal, documentado y aprobado para la identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información, tomando en cuenta el entorno operativo, la misión institucional y la criticidad de sus activos y servicios.
- b) La implementación de este proceso debe seguir la metodología detallada en la **NORTIC A9 – Norma para la Gestión de Riesgos Tecnológicos y Continuidad Operativa**, con el fin de asegurar la coherencia y comparabilidad de los resultados en todo el ecosistema de seguridad del Estado.
- c) Debe asegurarse una gestión continua del proceso de riesgos, lo que implica su revisión, actualización y aplicación sistemática ante cambios en el entorno de amenazas, la legislación aplicable o las prioridades estratégicas de la organización.
- d) Debe garantizarse una comunicación clara y continua de los procesos de gestión de riesgos, asegurando que todas las partes involucradas comprendan su rol, las acciones requeridas y los canales de reporte pertinentes.

Subsección 4.02.2.

Definición de criterios y tolerancia al riesgo

- a) El organismo debe establecer y documentar criterios claros y objetivos para determinar la criticidad de sus capacidades, servicios y activos. Estos criterios deben basarse en el impacto

potencial que una interrupción o compromiso tendría sobre la misión institucional, la prestación de servicios esenciales y el cumplimiento de los mandatos legales.

- b) Debe definirse formalmente la tolerancia al riesgo de la institución. Esta definición debe establecer límites claros y, en la medida de lo posible, medibles sobre la cantidad y el tipo de riesgo que el organismo está dispuesto a aceptar en sus operaciones.
- c) La definición de la tolerancia al riesgo debe estar alineada con el contexto, la misión y la capacidad de respuesta del organismo, y debe ser aprobada por la Máxima Autoridad Ejecutiva (MAE).
- d) La tolerancia al riesgo aprobada debe ser comunicada de forma efectiva a todas las partes interesadas relevantes, para asegurar que los umbrales definidos y su aplicación sean comprendidos en todos los niveles de la organización.

Subsección 4.02.3.

Plan de tratamiento de riesgos

- a) Como resultado del proceso de análisis y evaluación de riesgos, el organismo debe elaborar y mantener un plan de tratamiento de riesgos formal y documentado.
- b) Este plan debe detallar, para cada riesgo identificado que requiera tratamiento, la estrategia de respuesta seleccionada (mitigar, transferir, aceptar o evitar), conforme a la metodología definida en la NORTIC A9.
- c) Para los riesgos donde la estrategia seleccionada sea mitigar, el plan de tratamiento de riesgos debe especificar los controles que serán implementados, basándose en el catálogo de la NORTIC A8 – Norma General de Ciberseguridad.
- d) El plan de tratamiento de riesgos debe ser un documento de gestión que incluya, como mínimo, la siguiente información para cada acción de mitigación:

- (i) El riesgo específico que se está tratando.
 - (ii) El control o conjunto de controles seleccionados.
 - (iii) El responsable designado para la implementación.
 - (iv) Los recursos necesarios para su ejecución.
 - (v) Los plazos y fechas compromiso para la implementación.
- e) El plan de tratamiento de riesgos debe ser revisado y aprobado formalmente por el CIGETIC y la Máxima Autoridad Ejecutiva (MAE).

Sección 4.03.

Declaración de Aplicabilidad (SoA)

La Declaración de Aplicabilidad (SoA, por sus siglas en inglés, Statement of Applicability) es el documento central que resume la postura de seguridad de un organismo. Sirve como el vínculo formal entre el análisis de riesgos, las decisiones de tratamiento y el conjunto de controles implementados. Su propósito es proporcionar una justificación auditable de por qué cada control fue seleccionado o excluido.

Subsección 4.03.1.

Creación y contenido del SoA

- a) Como resultado del proceso de análisis y tratamiento de riesgos, el organismo debe elaborar y mantener una Declaración de Aplicabilidad (SoA).
- b) El SoA debe ser un documento formal que liste todos los controles referenciados en el catálogo de la **NORTIC A8 – Norma General de Ciberseguridad** y, si aplica, de otras normativas o marcos de referencia adoptados por la institución.
- c) Para cada control listado, el SoA debe indicar claramente lo siguiente:

- (i) Si el control ha sido implementado o se planea implementar.
 - (ii) Una justificación para la implementación del control, vinculándolo directamente a los riesgos identificados en el proceso de gestión de riesgos (conforme a la **NORTIC A9**) que dicho control ayuda a mitigar.
 - (iii) Si el control no ha sido implementado (excluido), se debe proporcionar una justificación clara y formal para su exclusión. Las razones para la exclusión pueden incluir, entre otras, que el riesgo asociado al control ha sido aceptado formalmente por la dirección, transferido, o que el control no es aplicable al contexto tecnológico u operativo del organismo.
 - (iv) Una referencia cruzada a la documentación específica (políticas, procedimientos, guías técnicas) donde se describe la implementación del control.
- d) El SoA debe reflejar el estado actual de la implementación de los controles, distinguiendo entre los controles que ya están plenamente operativos y aquellos que forman parte del Plan de Tratamiento de Riesgos y están pendientes de implementación.

Subsección 4.03.2.

Aprobación y mantenimiento del SoA

Apartado 4.03.2.1.

Aprobación formal

- a) La versión inicial del SoA, así como cualquier actualización mayor subsecuente, debe ser revisada y validada por el Comité de Implementación y Gestión de Estándares TIC (CIGETIC).
- b) Tras la validación del CIGETIC, el SoA debe ser presentado a la Máxima Autoridad Ejecutiva (MAE) o al nivel directivo que esta designe, para su aprobación formal.
- c) La aprobación formal del SoA constituye la aceptación por parte

de la alta dirección de los riesgos residuales del organismo. La evidencia de esta aprobación (como una firma en el documento o un acta de reunión) debe ser conservada como un registro auditable fundamental del Sistema de Administración de la Seguridad de la Información (SASI).

Apartado 4.03.2.2.

Mantenimiento y revisión periódica

- a) El SoA debe ser un documento vivo y debe ser revisado y actualizado para reflejar cualquier cambio en la postura de seguridad del organismo.
- b) Se debe realizar una revisión formal del SoA, como mínimo, una (1) vez al año, o siempre que ocurra uno de los siguientes eventos significativos:
 - (i) Cambios importantes en la infraestructura tecnológica o en la arquitectura de seguridad.
 - (ii) La introducción de nuevos sistemas o servicios críticos.

Cambios en los resultados del análisis de riesgos o del análisis de impacto al negocio (BIA).
 - (iii) Después de un incidente de seguridad significativo que revele debilidades en los controles.
 - (iv) Cambios en el marco legal, regulatorio o contractual que afecten los requisitos de seguridad.
- c) La responsabilidad de mantener el SoA actualizado debe ser formalmente asignada al Responsable de Seguridad de la Información (CISO o rol equivalente).

Apartado 4.03.2.3.

Disponibilidad y comunicación

- a) La versión vigente y aprobada del SoA debe estar disponible para todas las partes interesadas relevantes, incluyendo los equipos de auditoría interna y externa, para facilitar los procesos de

evaluación y verificación del cumplimiento.

Sección 4.04.

Seguridad en la cadena de suministro

Esta sección establece los requisitos de gobernanza para la gestión de los riesgos de seguridad de la información introducidos por terceros, incluyendo proveedores, socios tecnológicos y contratistas.

Subsección 4.04.1.

