NORTIC
A8
2025

NORMA GENERAL DE CIBERSEGURIDAD

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 A8

2025

NORMA GENERAL DE CIBERSEGURIDAD

SANTO DOMINGO, REPÚBLICA DOMINICANA
DICIEMBRE 2025.

NORTIC A8:2025 > NORMA GENERAL DE CIBERSEGURIDAD

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

CONT. CONTENIDO

PRÓLOGO

En la era digital, la confianza pública y la soberanía de la información del Estado dependen directamente de su capacidad para defenderse. Cada avance tecnológico es una oportunidad para servir mejor a la ciudadanía, pero también expande la superficie de ataque y expone a nuestras instituciones a ciberamenazas cada vez más sofisticadas, exigiendo una capacidad de defensa proactiva y robusta.

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 A8, la Norma General de Ciberseguridad, que establece el marco de controles técnicos y operativos para la ciberdefensa del sector público dominicano. Este no es un esfuerzo aislado, sino el resultado de una colaboración estratégica para dotar a cada institución del Estado de las herramientas para proteger activamente sus activos digitales.

Esta norma tiene un objetivo claro: proteger los activos de información y la infraestructura tecnológica del Estado contra ciberataques, garantizando la confidencialidad, integridad y disponibilidad de los datos. La NORTIC A8 proporciona un catálogo de controles, alineado con marcos internacionales como el NIST Cybersecurity Framework, para la identificación de activos y riesgos, la protección de sistemas, la detección de amenazas, la respuesta a incidentes y la recuperación segura.

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 las metodologías de la **NORTIC A9 – Norma para la Gestión de Riesgos Tecnológicos y Continuidad Operativa**, asegurando que la ciberdefensa activa (A8) y la resiliencia operativa (A9) sean dos caras de la misma moneda estratégica.

La ciberseguridad depende del liderazgo y compromiso institucional, no solo de la tecnología. Las autoridades deben garantizar el cumplimiento de esta norma. La defensa de los activos digitales es un objetivo estratégico de toda la administración pública, no solo del área tecnológica.

Reafirmamos así nuestro compromiso unificado con una arquitectura digital gubernamental segura y confiable. La NORTIC A8 es el instrumento de Estado para garantizar que la transformación digital de la República Dominicana avance sobre cimientos seguros.

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 General de Ciberseguridad, conocida como NORTIC A8, establece el catálogo de controles técnicos, operativos y de gestión obligatorios que deben seguir los organismos gubernamentales para la correcta implementación de sus programas de ciberdefensa. El objetivo principal de este estándar es proteger los activos de información y la infraestructura tecnológica del Estado frente a ciberamenazas, proporcionando un marco de controles estructurado que permita a cada entidad defender sus servicios contra ataques de cualquier índole.

Esta normativa se articula en torno a los pilares funcionales del ciclo de vida de la ciberseguridad, alineados con las mejores prácticas internacionales. El primer pilar se enfoca en la **Gestión de la Postura de Seguridad**, que abarca los controles preventivos y de preparación. Para ello, se detallan los procedimientos para la gestión y clasificación de activos, la evaluación de amenazas y vulnerabilidades (**Identificar**), así como la implementación de controles de acceso, protección de datos, seguridad de plataformas y resiliencia de la infraestructura (**Proteger**).

El segundo pilar de la norma se dedica a las **Operaciones de Seguridad y Respuesta**, y define los requisitos para la gestión activa de incidentes. Este pilar proporciona los controles para el monitoreo continuo y el análisis de eventos (**Detectar**), la gestión y coordinación de la respuesta ante incidentes (**Responder**), y la implementación de los controles de seguridad necesarios para asegurar que la restauración de los servicios se realice de forma segura y sin reintroducir amenazas (**Recuperar**).

Basado en este ciclo de vida, la norma establece las directrices detalladas para la implementación de un amplio rango de capacidades de ciberseguridad, desde la configuración segura de los sistemas hasta el análisis forense, la gestión de la inteligencia de amenazas y la protección de la cadena de suministro.

Finalmente, este documento define los requisitos para la validación y la mejora continua de todo el programa de ciberseguridad, detallando los procedimientos para la realización de pruebas de penetración, auditorías periódicas y la gestión de lecciones aprendidas, asegurando que las defensas del organismo se mantengan vigentes y efectivas ante un panorama de amenazas en constante evolución.

