NORTIC

A9

2025

NORMA PARA LA GESTIÓN DE RIESGOS TECNOLÓGICOS Y CONTINUIDAD OPERATIVA

Santo Domingo, República Dominicana
Diciembre 2025.

nortic

ogtic
Oficina Gubernamental de Tecnologías de la Información y Comunicación

GOBIERNO DE LA REPÚBLICA DOMINICANA

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

CNCS ogtic

NORTIC A9

2025

NORMA PARA LA GESTIÓN DE RIESGOS TECNOLÓGICOS Y CONTINUIDAD OPERATIVA

SANTO DOMINGO, REPÚBLICA DOMINICANA
DICIEMBRE 2025.

NORTIC A9:2025 > NORMA PARA LA GESTIÓN DE RIESGOS TECNOLÓGICOS Y CONTINUIDAD OPERATIVA

Edición: 1ra

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 1.0

Diagramado y diseñado por la Dirección de Innovación, OGTIC.

CONTENIDO

PRÓLOGO

En la era digital, la capacidad del Estado para operar de forma ininterrumpida no es solo una expectativa, sino un pilar fundamental de la confianza pública y la estabilidad nacional. Cada avance tecnológico representa una oportunidad para mejorar los servicios a la ciudadanía, pero también introduce riesgos que exigen una preparación robusta y una capacidad probada para resistir, adaptarse y recuperarse de cualquier eventualidad.

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 A9, la norma que establece el marco metodológico unificado para la Gestión de Riesgos Tecnológicos y la Continuidad Operativa en el sector público dominicano. Este no es un esfuerzo aislado, sino el resultado de una colaboración estratégica para dotar a cada institución del Estado de una visión y herramientas comunes para garantizar su resiliencia.

Esta norma tiene un objetivo claro: asegurar que, ante un incidente disruptivo —sea este un fallo técnico, un desastre natural o un ciberataque—, las funciones críticas del Estado se mantengan operativas y los servicios esenciales para la ciudadanía no se detengan. La NORTIC A9 proporciona una metodología formal, alineada con estándares internacionales como la ISO 22301, para la gestión de riesgos, la planificación de la continuidad del negocio y la recuperación ante desastres.

Este estándar opera dentro de un ecosistema normativo coherente y se integra con las demás normas de seguridad. Trabaja bajo los mandatos de la **NORTIC A7 - Norma para la Administración del Sistema de Seguridad de la Información** y se complementa con los controles defensivos de la **NORTIC A8 - Norma General de Ciberseguridad**, asegurando que la resiliencia operativa y la defensa cibernética sean dos caras de la misma moneda estratégica.

La resiliencia depende del liderazgo y compromiso institucional, no solo de la tecnología. Las autoridades deben garantizar el cumplimiento de esta norma. La continuidad operativa es un objetivo estratégico de toda la administración pública, no solo del área tecnológica.

Reafirmamos así nuestro compromiso unificado con una arquitectura digital gubernamental resiliente y sostenible. La NORTIC A9 es el instrumento de Estado para asegurar que, ante cualquier eventualidad, la República Dominicana no se detiene.

Edgar Batista Carrasco

Director general

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

Carlos Leonardo

Director ejecutivo

Centro Nacional de Ciberseguridad (CNCS)

INTRODUCCIÓN

La Norma para la Gestión de Riesgos Tecnológicos y Continuidad Operativa en el Estado Dominicano, conocida como NORTIC A9, establece las directrices, metodologías y controles obligatorios que deben seguir los organismos gubernamentales para la correcta implementación de sus programas de gestión de riesgos y de continuidad. El objetivo principal de este estándar es salvaguardar los activos de información críticos y asegurar la resiliencia de las operaciones, proporcionando un marco estructurado que permita a cada entidad proteger sus servicios frente a interrupciones de cualquier índole.

Esta normativa se articula en dos pilares funcionales complementarios. El primer pilar se enfoca en la **Gestión de Riesgos Tecnológicos**, estableciendo una metodología formal para la identificación, análisis, evaluación y tratamiento de los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de los activos tecnológicos y de información. Para ello, se detallan los procedimientos para la clasificación de activos, la evaluación de amenazas y vulnerabilidades, la determinación de los niveles de impacto y probabilidad, y la planificación de las medidas de mitigación correspondientes.

El segundo pilar de la norma se dedica a la **Continuidad Operativa**, y define los requisitos para el desarrollo e implementación de un programa integral que garantice la capacidad de la institución para mantener sus funciones esenciales durante y después de un evento disruptivo. Este pilar proporciona la metodología para realizar el Análisis de Impacto al Negocio (BIA), un proceso fundamental para identificar las prioridades de recuperación y establecer los Objetivos de Tiempo de Recuperación (RTO) y Punto de Recuperación (RPO).