Proceso de gestión de riesgos de terceros

- a) El organismo debe establecer, documentar y mantener un proceso formal para la identificación, evaluación y tratamiento de los riesgos de seguridad a lo largo de todo el ciclo de vida de la relación con terceros.
- b) Este proceso debe incluir una fase de debida diligencia (due diligence) de seguridad, que debe ser ejecutada antes de formalizar cualquier relación contractual con un proveedor de servicios críticos. Esta evaluación debe incluir, como mínimo:
 - (i) El análisis de la postura de seguridad del proveedor, revisando sus políticas, certificaciones (ej. ISO 27001, SOC 2) y resultados de auditorías previas.
 - (ii) Una evaluación de la capacidad del proveedor para cumplir con los requisitos de seguridad y regulatorios del organismo.
 - (iii) La identificación de los controles de seguridad que el proveedor tiene implementados para proteger la información del organismo.
- c) Todos los contratos y acuerdos de nivel de servicio (SLA) con terceros que manejen información o accedan a sistemas del organismo deben incluir cláusulas específicas y legalmente vinculantes de seguridad

- de la información. Estas cláusulas deben establecer, como mínimo:
- (i) La obligación del proveedor de cumplir con las políticas de seguridad del organismo.
 - (ii) Los requisitos de notificación de incidentes de seguridad, incluyendo plazos máximos de reporte.
 - (iii) El derecho del organismo a realizar o solicitar auditorías de seguridad al proveedor.
 - (iv) Las obligaciones de confidencialidad y los procedimientos para la devolución o destrucción segura de la información al finalizar el contrato.
- d) El organismo debe establecer un proceso de monitoreo continuo del desempeño de seguridad de sus proveedores críticos. Este proceso debe incluir revisiones periódicas de los servicios, análisis de informes de auditoría del proveedor y evaluaciones del cumplimiento de las cláusulas contractuales.
- e) El proceso debe incluir un procedimiento formal para la terminación segura de la relación contractual, que garantice:
- (i) La revocación inmediata de todos los accesos lógicos y físicos del proveedor a los sistemas e instalaciones del organismo.
 - (ii) La devolución segura de todos los activos de información propiedad del organismo.
 - (iii) La destrucción segura y verificable de cualquier copia de la información del organismo que pueda residir en los sistemas del proveedor.

Subsección 4.04.2. Requisitos de seguridad en contratos y acuerdos

- a) Todos los contratos, acuerdos de nivel de servicio (SLA) y convenios con terceros (proveedores, socios, contratistas)

que gestionen, procesen, almacenen o accedan a activos de información o sistemas del organismo, deben incluir cláusulas específicas, claras y legalmente vinculantes en materia de seguridad de la información.

- b) Dichas cláusulas contractuales deben establecer, como mínimo, los siguientes requisitos para el tercero:
- (i) **Cumplimiento normativo:** La obligación de cumplir con todas las leyes, regulaciones y normativas de seguridad y protección de datos aplicables al servicio prestado.
 - (ii) **Adhesión a políticas:** La obligación de adherirse y hacer cumplir entre su personal las políticas de seguridad de la información del organismo contratante.
 - (iii) **Confidencialidad:** La obligación de mantener la confidencialidad de la información del organismo, tanto durante la vigencia del contrato como después de su finalización.
 - (iv) **Notificación de incidentes:** La obligación de notificar al organismo sobre cualquier incidente de seguridad que afecte a sus datos o servicios en un plazo máximo definido, que no deberá exceder las 24 horas.
 - (v) **Derecho a auditoría:** El derecho del organismo a realizar auditorías de seguridad, ya sea directamente o a través de un tercero independiente, para verificar el cumplimiento de los controles de seguridad acordados.
 - (vi) **Seguridad en la subcontratación:** Si se permite la subcontratación, el proveedor principal es responsable de asegurar que sus subcontratistas cumplan con los mismos requisitos de seguridad establecidos en el contrato.
 - (vii) **Terminación segura:** Los procedimientos para la devolución o destrucción segura y certificada de la

información del organismo una vez finalizada la relación contractual.

Sección 4.05.

Seguridad en la gestión de recursos humanos

Esta sección establece los requisitos de gobernanza para integrar la seguridad de la información en el ciclo de vida completo del personal. Reconoce que las personas son un elemento central de la seguridad y detalla los mandatos para la creación de programas de concienciación, la formalización de acuerdos de confidencialidad y la gestión segura de los accesos durante toda la relación laboral, desde el ingreso hasta el cese de funciones.

Subsección 4.05.1.

Programa anual de concienciación y capacitación

Apartado 4.05.1.1.

Planificación y contenido del programa:

- a) El organismo debe elaborar un Plan Anual de Capacitación en Seguridad que defina los objetivos, las audiencias, los temas a cubrir, las metodologías a utilizar y el cronograma de actividades.
- b) El programa de concienciación general, dirigido a todo el personal, debe cubrir, como mínimo, las siguientes temáticas fundamentales:
 - (i) La importancia de la Política General de Seguridad de la Información y las consecuencias de su incumplimiento.
 - (ii) El uso seguro de contraseñas y la protección de credenciales.
 - (iii) La identificación y reporte de amenazas comunes, como el phishing y la ingeniería social.

- (iv) La protección de información sensible y el cumplimiento de la política de clasificación de datos.
 - (v) El uso seguro de los activos tecnológicos, incluyendo el correo electrónico, la navegación por internet y los dispositivos móviles.
 - (vi) La seguridad física en el entorno de trabajo.
- c) El programa debe contemplar, adicionalmente, una capacitación especializada y adaptada para el personal con funciones críticas o roles con privilegios elevados, conforme a los requisitos detallados en la **NORTIC A8 – Norma General de Ciberseguridad**.

Apartado 4.05.1.2.

Ejecución y metodología

- a) El programa debe implementarse a través de múltiples formatos para asegurar su alcance y efectividad, tales como sesiones presenciales o virtuales, cursos en línea, boletines informativos, campañas de comunicación interna e infografías.
- b) El programa debe incluir la realización periódica de simulaciones de ataques de ingeniería social, tales como campañas de phishing controladas, con el fin de medir la efectividad de la concienciación, generar retroalimentación y ajustar las estrategias educativas.

Apartado 4.05.1.3.

Seguimiento y medición de la efectividad

- a) El organismo debe mantener un registro de la participación y finalización de las actividades de capacitación por parte de todo el personal.
- b) Deben establecerse mecanismos para evaluar la comprensión de los temas impartidos, utilizando pruebas, ejercicios prácticos o encuestas que permitan medir la madurez del personal en materia de seguridad.

- c) Los resultados de las evaluaciones y de los ejercicios de simulación deben ser analizados y utilizados como insumo para la revisión y mejora continua del programa anual.

Subsección 4.05.2. Acuerdos de confidencialidad y aceptación de políticas

El organismo debe establecer un proceso formal para asegurar que todo el personal, así como los contratistas y terceros con acceso a información o sistemas institucionales, comprendan y acepten formalmente sus responsabilidades en materia de seguridad de la información.

Apartado 4.05.2.1. Proceso de incorporación

- a) Como parte del proceso de contratación e incorporación, todo nuevo colaborador debe firmar un Acuerdo de Confidencialidad y No Divulgación (NDA). Este acuerdo debe establecer claramente las obligaciones del empleado con respecto a la protección de la información sensible y confidencial a la que tendrá acceso, tanto durante su relación laboral como después de su finalización.
- b) El personal, antes de recibir acceso a los sistemas de información, debe recibir una inducción sobre la Política General de Seguridad de la Información y las políticas específicas más relevantes para su rol.
- c) Debe existir una evidencia formal (física o digital) de que cada colaborador ha leído, comprendido y aceptado cumplir con la Política General de Seguridad de la Información. Este registro de aceptación debe ser conservado por el área de Recursos Humanos.

Apartado 4.05.2.2. Mantenimiento durante la relación laboral

- a) El organismo debe implementar un mecanismo para asegurar que el personal confirme su conocimiento y aceptación de la Política General de Seguridad de la Información de forma

periódica, como mínimo, una (1) vez al año.

- b) Cada vez que se realicen actualizaciones significativas en la Política General de Seguridad o en políticas específicas que afecten las responsabilidades del personal, el organismo debe comunicar dichos cambios y requerir una nueva confirmación de lectura y aceptación por parte de los empleados afectados.

Apartado 4.05.2.3.