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 A8 – Norma General de Ciberseguridad, nace de esta evolución, heredando y expandiendo de manera exclusiva todos los componentes relacionados con la implementación de controles técnicos y operativos para la ciberdefensa del Estado.

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 A8 proporciona el **catálogo de controles técnicos y organizativos** (como el control de acceso y el cifrado) que las instituciones deben implementar para cumplir con este mandato constitucional.

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 A8 detalla cuáles son esas medidas de seguridad específicas que deben aplicarse para proteger los datos en reposo, en tránsito y en uso.

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 A8 contribuye a este derecho al asegurar que las interacciones digitales entre el ciudadano y el Estado se

realicen de forma segura, íntegra y confidencial.

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 sensible. La NORTIC A8 provee los **controles de clasificación y protección** para asegurar que solo la información pública sea accesible.

Marco legal de seguridad y tecnología

5. **Ley 53-07 contra crímenes y delitos de alta tecnología:** Protege los sistemas de información contra actos ilícitos. La NORTIC A8 es la materialización de esta ley a nivel de control, estableciendo las **defensas técnicas (firewalls, IDS/IPS, antimalware, etc.)** que los organismos deben implementar para prevenir y detectar estos delitos.

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. La NORTIC A8 es el **instrumento de control técnico principal** para que las instituciones cumplan con estos mandatos, implementando las defensas requeridas por la estrategia nacional.

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 A8 es fundamental para este objetivo, ya que una gestión pública digital solo es sostenible si es **segura** y protege los activos del Estado.

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 A8 refuerza este mandato al **especificar los controles de seguridad** que deben acompañar a la digitalización de trámites.

9. **Decreto 1090-04 y decreto 54-21:** Crean y transforman la OPTIC en OGTIC, otorgándole en su artículo 9 la responsabilidad de velar por la seguridad y privacidad de la información. La NORTIC A8 es la **herramienta de control técnico** clave para ejecutar este mandato.

10. **Decreto 229-07 sobre la implementación del gobierno electrónico:** Refuerza la obligación de adoptar las NORTIC. La NORTIC A8 provee los **controles de seguridad indispensables** para que la digitalización de los procesos gubernamentales sea confiable.

11. **Decreto 92-22 que establece el Marco Nacional de Interoperabilidad Gubernamental:** Define la interoperabilidad. La NORTIC A8 provee el marco para asegurar el **intercambio seguro de información** entre los sistemas que interoperan, mediante controles de cifrado y autenticación.

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. Estos decretos constituyen la base jurídica de la obligatoriedad de la presente norma, vinculando la eficiencia a una **base sólida de ciberseguridad.**

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 los controles de ciberseguridad obligatorios que deben seguir los organismos del Estado Dominicano para la protección de sus activos de información y la infraestructura tecnológica que los soporta, garantizando la confidencialidad, integridad y disponibilidad de los datos en los sistemas gubernamentales.

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:

- **Proteger la confidencialidad, integridad y disponibilidad (la tríada de la seguridad)** de la información y los sistemas del Estado.
- **Fortalecer la postura de defensa** del organismo mediante la implementación de controles de seguridad técnicos, administrativos y físicos para reducir los riesgos cibernéticos.

- **Establecer capacidades de monitoreo y respuesta** para detectar, analizar y contener incidentes de ciberseguridad de manera oportuna y eficaz.
- **Fomentar una cultura de ciberseguridad** a través de la concienciación y capacitación continua del personal.
- **Promover la mejora continua** de las prácticas de seguridad de la información, adaptándose a nuevas amenazas y cambios en el entorno tecnológico.

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, los delitos de alta tecnología y la protección de datos en el Estado.

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

- **NORTIC A7 – Norma para la Administración de la Seguridad de la Información:** Establece los mandatos de gobernanza, las políticas y los programas que esta norma ayuda a implementar a nivel técnico.
- **NORTIC A9 – Norma para la Gestión de Riesgos Tecnológicos y Continuidad Operativa:** Provee la metodología de gestión de riesgos y continuidad que esta norma utiliza como referencia.