Basado en los resultados de dicho análisis, la norma establece las directrices para el diseño, implementación y mantenimiento de los siguientes planes: el Plan de Continuidad de Negocio (BCP), enfocado en los procesos y las personas; el Plan de Recuperación ante Desastres (DRP), centrado en la restauración de la infraestructura tecnológica; y los Planes de Contingencia de Sistemas de Información (ISCP), para la recuperación de sistemas críticos específicos.

Finalmente, este documento define los requisitos para la validación y la mejora continua de todo el programa, detallando los procedimientos para la realización de pruebas y simulacros periódicos, así como para la revisión y actualización de los planes, asegurando que estos se mantengan vigentes y efectivos.

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. Se determinó que la profundidad requerida para dominios como la defensa cibernética y la continuidad operativa justificaba la creación de estándares dedicados. En consecuencia, la NORTIC A7 original fue reestructurada, dando paso a un ecosistema de normas interconectadas. La presente NORTIC A9:2025 nace de esta evolución, heredando y expandiendo de manera exclusiva todos los componentes de gestión de riesgos tecnológicos y continuidad operativa.

MARCO LEGAL

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 A9 proporciona la metodología para gestionar los riesgos que amenazan estos derechos y asegurar la continuidad de los servicios que los procesan.

2. **Ley 172-13 sobre protección integral de los datos personales:** Regula el tratamiento de datos personales y exige medidas de seguridad para su protección. La NORTIC A9 establece el marco para que los organismos evalúen los riesgos asociados al manejo de estos datos y planifiquen la continuidad de los sistemas que los albergan.

3. **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 A9 contribuye a este derecho al asegurar que los servicios públicos basados en tecnología sean resilientes y sus riesgos de interrupción sean gestionados.

4. **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 seguridad y tecnología

5. **Ley 53-07 contra crímenes y delitos de alta tecnología:** Protege los sistemas de información. La NORTIC A9 aborda esta ley al establecer la obligación de gestionar el riesgo de que estos delitos ocurran y de planificar la continuidad operativa para recuperarse de sus impactos.

6. **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 y establece la necesidad de gestionar riesgos y aumentar la resiliencia. La NORTIC A9 es el instrumento metodológico para que las instituciones cumplan con estos mandatos.

Mandatos de modernización y cumplimiento de las NORTIC

7. **Ley 1-12 sobre Estrategia Nacional de Desarrollo 2030:** Promueve el uso de las TIC para mejorar la gestión pública. La NORTIC A9 es fundamental para este objetivo, ya que una gestión pública digital solo es sostenible si es resiliente y gestiona sus riesgos.

8. **Ley 167-21 sobre mejora regulatoria y simplificación de trámites:** Obliga a las instituciones a usar tecnologías que aseguren la protección de datos. La NORTIC A9 refuerza este mandato al exigir la gestión de los riesgos que podrían comprometer esa protección.

9. **Decreto 1090-04 y decreto 54-21:** Crean y transforman la Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC) en la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC), otorgándole en su artículo 9 la responsabilidad de velar por la seguridad y privacidad de la

información en el sector público. La NORTIC A9 es una herramienta clave para ejecutar este mandato.

10. **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.

11. **Decreto 92-22 que establece el Marco Nacional de Interoperabilidad Gubernamental:** Define la interoperabilidad, la cual debe ser resiliente. La NORTIC A9 provee el marco para asegurar la continuidad de los sistemas que interoperan.

12. **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** elaboradas por la OGTIC. Estos decretos constituyen la base jurídica de la obligatoriedad de la presente norma, vinculando la eficiencia y la simplificación de trámites a una gestión robusta de los riesgos tecnológicos y la continuidad operacional.

CAPÍTULO 1

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 las directrices, requisitos y la metodología obligatoria que deben seguir los organismos del Estado Dominicano para el desarrollo, implementación y mantenimiento de sus programas de gestión de riesgos tecnológicos y continuidad operativa.

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 una metodología formal y sistemática para la gestión de los riesgos tecnológicos,** que permita identificar, analizar, evaluar y tratar las amenazas que puedan afectar la infraestructura y los activos de información críticos.

- **Desarrollar y mantener un programa de continuidad operativa,** basado en un Análisis de Impacto al Negocio (BIA),

que garantice la capacidad de la institución para mantener sus funciones y servicios esenciales durante y después de un evento disruptivo.

- **Implementar planes detallados de recuperación ante desastres (DRP) y de contingencia (ISCP),** que definan las estrategias y procedimientos técnicos necesarios para la restauración ordenada y eficaz de la infraestructura tecnológica crítica.
- **Fortalecer la resiliencia general del organismo,** asegurando que los planes de continuidad sean validados periódicamente a través de pruebas y simulacros, y que se mantengan actualizados para responder a los cambios en el entorno operativo y tecnológico.
- **Facilitar la toma de decisiones informada por parte de la alta dirección,** proporcionando una visión clara de los riesgos tecnológicos y el estado de preparación de la institución para enfrentar interrupciones.