Aplicabilidad a terceros

- a) Los requisitos de firma de Acuerdos de Confidencialidad y aceptación de políticas deben extenderse a todo personal de terceros, como contratistas, consultores o proveedores, que requieran acceso a los activos de información o a la infraestructura tecnológica del organismo.
- b) Estas obligaciones deben estar claramente estipuladas en las cláusulas contractuales de los servicios correspondientes.

Subsección 4.05.3.

Proceso de cese de funciones y revocación de accesos

El organismo debe implementar y mantener un procedimiento formal y documentado para gestionar el cese de funciones del personal (por renuncia, desvinculación, jubilación o traslado), con el fin de asegurar la revocación oportuna de todos los accesos y la devolución segura de los activos.

Apartado 4.05.3.1. 4.05.3.1. Notificación y coordinación

- a) El área de Recursos Humanos debe ser el punto central responsable de iniciar el proceso de cese de funciones y de notificar de manera formal e inmediata a todas las áreas involucradas, principalmente al departamento de Tecnología de la Información y Comunicación (TIC) y al supervisor directo del colaborador.

- b) El procedimiento debe establecer claramente los plazos máximos para que esta notificación se realice, asegurando que la revocación de los accesos se ejecute, como muy tarde, en el último día laborable del colaborador.

Apartado 4.05.3.2.

Revocación de accesos lógicos

- a) El procedimiento debe garantizar la revocación o desactivación de todas las cuentas de usuario y credenciales de acceso lógico asociadas al colaborador, incluyendo, pero no limitándose a:
- Acceso a la red institucional (Directorio Activo, VPN).
 - Cuentas de correo electrónico.
 - Acceso a aplicaciones y sistemas de información.
 - Acceso a plataformas en la nube y servicios de terceros.
- b) Debe implementarse una lista de verificación (checklist) estandarizada para asegurar que se revisen y revoquen todos los posibles puntos de acceso.

Apartado 4.05.3.3.

Revocación de accesos físicos y devolución de activos

- a) El procedimiento debe incluir la revocación de todos los accesos físicos a las instalaciones, tales como tarjetas de acceso, llaves o permisos biométricos.
- b) El organismo debe asegurar la devolución formal de todos los activos tecnológicos propiedad de la institución que estuvieran asignados al colaborador, incluyendo computadoras portátiles, dispositivos móviles, tokens de autenticación y cualquier otro medio de almacenamiento.

Apartado 4.05.3.4.

Registro y auditoría

- a) Todas las acciones realizadas durante el proceso de cese de funciones (notificación, revocación de accesos, devolución de activos) deben ser documentadas y registradas formalmente.
- b) Esta documentación debe ser conservada como evidencia auditable del cumplimiento del procedimiento, y debe estar firmada por las partes responsables (Recursos Humanos, TIC, supervisor).



EVALUACIÓN DEL DESEMPEÑO Y MEJORA DEL SISTEMA

Este capítulo cierra el ciclo de gestión del SASI. Se enfoca en los mecanismos que garantizan que el sistema de seguridad sea un ente vivo que se mide, se revisa y evoluciona para adaptarse a los cambios en el entorno y mejorar continuamente su eficacia.

Sección 5.01.

Monitoreo y medición del desempeño (KPIs)

El organismo debe establecer un proceso formal para el monitoreo y la medición del desempeño de su Sistema de Administración de la Seguridad de la Información (SASI). El objetivo es evaluar la efectividad de las políticas, los procesos y los controles implementados, y proporcionar a la alta dirección información cuantitativa para la toma de decisiones.

Subsección 5.01.1.

Definición de indicadores clave de desempeño

- a) El organismo debe definir, documentar y mantener un conjunto de Indicadores Clave de Desempeño (KPIs) de seguridad. Estos indicadores deben ser medibles, relevantes y estar alineados con los objetivos de seguridad de la institución.
- b) Los KPIs deben cubrir, como mínimo, la efectividad de los controles y procesos definidos en la NORTIC A8 – Norma

General de Ciberseguridad y en la NORTIC A9 – Norma para la Gestión de Riesgos Tecnológicos y Continuidad Operativa.

- c) La selección de KPIs debe incluir una mezcla equilibrada de indicadores que midan diferentes facetas del programa de seguridad, tales como:
- Indicadores de Cumplimiento: Porcentaje de sistemas con parches de seguridad críticos aplicados a tiempo, porcentaje de empleados que han completado la capacitación anual.
 - Indicadores de Desempeño Operativo: Tiempo medio para detectar un incidente (MTTD), tiempo medio para responder a un incidente (MTTR), porcentaje de disponibilidad de los servicios críticos.
 - Indicadores de Riesgo (KRIs): Número de vulnerabilidades críticas abiertas, número de incidentes de seguridad por mes, resultados de las simulaciones de phishing.

Subsección 5.01.2.

Proceso de medición y recopilación de datos

- a) Deben establecerse procedimientos formales para la recopilación, el análisis y la validación de los datos necesarios para calcular cada KPI.
- b) En la medida de lo posible, la recopilación de datos para los KPIs debe ser automatizada mediante el uso de las herramientas de seguridad y monitoreo de la institución (ej. SIEM, herramientas de escaneo de vulnerabilidades, sistemas de ticketing).
- c) Deben definirse claramente la frecuencia de medición de cada KPI (ej. diaria, semanal, mensual) y los responsables de su recopilación y reporte.

Subsección 5.01.3.

Análisis y reporte a la dirección

- a) Los resultados de los KPIs deben ser analizados en series temporales para identificar tendencias, patrones, desviaciones y áreas que requieran una acción de mejora.
- b) Se deben generar informes periódicos o cuadros de mando que presenten el estado del desempeño del SASI de una manera clara y visual para la alta dirección y el CIGETIC.
- c) Estos informes deben servir como el principal insumo para la Revisión por la Dirección (definida en la Sección 5.3 de esta norma), facilitando una toma de decisiones basada en datos sobre la asignación de recursos, la priorización de iniciativas y los ajustes a la estrategia de seguridad.

Sección 5.02.

Auditoría interna del SASI

El organismo debe establecer y mantener un programa de auditoría interna para evaluar de forma objetiva e independiente si el Sistema de Administración de la Seguridad de la Información (SASI) cumple con los requisitos de esta norma, con las políticas y procedimientos propios de la institución, y si está implementado y mantenido de manera eficaz.

Subsección 5.02.1.

Programa de auditoría anual

- a) El organismo debe planificar y ejecutar un ciclo completo de auditorías internas que cubra todos los aspectos del SASI, incluyendo las políticas, los procesos de gobernanza y los controles definidos en las NORTIC A7, A8 y A9, con una frecuencia mínima de una (1) vez al año.
- b) Se debe elaborar un Programa Anual de Auditoría que defina el alcance, los objetivos, la frecuencia y los métodos para cada auditoría planificada. La planificación debe basarse en el riesgo,

dando prioridad a las áreas y procesos de mayor criticidad para la organización.

- c) El programa de auditoría debe asegurar que los auditores sean independientes de las áreas que auditan, para garantizar la objetividad e imparcialidad de los hallazgos. El personal no puede auditar su propio trabajo.

Subsección 5.02.2.**Competencia y selección de auditores**

- a) Las auditorías internas deben ser realizadas por personal con el conocimiento y la competencia adecuados en principios de auditoría, seguridad de la información y en las normativas aplicables.
- b) El organismo podrá utilizar personal interno debidamente capacitado (como la unidad de auditoría interna) o contratar los servicios de auditores externos independientes para ejecutar el programa de auditoría.

Subsección 5.02.3.**Proceso de ejecución de la auditoría**

- a) Cada auditoría debe seguir un proceso formal y documentado que incluya, como mínimo: la planificación de la auditoría, la realización de reuniones de apertura, la recopilación de evidencia (mediante entrevistas, revisión de documentos y pruebas de controles), la evaluación de los hallazgos y la celebración de una reunión de cierre.
- b) Los hallazgos de la auditoría deben clasificarse según su severidad (ej. No Conformidad Mayor, No Conformidad Menor, Oportunidad de Mejora) y deben documentarse con la evidencia objetiva correspondiente.