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

- **Marco de Ciberseguridad del NIST (NIST Cybersecurity Framework):** Estructura principal que guía los capítulos de controles de esta norma.
- **Controles de Seguridad Críticos del CIS (Center for Internet Security):** Para la definición de controles de seguridad técnica esenciales.
- **ISO/IEC 27002 - Controles de seguridad de la información:** Guía internacional para la implementación de controles de seguridad.

Sección 1.04. Términos y definiciones

- **Activo:** Cualquier recurso de valor para la organización, incluyendo datos, sistemas, software, hardware, servicios, instalaciones y personal.
- **Autenticación Multifactor (MFA):** Mecanismo de verificación de identidad que combina al menos dos factores de autenticación distintos (algo que el usuario sabe, tiene o es).
- **Cadena de suministro:** El ecosistema de proveedores, servicios y componentes externos que contribuyen al funcionamiento de la infraestructura tecnológica de una organización.
- **Ciberseguridad:** Conjunto de prácticas y controles para proteger sistemas, redes, programas y datos frente a ataques, daños o accesos no autorizados en el ciberespacio.
- **Controles de seguridad:** Medidas (políticas, procedimientos, mecanismos técnicos o administrativos) implementadas para mitigar riesgos de seguridad.
- **Criptografía:** Ciencia y arte de escribir mensajes en forma

cifrada o en código, utilizada para proteger la confidencialidad e integridad de la información.

- **Gestión de incidentes:** El proceso completo de identificar, analizar, contener, erradicar y recuperarse de un incidente de seguridad, incluyendo las lecciones aprendidas.
- **Gestión de Identidades y Accesos (IAM):** El marco de políticas y tecnologías para garantizar que las personas y entidades adecuadas tengan el acceso apropiado a los recursos tecnológicos en el momento oportuno.
- **Marco de Ciberseguridad del NIST:** Estructura desarrollada por el Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. que proporciona una guía para mejorar la gestión del riesgo cibernético.
- **Resiliencia:** En el contexto de la ciberseguridad, la capacidad de un sistema para resistir, adaptarse y recuperarse rápidamente de incidentes que afecten su operatividad.
- **Riesgo cibernético:** La posibilidad de sufrir pérdidas o daños como resultado de una amenaza cibernética que explota una vulnerabilidad en los sistemas de información.
- **SIEM (Security Information and Event Management):** Sistema que centraliza, correlaciona y analiza eventos de seguridad generados por diversas fuentes en tiempo real para facilitar la detección de amenazas.
- **Vulnerabilidad:** Una debilidad en un sistema, proceso o control que puede ser explotada por una amenaza para causar un impacto adverso.
- **Zero Trust (Confianza Cero):** Un modelo de seguridad que opera bajo el principio de "nunca confiar, siempre verificar", asumiendo que las amenazas pueden originarse tanto dentro como fuera del perímetro de la red.

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

GOBERNANZA INSTITUCIONAL Y DE LA INFORMACIÓN

Este capítulo detalla los controles técnicos y operativos requeridos para implementar los programas de gestión de activos y de gestión de riesgos, conforme a los mandatos establecidos 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)

Esta sección establece los controles operativos para la identificación, inventario, clasificación y seguimiento de todos los activos institucionales. Abarca desde los componentes físicos y el software hasta los flujos de información, los activos externos y la clasificación de los datos según su criticidad, sentando las bases para una gestión de riesgos informada.

Subsección 2.01.1. Inventario de activos tecnológicos físicos

a) Debe mantenerse un inventario detallado de todos los dispositivos físicos bajo gestión del Organismo, incluyendo computadoras, servidores, enrutadores, cortafuegos, dispositivos de almacenamiento, impresoras y demás equipos tecnológicos relevantes.

b) Deben existir procedimientos de identificación y etiquetado de activos gestionados por el departamento de tecnología o seguridad de la información, que aseguren la asignación única de identificadores y su asociación con áreas o usuarios responsables.

c) El proceso de incorporación y retiro de activos físicos debe estar alineado con el procedimiento de actualización del inventario, de forma que cada alta o baja quede registrada de manera inmediata, verificable y documentada.

d) Debe utilizarse una herramienta tecnológica de gestión de activos que permita automatizar la identificación, clasificación, seguimiento y auditoría de los dispositivos, integrando funcionalidades de descubrimiento de red, reportes de estado y alertas sobre cambios no autorizados.