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 y decretos vigentes que regulan la seguridad de la información, la gestión de riesgos y la continuidad del Estado.

Asimismo, esta norma opera dentro del ecosistema de seguridad del Estado y se complementa con los requisitos establecidos en:

- **NORTIC A7 – Norma para la Administración de la Seguridad de la Información:** Establece los mandatos de alto nivel sobre la gestión de riesgos y la obligación de tener un programa de

continuidad.

- • **NORTIC A8 – Norma General de Ciberseguridad:** Detalla los controles técnicos de ciberseguridad, cuya falla puede ser un detonante para los planes de continuidad aquí descritos.

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

- **ISO/IEC 22301 - Seguridad y resiliencia - Sistemas de gestión de la continuidad del negocio:** Estándar internacional para la implementación y mantenimiento de planes de continuidad.
- **ISO/IEC 27001 - Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de la seguridad de la información:** Para la integración de la gestión de riesgos y la continuidad dentro del marco general de seguridad.
- **NIST special publication 800-34 - Contingency planning guide for federal information systems:** Guía de referencia para la planificación de la contingencia en sistemas tecnológicos.

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, comprometiendo la 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 soporte 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.

CAPÍTULO 2

METODOLOGÍA DE GESTIÓN DE RIESGOS TECNOLÓGICOS

Este capítulo establece la metodología formal que los organismos deben seguir para la gestión de sus riesgos tecnológicos, de acuerdo con el programa de gestión de riesgos exigido en la **NORTIC A7 – Norma para la Administración de la Seguridad de la Información.**

Sección 2.01. Liderazgo y compromiso de la alta dirección (MAE)

a) La metodología debe estar enfocada y orientada a los procesos del organismo y a los activos tecnológicos asociados.

b) La metodología debe incluir el análisis, la evaluación y el tratamiento de los riesgos que puedan afectar la continuidad operativa.

c) La metodología debe estar alineada con la práctica organizacional de gestión de riesgos existente en el organismo, si la hubiere.

d) La metodología debe incluir procesos para la revisión periódica de los niveles de riesgo en función de la evolución de las amenazas y sus impactos.

e) La metodología de gestión de riesgos debe aplicarse de forma obligatoria siempre que se realicen cambios sustanciales en la operación del organismo o se introduzcan o modifiquen elementos de TIC.

Sección 2.02. Metodología de análisis y evaluación de riesgos

a) El proceso de análisis de riesgos debe incluir la identificación de amenazas, utilizando para ello, como mínimo, los siguientes mecanismos:

- Talleres interdisciplinarios con expertos internos y externos.
- Análisis de registros históricos de incidentes propios del organismo.
- Estudio de tendencias y alertas de riesgos emergentes publicadas por fuentes confiables, como el Centro Nacional de Ciberseguridad (CNCS).

b) El proceso de análisis de riesgos debe incluir la identificación de vulnerabilidades. Esta actividad se nutre de los resultados de los controles operativos definidos en la **NORTIC A8 – Norma General de Ciberseguridad**, tales como auditorías de seguridad, pruebas de penetración y escaneos de vulnerabilidades, así como del análisis de procesos operativos para detectar puntos débiles.

c) La evaluación de riesgos debe basarse en la fórmula conceptual **Riesgo = Probabilidad x Impacto.** Para determinar el nivel de riesgo, se deben evaluar ambos componentes de la siguiente manera:

(i) La evaluación de riesgos debe incluir la determinación de la **probabilidad de ocurrencia** de una amenaza dentro de

un **período de 12 meses.** Para ello, se deben considerar factores como eventos históricos y vectores de riesgo, y utilizar una nomenclatura de clasificación formal, como la siguiente:

- Alta probabilidad
- Muy probable
- Probable
- Poco probable
- Improbable

(ii) La evaluación de riesgos debe incluir la determinación del **impacto potencial** sobre los activos críticos y la operación del organismo. Para ello, se deben considerar factores como pérdidas de eventos históricos y proyecciones, y utilizar una nomenclatura de clasificación formal, como la siguiente:

- Catastrófico
- Muy severo
- Severo
- Moderado
- No significativo

Sección 2.03. Metodología de priorización del riesgo

a) Se deben definir y documentar criterios claros para clasificar los riesgos resultantes en categorías, como mínimo: **Crítico, Alto, Medio y Bajo.** Esta clasificación debe basarse en umbrales predefinidos en una **matriz de riesgo (o mapa de calor),** que

combine los niveles de probabilidad e impacto evaluados previamente.