Subsección 5.02.4.**Informe de auditoría y seguimiento**

- a) Los resultados de cada auditoría deben documentarse en un Informe de Auditoría Interna formal. Este informe debe ser

comunicado a los responsables de las áreas auditadas y a la alta dirección a través del CIGETIC.

- b) El informe debe ser un insumo fundamental para la Revisión por la Dirección (definida en la Sección 5.3) y para el proceso de Gestión de Hallazgos y Acciones de Mejora (definido en la Sección 5.4).

Sección 5.03.

Revisión por la dirección

La Máxima Autoridad Ejecutiva (MAE) debe revisar el Sistema de Administración de la Seguridad de la Información (SASI) del organismo a intervalos planificados, con una frecuencia mínima de una (1) vez al año, para asegurar su continua idoneidad, adecuación y eficacia.

Subsección 5.03.1.

Planificación y convocatoria

- a) La revisión por la dirección debe ser una reunión formal, convocada y presidida por la MAE o el nivel directivo que esta designe.
- b) El Comité de Implementación y Gestión de Estándares TIC (CIGETIC), a través del Responsable de Seguridad de la Información (CISO o rol equivalente), debe ser el encargado de preparar la agenda y la documentación necesaria para la revisión.

Subsección 5.03.2.

Elementos de entrada para la revisión

- a) La Revisión por la Dirección debe considerar y analizar, como mínimo, la siguiente información de entrada:
 - (i) El estado de las acciones derivadas de las revisiones por la dirección anteriores.
 - (ii) Los resultados de la medición del desempeño del SASI,

incluyendo el análisis de los Indicadores Clave de Desempeño (KPIs).

- (iii) Los resultados de las auditorías internas y externas, incluyendo el estado de las no conformidades y las acciones correctivas.
- (iv) El estado de la implementación del Plan de Tratamiento de Riesgos.
- (v) Los incidentes de seguridad significativos ocurridos desde la última revisión y las lecciones aprendidas.
- (vi) Cambios en el contexto interno o externo que puedan impactar al SASI, tales como nuevas amenazas, cambios en el marco legal o modificaciones en la estrategia del organismo.
- (vii) La retroalimentación de las partes interesadas relevantes.

Subsección 5.03.3. Elementos de salida y toma de decisiones

- a) Como resultado de la revisión, se deben tomar decisiones estratégicas relacionadas con las oportunidades de mejora continua del SASI. Las salidas de la reunión deben incluir, como mínimo:
 - (i) Decisiones sobre cambios necesarios en las políticas, objetivos o en la dirección estratégica de la seguridad de la información.
 - (ii) La asignación o reasignación de recursos necesarios para abordar las deficiencias identificadas o para impulsar nuevas iniciativas de seguridad.
 - (iii) La aprobación de planes de acción para la mejora del desempeño del SASI.

Subsección 5.03.4.

Documentación

- a) Los resultados, decisiones y planes de acción derivados de la Revisión por la Dirección deben ser documentados formalmente a través de un acta de reunión o un informe de conclusiones.
- b) Esta documentación debe ser conservada como evidencia auditable del ejercicio de la gobernanza y la supervisión por parte de la alta dirección.

Sección 5.04.

Gestión de hallazgos y acciones de mejora

El organismo debe establecer y mantener un proceso formal para documentar, analizar y dar seguimiento a todos los hallazgos y no conformidades identificadas, asegurando que se implementen y se verifique la eficacia de las acciones de mejora correspondientes.

Subsección 5.04.1.

Registro centralizado de hallazgos

- a) Debe implementarse un registro centralizado para documentar todos los hallazgos que requieran una acción correctiva o de mejora.
- b) Este registro debe incluir, como mínimo, los hallazgos provenientes de:
 - Auditorías internas y externas.
 - Revisiones por la Dirección.
 - Resultados de la medición de KPIs que indiquen un bajo desempeño.
 - Lecciones aprendidas de incidentes de seguridad.
 - Resultados de pruebas y simulacros de continuidad.

- Cualquier otra revisión o evaluación del SASI.

Subsección 5.04.2.**Análisis de causa raíz y plan de acción**

- a) Para cada no conformidad identificada, el organismo debe realizar un análisis para determinar su causa raíz y evitar su recurrencia.
- b) Basado en el análisis, debe elaborarse un Plan de Acción Correctiva. Este plan debe documentar, como mínimo:
 - La descripción de la no conformidad y su causa raíz.
 - Las acciones correctivas específicas que se implementarán.
 - El responsable asignado para la ejecución de cada acción.
 - Los plazos y fechas compromiso para la finalización.

Subsección 5.04.3.**Implementación y seguimiento**

- a) Las acciones correctivas definidas en el plan deben ser implementadas de acuerdo con los plazos establecidos.
- b) El CIGETIC, a través del Responsable de Seguridad de la Información, debe realizar un seguimiento continuo del progreso de los planes de acción.
- c) El estado de los hallazgos y sus correspondientes planes de acción debe ser un punto de revisión obligatorio en las reuniones periódicas del CIGETIC.

Subsección 5.04.4.**Verificación de la eficacia y cierre**

- a) Una vez que una acción correctiva ha sido implementada, debe realizarse una verificación para confirmar que la acción fue eficaz y que la no conformidad ha sido eliminada de forma permanente.

- b) Solo después de una verificación exitosa, el hallazgo podrá ser formalmente cerrado en el registro centralizado.
- c) La evidencia de la implementación y de la verificación de la eficacia debe ser conservada como registro auditable.

Subsección 5.04.5.**Oportunidades de mejora**

- a) El organismo debe identificar y gestionar no solo las no conformidades (acciones reactivas), sino también las oportunidades de mejora (acciones proactivas) para fortalecer continuamente el SASI.

BIBLIOGRAFÍA

1. Center for Internet Security. (2021). CIS critical security controls v8. <https://www.cisecurity.org/controls/>
2. Cloud Security Alliance. (2011). Security guidance for critical areas of focus in cloud computing v3.0. <https://cloudsecurityalliance.org/guidance/csaguidance.v3.0.pdf>
3. Dirección de Tecnologías de Información y Comunicaciones. (2007). Manual para elaborar un plan de continuidad de la gestión en tecnologías de información y comunicaciones. Gobierno de Costa Rica.
4. International Organization for Standardization. (2018). ISO/IEC 27005:2018 – Information technology – Security techniques – Information security risk management. ISO.
5. International Organization for Standardization. (2019). ISO 22301:2019 – Security and resilience – Business continuity management systems – Requirements. ISO.
6. International Organization for Standardization. (2022). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. ISO.
7. International Organization for Standardization. (2022). ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection – Information security controls. ISO.
8. Ministerio de Hacienda y Administraciones Públicas; Centro Criptológico Nacional. (2013). Guía/Norma de seguridad de las TIC: Seguridad en entornos cloud. Gobierno de España.
9. Ministerio de Industria, Turismo y Comercio; Instituto Nacional de Tecnologías de la Comunicación. (2011). Guía sobre almacenamiento y borrado seguro de la información. Gobierno de España.

10. National Institute of Standards and Technology. (2010). NIST Special Publication 800-34 Rev. 1: Contingency planning guide for federal information systems. U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-34r1>
11. National Institute of Standards and Technology. (2012). NIST Special Publication 800-30 Rev. 1: Guide for conducting risk assessments. U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-30r1>

ABREVIATURAS Y ACRÓNIMOS

No.	Abreviaturas y Acrónimos	Inglés	Español
1	BCP	Business Continuity Plan	Plan de Continuidad de Negocio
2	BIA	Business Impact Analysis	Análisis de Impacto del Negocio
3	CIGETIC	N/A	Comité de Implementación y Gestión de Estándares TIC
4	DRP	Disaster Recovery Plan	Plan de Recuperación de Desastres
5	ISCP	Information System Contingency Plan	Plan de Contingencia de sistemas de Información
6	ISO	International Organization for Standardization	Organización Internacional de Normalización
7	KPI	Key Performance Indicator	Indicador Clave de Desempeño
8	MAC Address	Media Access Control Address	Dirección de Control Acceso al Medio
9	MAP	N/A	Ministerio de Administración Pública
10	NIST	National Institute of Standards and Technology	Instituto Nacional de Estándares y Tecnología
11	OGTIC	N/A	Oficina Gubernamental de Tecnologías de la Información y Comunicación
12	RPO	Recovery Point Objective	Objetivo de Punto de Recuperación
13	RTO	Recovery Time Objective	Objetivo de Tiempo de Recuperación

14	SLA	Service Level Agreement	Acuerdo de Nivel servicio
15	SSID	Service Set Identifier	Identificador de Conjunto de Servicios
16	TIC	N/A	Tecnología de la Información y Comunicación

ANEXOS

Anexo A: Matriz de controles por nivel de madurez

Bloque 1: GOBERNANZA Y FUNDAMENTOS					
Capacidad 1: Liderazgo y compromiso institucional					
ID	Fuente	Práctica / Requisito	MIL 1	MIL 2	MIL 3
GOB-01	A7:2.3	Establecer y aprobar la Política General de Seguridad. La institución elabora y mantiene una Política General de Seguridad de la Información, la cual es formalmente aprobada por la MAE con evidencia documental.	✓	✓	✓
GOB-02	A7:2.1	Documentar la asignación de recursos para la seguridad. La asignación de recursos para el programa de seguridad se documenta en los instrumentos de planificación de la institución (Plan Operativo Anual, presupuesto).	✓	✓	✓
GOB-03	A7:2.1	Demostrar el liderazgo y patrocinio activo de la MAE. Se evidencia la participación y visible de la MAE en la promoción de una cultura de seguridad (comunicaciones, respaldo a programas, etc.).	✓	✓	✓
GOB-04	A7:5.3	Ejecutar un proceso formal de Revisión por la Dirección. La MAE o un nivel directivo designado lidera una revisión formal, al menos una vez al año, para evaluar la idoneidad y eficacia del SASI.		✓	✓
GOB-05	A7:5.1	Gestionar el desempeño del SASI mediante métricas (KPIs). Se definen, miden y analizan Indicadores Clave de Desempeño (KPIs) de seguridad, y sus resultados son utilizados como insumo en la Revisión por la Dirección.			✓
Capacidad 2: Estructura organizativa y roles de seguridad					
ID	Fuente	Práctica / Requisito	MIL 1	MIL 2	MIL 3
GOB-06	A7:2.2, Res. 342-2024	Establecer y operar la función de Ciberseguridad. Se designa formalmente un Responsable de Seguridad (CISO o equivalente) y se establece una Unidad de Ciberseguridad, conforme a la estructura mínima definida por el órgano rector.	✓	✓	✓

GOB-07	A7:2.2, Res. 342-2024	Asegurar la autoridad e independencia de la función de seguridad. La estructura organizacional garantiza que el Responsable de Seguridad posee la autoridad y línea de reporte directo a la alta dirección necesarias para la supervisión efectiva del programa, conforme lo establece el órgano rector.	✓	✓	✓
GOB-08	A7:2.3	Operar un Comité de Gobernanza de Seguridad (CIGETIC). Se conforma y opera un comité multidisciplinario (CIGETIC) que se reúne periódicamente de forma documentada (actas) para la supervisión de la implementación de las normas.	✓	✓	✓
GOB-09	A7:2.2	Definir y documentar las responsabilidades de seguridad en toda la organización. Se definen, documentan y comunican formalmente los roles y responsabilidades de seguridad para todo el personal, desde la alta dirección hasta los usuarios finales.		✓	✓
GOB-10	A7:2.2	Integrar las responsabilidades de seguridad en los procesos de RRHH. Las responsabilidades de seguridad se integran formalmente en las descripciones de puestos y en los criterios de evaluación de desempeño del personal.			✓
Capacidad 3: Marco normativo y político de seguridad					
ID	Fuente	Práctica / Requisito	MIL 1	MIL 2	MIL 3
GOB-11	A7:2.03.1	Establecer y aprobar la Política General de Seguridad de la Información. La institución elabora, documenta y mantiene una Política General de alto nivel, aprobada por la MAE, que establece la dirección estratégica y los principios de seguridad.	✓	✓	✓
GOB-12	A7:2.03	Desarrollar y mantener un marco de políticas y procedimientos derivados. A partir de la Política General, el organismo desarrolla y documenta las políticas o procedimientos específicos necesarios para gobernar.		✓	✓
GOB-13	A7:5.3	Revisar y actualizar periódicamente el marco documental. Se implementa un proceso formal, como parte de la Revisión por la Dirección, para la revisión y actualización de todo el conjunto de políticas y procedimientos de seguridad, asegurando su continua relevancia y eficacia.			✓
Capacidad 4: Gestión de activos y clasificación de la información					
ID	Fuente	Práctica / Requisito	MIL 1	MIL 2	MIL 3
ACT-01	A9:3.03.1	Mantener un inventario de activos tecnológicos críticos. Se establece y mantiene un inventario que identifique los activos tecnológicos que soportan los procesos críticos del organismo (ej. servidores, aplicaciones principales, equipos de red).	✓	✓	✓

ACT-02	A7:2.4	Aplicar un esquema de clasificación de la información. Se aplica el esquema de clasificación de la información definido en la política, asignando un nivel de sensibilidad (ej. Pública, Interna, Confidencial) a los principales repositorios de datos.	✓	✓	✓
ACT-03	A7:4.2	Asignar propietarios a los activos de información. Se asigna formalmente un propietario (un rol o área de negocio) a cada activo de información crítico, quien será responsable de su protección y uso adecuado.		✓	✓
ACT-04	A8:2.01.1	Mantener un inventario detallado de todos los activos tecnológicos. El inventario de activos tecnológicos se expande para incluir todos los dispositivos físicos bajo gestión, con atributos detallados (ubicación, responsable, etc.).		✓	✓
ACT-05	A7:2.4	Implementar el etiquetado y manejo seguro de activos. Se implementan procedimientos para el etiquetado (físico o digital) de los activos según su clasificación, y se aplican las reglas de manejo seguro correspondientes.		✓	✓
ACT-06	A8:2.01.2	Mantener un inventario de plataformas y software. Se establece y mantiene un inventario de todas las plataformas y aplicaciones de software utilizadas, garantizando el control sobre las versiones y licencias.			✓
ACT-07	A8:2.01.1.d	Utilizar herramientas automatizadas para el descubrimiento de activos. Se emplean herramientas tecnológicas para el descubrimiento automático y continuo de activos en la red, asegurando que el inventario se mantenga preciso y actualizado.			✓
Bloque 2: GESTIÓN DE RIESGOS Y DEFENSA PROACTIVA					
Capacidad 5: Gestión de riesgos de seguridad de la información					
ID	Fuente	Práctica / Requisito	MIL 1	MIL 2	MIL 3
RIS-01	A9:2.02	Identificar y registrar los riesgos de seguridad principales. Se identifican y mantienen en un registro los riesgos de seguridad más evidentes y de alto impacto para los activos y procesos críticos del organismo.	✓	✓	✓
RIS-02	A9:2.02	Ejecutar un proceso formal de análisis y evaluación de riesgos. Se establece y ejecuta un proceso documentado para identificar amenazas y vulnerabilidades, y evaluar el riesgo (Probabilidad x Impacto) de forma sistemática, al menos una vez al año.		✓	✓
RIS-03	A7:4.1	Elaborar y aprobar un Plan de Tratamiento de Riesgos. Como resultado del análisis, se elabora un Plan de Tratamiento que detalla las estrategias de respuesta (mitigar, aceptar, etc.) para cada riesgo, el cual es formalmente aprobado por la dirección.		✓	✓