b) Se **debe** utilizar un mecanismo formal para la visualización y priorización de riesgos, como una **matriz de riesgo o mapa de calor**, que represente gráficamente el nivel de riesgo resultante de la combinación de probabilidad e impacto. El propósito de este mecanismo es facilitar la comunicación de la postura de riesgo y la toma de decisiones sobre su tratamiento. Ver Anexo B: *Ejemplo de Matriz de Criticidad de Activos.*

c) Al momento de priorizar las acciones de mitigación, la metodología debe asegurar que se otorgue mayor peso y urgencia a aquellos riesgos que afectan a los activos y procesos de negocio identificados como de mayor criticidad para la operación institucional, según los resultados del Análisis de Impacto al Negocio (BIA).

Sección 2.04. Metodología para el tratamiento del riesgo y la documentación

a) Para cada riesgo identificado que supere la tolerancia definida, el Organismo **debe** seleccionar y documentar formalmente una de las siguientes estrategias de tratamiento:

- **Mitigar:** Aplicar controles para reducir la probabilidad o el impacto del riesgo.
- **Transferir:** Trasladar total o parcialmente el impacto financiero del riesgo a un tercero, como a través de la adquisición de una póliza de seguros.
- **Aceptar:** Asumir formalmente el riesgo sin tomar acciones de mitigación adicionales, siempre que esta decisión sea aprobada por la autoridad competente y el riesgo se

encuentre dentro de la tolerancia al riesgo definida por el organismo.

- **Evitar:** Decidir no iniciar o descontinuar la actividad, proceso o uso del activo tecnológico que da origen al riesgo.

b) En los casos en que la estrategia seleccionada sea **mitigar**, el Organismo **debe** seleccionar e implementar los controles preventivos, detectivos y correctivos aplicables. La selección de estos controles se basará principalmente en el catálogo definido en la **NORTIC A8 – Norma General de Ciberseguridad**, así como en otros controles definidos internamente.

c) Para la implementación de los controles, el Organismo **debe** diseñar planes de acción que cumplan, como mínimo, con los siguientes elementos:

(i) Detallar las acciones de mitigación, incluyendo responsables, plazos y recursos necesarios.

(ii) Asegurar la implementación efectiva de los controles seleccionados.

(iii) Incluir mecanismos para monitorear y evaluar continuamente la efectividad de los controles implementados.

d) El proceso de seguimiento de la implementación de controles **debe** incluir, como mínimo:

(i) La evaluación del impacto de los controles para asegurar que no afecten negativamente las operaciones.

(ii) La revisión continua de los controles para su adaptación a nuevas amenazas y cambios en el entorno tecnológico.

e) El Organismo **debe** documentar de manera formal todo el proceso de gestión de riesgos. Este proceso de documentación

debe cumplir con:

(i) Documentar cada etapa, incluyendo los métodos utilizados, criterios de evaluación y resultados.

(ii) Asegurar que los registros se actualicen regularmente para reflejar cambios.

(iii) Utilizar formatos y plantillas estandarizadas para asegurar la consistencia.

f) El proceso de monitoreo continuo **debe** incluir el seguimiento de los Indicadores Clave de Desempeño (KPIs) para asegurar la mejora continua del proceso de gestión de riesgos.

g) Como resultado del proceso de análisis y tratamiento de riesgos, el Organismo debe elaborar y mantener una Declaración de Aplicabilidad. Este documento debe listar los controles seleccionados para tratar los riesgos y proporcionar una justificación para cualquier control que se haya decidido excluir.

CAPÍTULO 3

MARCO DE GESTIÓN Y PLANIFICACIÓN DE LA CONTINUIDAD

Este capítulo establece las directrices y metodologías para la planificación de la continuidad operativa. Detalla los requisitos de la política de continuidad y el proceso para realizar el Análisis de Impacto al Negocio (BIA), sentando las bases para el desarrollo de los planes que permitirán al organismo cumplir con el programa de continuidad exigido en la **NORTIC A7 – Norma para la Administración de la Seguridad de la Información.**

Sección 3.01. Requisitos de la política de continuidad tecnológica

Conforme al mandato establecido en la NORTIC A7, el organismo debe desarrollar, documentar e implementar una política de gestión de continuidad tecnológica. Esta política es el documento fundamental que establece las directrices y el compromiso de la institución para garantizar que sus sistemas y operaciones puedan ser rápidamente restaurados en caso de una interrupción.

La política **debe** cumplir, como mínimo, con los siguientes requisitos de contenido:

a) Objetivos: La política debe definir claramente sus objetivos, incluyendo, pero no limitándose a:

(i) **Garantizar la resiliencia:** Asegurar que los sistemas tecnológicos puedan resistir y recuperarse de interrupciones.