RIS-04	A7:4.2	Crear y mantener una Declaración de Aplicabilidad (SoA). Se elabora y mantiene un SoA que lista los controles de las NORTIC A8 y A9, justificando su implementación o exclusión basándose en el Plan de Tratamiento de Riesgos.		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
RIS-05	A9:2.01	Asegurar que la gestión de riesgos forme parte de la toma de decisiones. Se evidencia que los resultados del análisis de riesgos son utilizados como un insumo para la toma de decisiones estratégicas por parte de la alta dirección y el CIGETIC.			<input checked="" type="checkbox"/>
RIS-06	A8:2.02.2	Integrar la inteligencia de amenazas en la gestión de riesgos. El proceso de gestión de riesgos se nutre proactivamente de fuentes de inteligencia de amenazas para anticipar y evaluar nuevas tácticas de ataque y vulnerabilidades emergentes.			<input checked="" type="checkbox"/>
Capacidad 6: Gestión de la seguridad en recursos humanos					
ID	Fuente	Práctica / Requisito	MIL 1	MIL 2	MIL 3
HUM-01	A7:4.3	Implementar un proceso de cese de funciones seguro. Se implementa y sigue un procedimiento formal para la revocación inmediata de todos los accesos lógicos y físicos y la devolución de activos cuando un empleado o contratista cesa sus funciones.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HUM-02	A7:4.3	Formalizar acuerdos de confidencialidad. Se requiere que todo el personal y los terceros relevantes firmen Acuerdos de Confidencialidad y No Divulgación (NDA) como parte de su proceso de incorporación.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HUM-03	A8:3.02.1	Ejecutar un programa de concientización y capacitación. Se implementa y mantiene un programa anual y formal de concientización y capacitación en seguridad para todo el personal, con seguimiento documentado de la participación.		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HUM-04	A8:3.02.2	Proveer capacitación especializada para roles críticos. Se identifican los roles con funciones críticas o acceso privilegiado y se les provee capacitación técnica especializada y adaptada a los riesgos de sus funciones.		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HUM-05	A7:4.3	Medir la efectividad del programa de concientización. Se establecen y utilizan mecanismos para evaluar la comprensión y la madurez del personal en materia de seguridad, tales como simulaciones de ataques de ingeniería social (ej. campañas de phishing controladas).			<input checked="" type="checkbox"/>
Capacidad 7: Seguridad física y ambiental					
ID	Fuente	Práctica / Requisito	MIL 1	MIL 2	MIL 3
DEF-01	A8:3.05.2	Implementar controles de acceso físico a áreas críticas. Se implementan y mantienen medidas de control de acceso físico (ej. cerraduras, control de acceso electrónico) para proteger áreas críticas como centros de datos y salas de comunicaciones.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

DEF-02	A8:3.05.2	Mantener un registro de acceso físico. Se mantienen registros de acceso físico actualizados para las áreas críticas, que incluyan, como mínimo, la identidad de la persona, la fecha y la hora de entrada y salida.	✓	✓	✓
DEF-03	A8:3.05.2	Implementar medidas de protección ambiental. Se implementan medidas básicas de protección contra amenazas ambientales en los centros de datos, incluyendo detectores de humo y sistemas de supresión de incendios.		✓	✓
DEF-04	A8:3.05.2	Implementar vigilancia y monitoreo físico. Se despliegan sistemas de vigilancia física (ej. cámaras de CCTV) en las áreas críticas para monitorear y registrar la actividad.		✓	✓
DEF-05	A8:3.05.2	Implementar sistemas de climatización y energía redundantes. Los centros de datos críticos cuentan con unidades de climatización (HVAC) y sistemas de alimentación ininterrumpida (UPS) con capacidad de redundancia.			✓
Capacidad 8: Gestión de identidades y control de acceso lógico					
ID	Fuente	Práctica / Requisito	MIL 1	MIL 2	MIL 3
DEF-06	A8:3.01.5	Aplicar el principio de mínimo privilegio. Se establecen y aplican mecanismos para asegurar que a cada usuario se le asigne únicamente el nivel de acceso y los privilegios necesarios para el desempeño de sus responsabilidades.	✓	✓	✓
DEF-07	A8:3.01.1	Gestionar el ciclo de vida de las identidades y credenciales. Se implementa un proceso formal para la emisión, modificación y revocación de identidades y credenciales de acceso, asegurando que solo los usuarios autorizados tengan acceso.	✓	✓	✓
DEF-08	A8:3.01.3	Implementar autenticación multifactor (MFA) para accesos críticos. Se requiere el uso obligatorio de MFA para todos los accesos a recursos críticos, sistemas con información sensible, administración de infraestructuras y servicios expuestos externamente.		✓	✓
DEF-09	A8:3.01.5	Implementar la separación de funciones (SoD) para tareas críticas. Se establecen mecanismos para asegurar que las tareas críticas (ej. aprobación y ejecución de pagos) no puedan ser realizadas por una misma persona sin controles compensatorios.		✓	✓
DEF-10	A7:5.2	Realizar revisiones periódicas de los derechos de acceso. Se implementa un proceso formal para la revisión periódica (al menos semestral) de las autorizaciones de acceso, con el fin de validar su vigencia, necesidad y adecuación al rol funcional.		✓	✓
DEF-11	A8:3.01.2	Implementar mecanismos de autenticación adaptativa. Se implementan mecanismos que ajustan dinámicamente el nivel de autenticación requerido según el riesgo contextual de la conexión (ubicación, dispositivo, comportamiento).			✓

Capacidad 9: Protección de datos y criptografía					
ID	Fuente	Práctica / Requisito	MIL 1	MIL 2	MIL 3
DEF-12	A8:3.03.1	Implementar controles de cifrado para datos en reposo. Se implementan mecanismos de cifrado robusto para proteger la confidencialidad de los datos sensibles almacenados en servidores, bases de datos y soportes de respaldo.	✓	✓	✓
DEF-13	A8:3.03.2	Implementar controles de cifrado para datos en tránsito. Se utiliza cifrado robusto (ej. TLS 1.2 o superior) para proteger todas las comunicaciones que transmitan información sensible a través de redes internas y externas.	✓	✓	✓
DEF-14	A8:3.03.1	Gestionar el ciclo de vida de las claves criptográficas. Se establecen y siguen procedimientos seguros y documentados para la generación, almacenamiento, uso, rotación y destrucción de las claves criptográficas utilizadas en la institución.		✓	✓
DEF-15	A8:3.03.3	Implementar controles para la protección de datos en uso. Se aplican técnicas de protección (ej. aislamiento de procesos, limpieza de memoria) para salvaguardar datos confidenciales mientras son procesados por los sistemas.			✓
Capacidad 10: Gestión de vulnerabilidades técnicas					
ID	Fuente	Práctica / Requisito	MIL 1	MIL 2	MIL 3
DEF-16	A8:2.02.1	Aplicar parches de seguridad. Se implementa un proceso para la aplicación oportuna de parches de seguridad, priorizando aquellos catalogados como "críticos" por los fabricantes, en todos los sistemas y aplicaciones.	✓	✓	✓
DEF-17	A8:2.02.1	Realizar escaneos de vulnerabilidades. Se ejecutan escaneos de vulnerabilidades periódicos (al menos trimestrales) sobre la infraestructura tecnológica para identificar debilidades técnicas.	✓	✓	✓
DEF-18	A7:4.1	Establecer un programa formal de gestión de vulnerabilidades. Se documenta y aprueba una política y un procedimiento que definen el ciclo de vida completo: descubrimiento, análisis, priorización basada en riesgo y remediación.		✓	✓
DEF-19	A8:2.02.1	Mantener un repositorio centralizado de vulnerabilidades. Las vulnerabilidades identificadas se registran y gestionan en un repositorio o sistema de tickets que permita su seguimiento, asignación y verificación de cierre.		✓	✓
DEF-20	A8:2.03.2	Realizar pruebas de penetración externas. Se contratan pruebas de penetración por parte de terceros independientes, de forma periódica (al menos anualmente), para validar de forma objetiva la eficacia de los controles de seguridad.			✓