(ii) **Proteger la información:** Mantener la confidencialidad, integridad y disponibilidad de la información durante y después de una interrupción.

(iii) **Minimizar el impacto:** Reducir al mínimo el impacto negativo de las interrupciones en las operaciones y servicios gubernamentales.

(iv) **Cumplir con las normativas:** Asegurar el cumplimiento de las leyes y regulaciones vigentes, así como de los estándares internacionales aplicables.

b) **Alcance:** El alcance de la política debe especificar claramente:

(i) **Aplicabilidad:** Las áreas, procesos y sistemas tecnológicos que abarca, incluyendo todas las unidades organizativas dentro de la institución.

(ii) **Tipos de interrupciones:** Las diferentes clases de eventos que la política pretende cubrir, tales como desastres naturales, fallos técnicos, ciberataques y errores humanos.

c) **Integración con la gestión de riesgos:** La política debe establecer que el programa de continuidad se basará en la metodología de gestión de riesgos definida en el Capítulo 2 de esta norma. Debe exigir, como mínimo:

(i) La realización de un análisis exhaustivo de riesgos para identificar amenazas potenciales a la continuidad tecnológica.

(ii) La evaluación de dichos riesgos en términos de probabilidad e impacto.

(iii) La implementación de controles y medidas de mitigación para minimizar las amenazas a la continuidad de las operaciones.

d) Referencia a planes y protocolos: La política debe ordenar el desarrollo y mantenimiento de los siguientes planes y protocolos específicos:

(i) Procedimientos para la identificación y evaluación de los activos tecnológicos y de información que son esenciales para las operaciones de la institución.

(ii) El Plan de Recuperación ante Desastres (DRP).

(iii) El Plan de Continuidad de Negocio (BCP).

(iv) Los Planes de Contingencia de Sistemas de Información (ISCP).

(v) Protocolos para la comunicación y coordinación durante una interrupción.

e) Aprobación y ciclo de vida: La política debe definir su proceso de gobernanza, estableciendo, como mínimo:

(i) Aprobación formal: La política, y cualquier revisión mayor de la misma, debe ser formalmente aprobada por el Comité de Implementación y Gestión de Estándares TIC (CIGETIC) y ratificada por la Máxima Autoridad Ejecutiva (MAE).

(ii) Revisión periódica: La política debe ser revisada con una frecuencia mínima anual, o cuando ocurran cambios significativos en el entorno, para asegurar su continua relevancia y efectividad.

a) El organismo debe realizar un análisis de impacto al negocio (BIA) para evaluar las consecuencias de una interrupción de sus procesos y activos críticos, y para establecer las prioridades de recuperación.

b) El proceso de BIA debe incluir, como mínimo, las siguientes actividades:

   (i) Evaluar el impacto potencial de una interrupción en términos de tiempo de inactividad, pérdida de datos, costos, y efectos legales y reputacionales.

   (ii) Evaluar el impacto potencial en la reputación de la institución, especialmente en términos de confianza pública.

   (iii) Desarrollar un mapa de procesos que muestre cómo interactúan los diferentes procesos críticos dentro de la institución.

   (iv) Identificar y analizar los riesgos que pueden afectar la continuidad tecnológica, considerando tanto amenazas internas como externas.

   (v) Realizar una clasificación y priorización de recuperación para cada activo y proceso crítico.

   (vi) Definir el Tiempo Máximo de Recuperación (RTO) para cada proceso crítico, que es el tiempo máximo en el que debe ser recuperado para evitar impactos graves.

   (vii) Determinar el Punto Máximo de Pérdida de Datos (RPO), que define la cantidad de información que puede permitirse perder y determina la frecuencia de las copias de seguridad.

(viii) Establecer los requisitos de recursos (humanos, tecnológicos, etc.) necesarios para recuperar los procesos críticos.

c) Se debe construir un documento formal y detallado del BIA que incluya todos los hallazgos y las prioridades de recuperación. Este documento debe ser validado por las partes interesadas clave y, una vez aprobado, servirá como el insumo principal para el desarrollo de los planes de recuperación (DRP) y contingencia (ISCP).

Sección 3.03. Gestión de la disponibilidad y la capacidad

Para garantizar que los servicios tecnológicos se mantengan operativos y respondan a las necesidades del organismo, se deben implementar procesos formales para la gestión continua de la disponibilidad y la capacidad de la infraestructura de TIC.