Capacidad 11: Configuración segura y gestión de cambios					
ID	Fuente	Práctica / Requisito	MIL 1	MIL 2	MIL 3
DEF-21	A8:3.04	Aplicar configuraciones seguras (hardening) a sistemas críticos. Se aplican configuraciones de seguridad básicas a los sistemas operativos, servidores y equipos de red críticos para eliminar servicios y puertos innecesarios y proteger contra vulnerabilidades comunes.	✓	✓	✓
DEF-22	A8:3.04.1	Implementar un proceso formal de gestión de cambios. Se establece y sigue un proceso documentado para solicitar, evaluar, aprobar, implementar y registrar todos los cambios en la infraestructura y sistemas críticos.		✓	✓
DEF-23	A8:3.04	Establecer y mantener líneas base de configuración segura. Se documentan, aprueban y mantienen configuraciones estándar de seguridad (líneas base) para los principales tipos de activos tecnológicos de la institución.		✓	✓
DEF-24	A8:3.04.1	Integrar la evaluación de riesgos en el proceso de gestión de cambios. Todo cambio significativo es precedido por una evaluación formal de riesgos de seguridad para analizar su impacto potencial, y sus resultados son documentados como parte de la aprobación.			✓
DEF-25	A7:5.1	Automatizar la verificación de la integridad de las configuraciones. Se utilizan herramientas tecnológicas para monitorear de forma continua los sistemas críticos y generar alertas ante desviaciones no autorizadas de las líneas base de configuración segura.			✓
Capacidad 12: Seguridad de redes y perímetro					
ID	Fuente	Práctica / Requisito	MIL 1	MIL 2	MIL 3
DEF-26	A8:3.05.1	Implementar defensas perimetrales. Se implementan y mantienen firewalls de red para controlar el tráfico entre las redes internas y externas, bloqueando por defecto todo el tráfico no autorizado explícitamente.	✓	✓	✓
DEF-27	A8:3.05.1	Implementar la segmentación de la red. Se divide y aísla la red interna en segmentos lógicos (ej. VLANs) para separar los sistemas críticos de las redes de usuarios generales, limitando la propagación de amenazas.		✓	✓
DEF-28	A8:3.05.1	Implementar defensas contra ataques de denegación de servicio (DoS/DDoS). Se aplican medidas técnicas para asegurar la resiliencia de los servicios expuestos a internet ante ataques de denegación de servicio.		✓	✓

DEF-29	A8:4.02.1	Implementar herramientas de monitoreo de tráfico de red. Se despliegan herramientas (ej. IDS/IPS, NDR) para inspeccionar el tráfico de red, identificar comportamientos anómalos o maliciosos y generar alertas.			<input checked="" type="checkbox"/>
DEF-30	A8:3.05.1	Implementar una arquitectura de Zero Trust para accesos críticos. Se implementan arquitecturas de microsegmentación y mecanismos de autenticación y autorización estrictos para los accesos a las zonas más críticas de la red (DMZ, redes de control).			<input checked="" type="checkbox"/>
Capacidad 13: Seguridad en el desarrollo de aplicaciones (SDLC)					
ID	Fuente	Práctica / Requisito	MIL 1	MIL 2	MIL 3
DEF-31	A8:3.04.4	Aplicar prácticas básicas de codificación segura. Los equipos de desarrollo siguen prácticas fundamentales de seguridad en la codificación de aplicaciones, como la validación de todas las entradas de usuario para prevenir ataques de inyección (ej. SQLi, XSS).	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEF-32	A8:3.04.4	Implementar un Ciclo de Vida de Desarrollo Seguro (SDLC). Se elabora e implementa un SDLC institucional que integra formalmente actividades y controles de seguridad en cada una de sus fases (planificación, diseño, desarrollo, pruebas, etc.).		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEF-33	A8:3.04.4	Realizar revisiones de código y pruebas de seguridad. Se incorporan pruebas de seguridad específicas como parte de la validación funcional, incluyendo análisis estático de código (SAST) y análisis dinámico de aplicaciones (DAST).		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DEF-34	A8:3.04.4	Proveer formación en desarrollo seguro a los equipos. Los equipos de desarrollo, diseño y gestión de proyectos reciben formación periódica y concientización en desarrollo seguro.			<input checked="" type="checkbox"/>
DEF-35	A8:3.04.4	Gestionar la seguridad de los componentes de terceros. Se implementan revisiones sistemáticas del código fuente y análisis de composición de software (SCA) para asegurar el uso de librerías confiables y sin vulnerabilidades conocidas.			<input checked="" type="checkbox"/>
Capacidad 14: Gestión de riesgos de la cadena de suministro					
ID	Fuente	Práctica / Requisito	MIL 1	MIL 2	MIL 3
RIS-07	A7:4.04	Incluir requisitos de seguridad en contratos y acuerdos. Todos los contratos y acuerdos de nivel de servicio (SLA) con terceros que gestionen información o sistemas críticos incluyen cláusulas específicas y legalmente vinculantes de seguridad.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
RIS-08	A7:4.04	Implementar un proceso de debida diligencia de seguridad para proveedores. Se ejecuta un proceso de evaluación de la postura de seguridad de los proveedores críticos antes de formalizar cualquier relación contractual.		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

RIS-09	A7:4.04	Establecer una política de gestión de riesgos de la cadena de suministro. Se exige la implementación de procesos formales para la identificación, evaluación, mitigación y supervisión continua de los riesgos de ciberseguridad introducidos por proveedores y terceros.		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
RIS-10	A8:2.02.9	Realizar evaluaciones periódicas de seguridad a proveedores. Se realizan evaluaciones y auditorías de seguridad periódicas a los proveedores críticos para verificar el cumplimiento continuo de los requisitos contractuales.			<input checked="" type="checkbox"/>
RIS-11	A7:4.04	Integrar a los proveedores en los planes de respuesta a incidentes. Se establecen y prueban protocolos para la notificación, comunicación y colaboración con proveedores críticos durante la gestión de un incidente de seguridad.			<input checked="" type="checkbox"/>
Bloque 3: OPERACIONES DE SEGURIDAD, RESILIENCIA Y MEJORA					
Capacidad 15: Detección y monitoreo de eventos de seguridad					
ID	Fuente	Práctica / Requisito	MIL 1	MIL 2	MIL 3
DET-01	A8:3.04.3	Generar y recolectar registros de auditoría (logs) de sistemas críticos. Se configuran los sistemas, aplicaciones y dispositivos de red críticos para generar registros (logs) de eventos relevantes para la seguridad.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DET-02	A8:4.01.1	Establecer y mantener líneas base operacionales. Se definen y documentan los patrones normales de operación (tráfico, autenticaciones, uso de servicios) para poder identificar desviaciones significativas.		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DET-03	A8:4.01.2	Centralizar y proteger los registros de auditoría. Los registros (logs) generados por los sistemas críticos se envían a un repositorio centralizado para su almacenamiento, protección y análisis.		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DET-04	A8:4.02.1	Implementar un sistema de detección de intrusiones (IDS/IPS). Se despliegan herramientas especializadas para inspeccionar el tráfico de red, identificar comportamientos maliciosos y generar alertas en tiempo real.		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DET-05	A8:4.01.2	Implementar una plataforma SIEM para la correlación automatizada de eventos. Se implementa y opera una solución SIEM que permita la correlación automática de eventos de múltiples fuentes para detectar amenazas complejas.			<input checked="" type="checkbox"/>
DET-06	A8:4.02.3	Monitorear la actividad del personal para detectar comportamientos de riesgo. Se implementan procedimientos y herramientas (ej. UEBA) para analizar el comportamiento de los usuarios, detectar actividades atípicas y señales de abuso de privilegios.			<input checked="" type="checkbox"/>