Subsección 3.03.1. Gestión de la disponibilidad

a) El organismo debe establecer y mantener procedimientos documentados y recursos tecnológicos para el monitoreo continuo de la disponibilidad de todos los sistemas y activos de información críticos.

b) Debe implementarse un sistema de registro centralizado para documentar cualquier evento o condición que afecte la disponibilidad de los sistemas, incluyendo la fecha, hora, duración, sistemas afectados y el impacto inicial observado.

c) Debe existir un procedimiento formal para evaluar los problemas de disponibilidad, con el fin de determinar si constituyen un incidente de seguridad. En caso afirmativo, el evento debe ser gestionado conforme a los lineamientos establecidos en la

NORTIC A8 – Norma General de Ciberseguridad.

d) El organismo debe implementar mecanismos de alerta y notificación automatizados que informen de manera inmediata al personal técnico responsable cuando los sistemas críticos dejen de estar disponibles o su rendimiento se degrade por debajo de los umbrales establecidos.

e) Debe realizarse un análisis periódico de los registros históricos de eventos de disponibilidad para identificar tendencias, problemas recurrentes y realizar un análisis de causa raíz que permita implementar soluciones definitivas.

Subsección 3.03.2. Gestión de la capacidad

a) El organismo debe disponer de procedimientos y recursos tecnológicos para el monitoreo continuo del uso de los recursos de TIC, incluyendo, como mínimo, la capacidad de procesamiento (CPU), memoria (RAM), almacenamiento y ancho de banda de la red.

b) Deben generarse y analizarse informes periódicos sobre el consumo de capacidad para identificar tendencias de crecimiento y realizar proyecciones de necesidades futuras, a fin de planificar las adquisiciones o ampliaciones de manera proactiva.

c) Deben establecerse y monitorearse umbrales de utilización de recursos. Al alcanzarse dichos umbrales, se deben generar alertas y notificaciones automáticas al personal responsable para prevenir la degradación del servicio y evitar interrupciones por falta de capacidad.

CAPÍTULO 4

DESARROLLO Y VALIDACIÓN DE PLANES DE CONTINUIDAD

Este capítulo establece los requisitos operativos para el desarrollo, la validación y el mantenimiento de los planes de continuidad. Detalla la estructura y el contenido mínimo del Plan de Continuidad de Negocio (BCP), el Plan de Recuperación ante Desastres (DRP) y los Planes de Contingencia (ISCP), así como la metodología para su prueba y mejora continua, conforme a lo requerido por la **NORTIC A7 – Norma para la Administración de la Seguridad de la Información.**

Sección 4.01. Desarrollo del plan de continuidad de negocio (BCP)

El Plan de Continuidad de Negocio (BCP) es el documento estratégico y operativo que define cómo el organismo mantendrá sus funciones críticas durante una interrupción.

Subsección 4.01.1. Principios y alcance del BCP

a) El BCP debe estar alineado con el plan estratégico de la máxima autoridad y considerar las debilidades del organismo para proteger la información y los servicios críticos.

b) La gestión de riesgos tecnológicos y continuidad operativa debe estar integrada dentro del BCP.

c) Para asegurar la consistencia, el organismo debe utilizar un único marco de referencia para la elaboración de todos sus planes de continuidad.

d) El plan debe tener un propietario formalmente designado.

e) En caso de que el organismo disponga de varias localidades, el plan debe residir en cada una de ellas, y los controles de seguridad en sitios temporales deben ser equivalentes a los de las localidades principales.

Subsección 4.01.2. Contenido y estructura del BCP

a) El BCP debe ser un documento formal que contenga, como mínimo, los siguientes elementos:

(i) Las condiciones para la activación del plan, basadas en los resultados del BIA.

(ii) Los procedimientos de emergencia y las acciones de respuesta inicial, incluyendo la forma en que se evaluará la toma de decisiones.

(iii) Los procedimientos de contingencia, incluyendo las acciones para el traslado a locales temporales, si aplica.

(iv) Las responsabilidades de las personas y equipos designados como dueños de planes y del personal alternativo.

(v) La identificación de los activos y recursos críticos de TIC necesarios para realizar tareas de emergencia, respaldo y reanudación.

(vi) La identificación de la pérdida de información aceptable (RPO) y los servicios críticos a restaurar.

(vii) La evaluación de la dependencia de servicios de TIC externos o internos.

(viii) Las especificaciones para la reanudación de las operaciones y servicios de TIC.

Subsección 4.01.3. Procedimientos de continuidad y respuesta

a) El organismo debe disponer de procedimientos detallados que contengan los pasos necesarios para la recuperación ordenada de los procesos críticos.

b) Los procedimientos deben establecer por adelantado la habilitación de un Centro de Comando desde donde se dirigirán las labores de recuperación.

c) Los procedimientos deben indicar claramente los pasos para la activación del plan, así como quién o quiénes son las personas autorizadas para activarlo.

d) Los procedimientos deben definir las personas, los roles y los recursos necesarios para la recuperación, así como la forma de comunicación que existirá entre los equipos.

e) Los procedimientos deben indicar qué personas asumirán los roles de liderazgo en caso de que el personal principal no esté disponible.