Capacidad 16: Gestión de incidentes de seguridad					
ID	Fuente	Práctica / Requisito	MIL 1	MIL 2	MIL 3
INC-01	A8:5.03	Establecer un punto de contacto y notificar los incidentes. Se define y comunica un punto de contacto formal para el reporte de incidentes. Se cumple con la notificación obligatoria a las autoridades nacionales (CSIRT-RD) conforme a la regulación.	✓	✓	✓
INC-02	A8:5.01	Implementar un Plan de Respuesta a Incidentes (PRI). Se desarrolla, documenta y mantiene un PRI que define el ciclo de vida de la gestión de incidentes (preparación, identificación, contención, erradicación, recuperación y lecciones aprendidas).		✓	✓
INC-03	A8:5.01	Establecer y operar un Equipo de Respuesta a Incidentes. Se designa formalmente un equipo (interno o externo) con los roles y responsabilidades definidos para gestionar la respuesta a incidentes de seguridad.		✓	✓
INC-04	A8:5.01.1	Implementar un proceso para la categorización y priorización de incidentes. Se utiliza un esquema formal para clasificar los incidentes según su impacto y severidad, permitiendo una priorización eficiente de la respuesta.		✓	✓
INC-05	A8:5.04.2	Establecer un proceso de lecciones aprendidas post-incidente. Se implementa un proceso formal para analizar cada incidente significativo, identificar la causa raíz y las lecciones aprendidas, y utilizar esta información para la mejora continua.			✓
INC-06	A8:5.02.2	Establecer capacidades de análisis técnico y forense. Se cuenta con los recursos, herramientas y procedimientos (internos o externos) para realizar análisis forense digital cuando la naturaleza del incidente lo requiera.			✓
INC-07	A7:5.1	Medir la efectividad del proceso de respuesta a incidentes. Se definen y monitorean indicadores Clave de Desempeño (KPIs), como el "Tiempo Medio para Detectar" (MTTD) y el "Tiempo Medio para Responder" (MTTR), para evaluar y mejorar la eficacia del proceso.			✓
Capacidad 17: Gestión de la continuidad operativa					
ID	Fuente	Práctica / Requisito	MIL 1	MIL 2	MIL 3
CON-04	A9:4.03	Desarrollar Planes de Contingencia para Sistemas Críticos (ISCP). Se documentan y mantienen planes de contingencia para la recuperación de sistemas de información críticos específicos ante interrupciones leves o moderadas.	✓	✓	✓

CON-05	A9:3.02	Realizar un Análisis de Impacto al Negocio (BIA). Se ejecuta y documenta un BIA formal para identificar los procesos críticos, sus dependencias, y definir los objetivos de recuperación (RTO/RPO) para toda la institución.		✓	✓
CON-06	A9:4.02	Desarrollar y mantener un Plan de Recuperación ante Desastres (DRP). Se desarrolla un DRP documentado que detalla los procedimientos para la recuperación de la infraestructura tecnológica crítica, basado en los resultados del BIA.		✓	✓
CON-07	A9:4.01	Desarrollar y mantener un Plan de Continuidad de Negocio (BCP). Se desarrolla un BCP a nivel institucional que define cómo la organización mantendrá sus funciones de negocio críticas durante una interrupción, incluyendo la gestión de crisis y las comunicaciones.		✓	✓
CON-08	A9:3.01	Integrar la gestión de riesgos en la planificación de la continuidad. Se asegura que la política y los planes de continuidad se basen en la metodología y los resultados del proceso de gestión de riesgos del organismo.			✓
Capacidad 18: Pruebas, validación y resiliencia					
ID	Fuente	Práctica / Requisito	MIL 1	MIL 2	MIL 3
CON-09	A9:4.04	Realizar pruebas periódicas de restauración de copias de seguridad. Se ejecutan pruebas de restauración de las copias de seguridad de los sistemas y datos críticos, al menos semestralmente, para validar su integridad y la viabilidad de la recuperación.	✓	✓	✓
CON-10	A9:4.04	Establecer un programa formal de pruebas y ejercicios de continuidad. Se establece y mantiene un programa formal para validar periódicamente la efectividad de todos los planes de continuidad (BCP, DRP, ISCP), asegurando que se mantengan actualizados.		✓	✓
CON-11	A9:4.04	Realizar simulacros y pruebas parciales de los planes. Se realizan pruebas parciales y ejercicios de mesa (simulacros) con los equipos involucrados para validar los procedimientos, las comunicaciones y los roles definidos en los planes.		✓	✓
CON-12	A9:4.04	Documentar y analizar los resultados de todas las pruebas. Los resultados, hallazgos y lecciones aprendidas de cada prueba o simulacro se documentan formalmente y se utilizan como insumo para la mejora continua de los planes.		✓	✓
CON-13	A9:4.04	Ejecutar pruebas funcionales completas de los planes de recuperación. Se ejecutan pruebas funcionales completas del DRP y BCP, al menos anualmente, que simulen escenarios realistas y permitan medir el logro de los objetivos de recuperación (RTO/RPO).			✓

Capacidad 19: Evaluación del desempeño y mejora Continua					
ID	Fuente	Práctica / Requisito	MIL 1	MIL 2	MIL 3
GOB-13	A7:5.2	Realizar auditorías internas del SASI. Se planifica y ejecuta un ciclo de auditorías internas, con una frecuencia mínima anual, para evaluar de forma objetiva la conformidad y eficacia del Sistema de Administración de Seguridad de la Información (SASI).		✓	✓
GOB-14	A7:5.4	Gestionar formalmente los hallazgos y las acciones de mejora. Se establece y mantiene un proceso formal y centralizado para documentar, analizar (causa raíz), dar seguimiento y verificar la eficacia de las acciones correctivas y de mejora derivadas de auditorías, revisiones o incidentes.		✓	✓
GOB-15	A7:5.3	Ejecutar un proceso formal de Revisión por la Dirección. La MAE o un nivel directivo designado lidera una revisión formal, al menos una vez al año, para evaluar la idoneidad y eficacia del SASI, analizando insumos clave (auditorías, KPIs, riesgos) y documentando las decisiones estratégicas resultantes.			✓
GOB-16	A7:5.1	Gestionar el desempeño del SASI mediante métricas (KPIs/KRIs). Se definen, miden y analizan Indicadores Clave de Desempeño (KPIs) e Indicadores Clave de Riesgo (KRIs), y sus resultados son utilizados como insumo principal para la toma de decisiones basada en datos en la Revisión por la Dirección.			✓

EQUIPO DE TRABAJO

Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC)

Edgar Batista, Director General

Leo VanTroi Mercedes, Director de Gabinete

Reyson Lizardo, Director de Transformación Digital Gubernamental

Elupina Almonte, Encargada del Departamento de Normas y Estándares

Enyer Pérez, Encargado de División de Investigación y Documentación de Normas

Juan Bautista Torres Santana, Especialista de Estándares y Normativas

César Miguel Cordero Medina, Especialista de Estándares y Normativas

Rafael Leonel Báez Vásquez, Especialista de Estándares y Normativas

Carlos Guerrero, Analista de Normas y Estándares

Jason Crisóstomo, Encargado de División de Implementación de Normas

Melvin Hilario, Encargado de División de Auditoría y Monitoreo de Normas

Gloria Alexandra Sánchez Valverde, Directora de Planificación y Desarrollo

Francisco Félix De Jesús Jiménez, Director del Centro de Datos del Estado

Juan Hernández, Director de Tecnología de la Información y Comunicación

José Estévez, Encargado de Seguridad y Monitoreo TIC

Ángel Ortega, CISO

Centro Nacional de Ciberseguridad (CNCS)

Carlos Leonardo, Director Ejecutivo

Eduardo Jana, Director CSIRT-RD

Ángela Martínez, Directora de Coordinación de Estrategias

Jenny de Jesús, Coordinadora de Políticas, Procedimientos y Normas

Consultor

Elvyn Peguero

Agradecimientos

Miguel Román,

Harom Ramos,

Elvyn Gomez,

Santiago Moral



Av. Rómulo Betancourt #311, Edificio Corporativo Vista 311,
Bella Vista, Sto. Dgo., R.D.
Tel.: +1 (809) 286-1009 | info@ogtic.gob.do
www.ogtic.gob.do | www.gob.do

    @OGICRD   @OGICRDO