Subsección 4.01.4. Gestión y comunicación de crisis

a) El BCP debe definir la estructura y composición de un Equipo de Gestión de Crisis (EGC), con roles y responsabilidades claramente definidos para el manejo de la interrupción a nivel estratégico.

b) El BCP debe incluir un Plan de Comunicación de Crisis que establezca los protocolos, voceros autorizados y mensajes clave para comunicarse con las partes interesadas (empleados,

prensa, ciudadanos, gobierno) durante la interrupción.

c) El Plan de Comunicación de Crisis debe contemplar la gestión de las relaciones con los medios, los mensajes clave y los procedimientos de aprobación interna para comunicar antes, durante y después de un incidente.

Sección 4.02. Desarrollo del plan de recuperación ante desastres (DRP)

El Plan de Recuperación ante Desastres (DRP) detalla los procedimientos y estrategias para la recuperación de la infraestructura tecnológica crítica.

Subsección 4.02.1. Metodología y estrategias de recuperación

a) El DRP debe basarse en la metodología de gestión de riesgos del Capítulo 2 y en los resultados del BIA del Capítulo 3.

b) El organismo debe definir, desarrollar y documentar los métodos y procedimientos de restauración para asegurar la continuidad de los servicios tecnológicos críticos ante diferentes tipos de desastres, incluyendo, pero no limitándose a:

- Fallos de infraestructura de TI.
- Desastres naturales.
- Ciberataques.

c) El organismo debe identificar, documentar y establecer las estrategias de recuperación, considerando la utilización de sitios alternativos según las necesidades definidas en el BIA:

- Recuperación inmediata (Hot Site).
- Recuperación rápida (Warm Site).

- Recuperación diferida (Cold Site).

d) Deben implementarse soluciones de alta disponibilidad (HA) que incluyan redundancia en servidores, almacenamiento y conectividad de red, y considerar el uso de tecnologías de virtualización y contenedores para facilitar la migración rápida de aplicaciones.

e) Los planes deben identificar los posibles puntos únicos de falla para crear esquemas alternos de recuperación.

Subsección 4.02.2. Estrategia de recuperación de datos y respaldos

a) Se debe definir, documentar y establecer la estrategia de recuperación de datos para los DRP, la cual debe incluir una estrategia de respaldo basada en la criticidad de los datos y los RPO definidos en el BIA.

b) La estrategia de respaldo debe contemplar, como mínimo:

(i) Utilizar almacenamiento en otras localidades (off-site) para los datos más críticos.

(ii) Asegurar que los respaldos sean cifrados.

(iii) Utilizar soluciones de respaldo automatizadas y almacenar copias en ubicaciones seguras fuera del sitio principal.

(iv) Realizar verificaciones periódicas de la integridad de los datos respaldados.

(v) Mantener copias de seguridad en almacenamiento offline para proteger contra ciberataques, como ransomware.

c) Deben establecerse y documentarse procedimientos detallados para la restauración de datos, incluyendo guías paso a paso y listas de verificación para restaurar sistemas, bases de datos y archivos críticos.

d) Debe implementarse replicación síncrona para datos críticos que no pueden permitirse ninguna pérdida, y considerar la replicación asíncrona para sistemas menos críticos.

Subsección 4.02.3. Contenido y procedimientos del DRP

a) El DRP debe establecer una cadena de mando clara para la toma de decisiones sobre su activación, definiendo responsables e instrucciones claras sobre cuándo y cómo activar el plan.

b) El DRP debe contemplar los requerimientos para protegerse de fallos de proveedores de servicios, incluyendo contratos de mantenimiento, soportes y garantías para asegurar la disponibilidad de los recursos.

c) El DRP debe contemplar vías alternas y la disposición de recursos necesarios, como repuestos locales, para la recuperación de servicios tecnológicos.

d) Todas las estrategias y procedimientos deben estar documentados en el documento formal del DRP.

Subsección 4.02.4. Ejecución, seguimiento y cierre del DRP

a) El DRP debe definir los criterios y procedimientos para su activación de manera oportuna y eficaz, garantizando una transición ordenada hacia la restauración de las operaciones.

b) El plan debe incluir un proceso formal para la selección y ajuste dinámico de las acciones de recuperación, priorizando la restauración de funciones críticas conforme a los resultados del BIA.

c) Las decisiones de ajuste al plan durante una recuperación deben ser documentadas y autorizadas por el equipo responsable de la gestión del incidente.

d) El DRP debe incluir los procedimientos para la supervisión posterior a la restauración, a fin de detectar errores persistentes o signos de reinfección.

e) El plan debe definir los criterios objetivos para declarar el final del proceso de recuperación y los procedimientos para la elaboración del informe post-incidente y la gestión de lecciones aprendidas.

Sección 4.03. Desarrollo del plan de contingencia de sistemas de información (ISCP)

El Plan de Contingencia de Sistemas de Información (ISCP, por sus siglas en inglés) establece los procedimientos para la recuperación de sistemas de información específicos ante interrupciones leves o moderadas.

Subsección 4.03.1. Requisitos técnicos de contingencia

a) Para asegurar la continuidad de los sistemas críticos, el organismo debe aplicar los siguientes requerimientos técnicos:

(i) Implementar redundancias y alta capacidad para los sistemas.

(ii) Realizar respaldos regulares de los sistemas críticos y almacenarlos en ubicaciones seguras, conforme a la estrategia de respaldos definida en la **sección 4.2.**

(iii) Asegurar que los sistemas de información cumplan con los estándares de seguridad pertinentes definidos en la **NORTIC A8 – Norma General de Ciberseguridad.**

(iv) Implementar controles preventivos, los cuales deben estar integrados en la arquitectura del sistema y documentarse como parte de la estrategia de recuperación.

a) El organismo debe desarrollar un ISCP para cada sistema crítico, el cual debe contener, como mínimo, la siguiente información:

- **Objetivo y alcance:** Definición del sistema que cubre el plan.
- **Escenarios:** Descripción de los distintos escenarios de interrupción aplicables al sistema.
- **Protocolo de activación:** Incluyendo el tiempo límite para activar la contingencia, el tiempo máximo de duración y la autoridad para activarla.
- **Procedimientos de respuesta inmediata:** Definición de canales de comunicación y acciones a tomar inmediatamente después de detectar un incidente.
- **Procedimientos de restauración:** Pasos necesarios para restaurar el sistema a su estado operativo, incluyendo la restauración de datos desde respaldos.
- **Instructivo de contingencia:** Una guía detallada paso a paso que defina qué hacer, quién lo hace y cómo se hace durante las fases de activación, contingencia y retorno a la normalidad.
- **Recursos necesarios:** Especificación de los recursos requeridos para activar y operar durante la contingencia.
- **Prueba post-restauración:** Protocolo para verificar que los datos restaurados son completos y que el sistema está operando como se esperaba.

Sección 4.04. Metodología para pruebas, mantenimiento y mejora continua

La simple existencia de planes no garantiza la resiliencia. El organismo debe establecer un programa formal para validar, mantener y mejorar continuamente sus capacidades de continuidad operativa.

Subsección 4.04.1. Programa de pruebas y simulacros

a) El organismo debe probar sus planes de continuidad (BCP, DRP, ISCP) al menos una (1) vez al año, o cuando ocurran cambios importantes en la operación o el contexto del organismo.

b) Las pruebas deben realizarse bajo escenarios hipotéticos realistas que permitan medir el logro de los objetivos de recuperación (RTO/RPO) y la efectividad de los procedimientos.

c) Las pruebas y simulacros deben medir los niveles de efectividad del desempeño del personal en la ejecución de sus roles y, cuando aplique, en labores de evacuación y rescate.

d) Las pruebas no deben introducir elementos de falla en los ambientes reales de producción, a menos que se realicen de forma controlada y autorizada.

e) Los resultados, hallazgos, lecciones aprendidas y ajustes necesarios de cada prueba deben documentarse formalmente.

Subsección 4.04.2. Pruebas post-restauración

a) El organismo debe implementar un protocolo de pruebas post-restauración para ser ejecutado después de un evento de contingencia real.

b) Este protocolo debe incluir, como mínimo, pruebas de funcionalidad y consistencia de datos, así como pruebas de integridad de las aplicaciones y procesos que dependen de los datos restaurados.

a) El organismo debe mantener un registro de las evaluaciones periódicas de los planes de continuidad, el cual debe incluir, como mínimo, el análisis sobre nuevos riesgos, la revisión del impacto económico y la evaluación de los simulacros realizados.

b) El organismo debe generar informes periódicos sobre la ejecución y el estado de sus planes de continuidad, los cuales serán dirigidos a la alta gerencia y al CIGETIC.

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 Perfomance 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: Tabla no.1 - Ejemplo de matriz de criticidad de activos

Activo	Criticidad	Impacto Potencial	Dependencias	Clasificación	Prioridad
Servidor de Base de Datos	Alta	Muy alto	Aplicaciones de gestión pública, sistemas de reporte	Crítico	Alta
Sistema de Correo Electrónico	Media	Medio	Comunicaciones internas y externas	Importante	Media
Estación de Trabajo	Baja	Bajo	Ninguna	Menor	Baja

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 Auditoria 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

@OGTICRD **@OGTICRDO**