Subsección 2.01.2. Inventario de plataformas y aplicaciones de software

a) Debe mantenerse evidencia de un inventario actualizado de todas las plataformas y aplicaciones utilizadas por el Organismo, incluyendo sistemas operativos, aplicaciones administrativas, plataformas en la nube, herramientas de productividad, aplicaciones personalizadas y software crítico para la misión.

b) Debe establecerse una clasificación de las plataformas y aplicaciones conforme a su categoría lógica (por ejemplo, bases de datos, software de gestión, herramientas de comunicación), su función institucional y el departamento responsable de su gestión o uso. Asimismo, debe utilizarse una nomenclatura institucional que permita asignar identificadores únicos a cada plataforma y mantener documentación detallada que relacione esos identificadores con sus atributos técnicos y operacionales.

c) Debe garantizarse la actualización continua del inventario, especialmente al momento de incorporar o retirar software,

realizar migraciones, actualizaciones mayores o cambios de arquitectura tecnológica, con evidencia documental que respalde cada modificación.

d) Debe implementarse una herramienta tecnológica de gestión de activos de software que automatice la identificación, seguimiento y auditoría del uso de plataformas y aplicaciones, integrándose cuando sea posible con sistemas de gestión de configuración, monitoreo o control de licencias.

Subsección 2.01.3. Mapeo de flujos de información

a) Debe mantenerse evidencia documental sobre cómo fluye la información dentro del Organismo, detallando los sistemas, servicios, redes, procesos y ubicaciones físicas o lógicas que participan en la generación, transmisión, almacenamiento y consumo de datos.

b) Deben identificarse y documentarse formalmente todos los canales de comunicación utilizados para la transferencia de información institucional, incluyendo correo electrónico, VPN, transferencias vía SFTP, conexiones entre servidores, APIs y herramientas colaborativas autorizadas. Asimismo, deben elaborarse diagramas o esquemas actualizados que representen los flujos de información internos y externos.

c) Debe disponerse de una herramienta de monitoreo de red que permita analizar, registrar y alertar sobre el tráfico de información entre los sistemas del Organismo, facilitando la identificación de patrones normales de uso y la detección de comportamientos anómalos o no autorizados.

d) Esta información debe utilizarse para validar que los canales utilizados estén alineados con las políticas de seguridad institucional y que no existan rutas informales, inseguras o desconocidas de intercambio de información que representen un riesgo.

Subsección 2.01.4. Catálogo de activos tecnológicos externos

a) Debe mantenerse un catálogo actualizado de los sistemas de información, plataformas, servicios, componentes y recursos tecnológicos que se encuentran fuera del entorno interno del Organismo pero que son utilizados en sus procesos institucionales o que impactan en la seguridad, continuidad o integridad de su información.

b) Este catálogo debe incluir, al menos, servicios en la nube (IaaS, PaaS, SaaS), infraestructuras compartidas, soluciones de terceros interconectadas, integraciones API, repositorios externos, herramientas administradas por proveedores y cualquier otro activo digital gestionado fuera del entorno directo del Organismo.

c) La documentación del catálogo debe reflejar las relaciones funcionales y de dependencia entre estos servicios externos y los procesos institucionales, así como sus responsables, niveles de criticidad y frecuencia de uso.

d) Debe evidenciarse la actualización periódica del catálogo, así como la evaluación de los riesgos asociados a cada sistema o componente externo identificado, incluyendo aspectos de confidencialidad, disponibilidad, integridad y cumplimiento normativo.

Subsección 2.01.5. Clasificación y priorización de recursos

a) Deben priorizarse recursos tales como hardware, software, dispositivos móviles, datos, personal técnico y tiempo operativo, en función de su relevancia para los procesos misionales y de apoyo del Organismo.

b) Debe disponerse de evidencia documental que refleje la clasificación de los recursos conforme a su valor para el negocio, incluyendo criterios de sensibilidad de los datos, impacto

reputacional, obligatoriedad legal, dependencia operativa y coste de recuperación.

c) Debe establecerse la criticalidad de cada recurso, basada en su potencial impacto negativo ante un evento disruptivo, ya sea por pérdida de disponibilidad, compromiso de integridad, pérdida de confidencialidad o interrupción de la función que respalda.

d) Debe definirse y aplicarse una jerarquía de priorización institucional que permita tomar decisiones de asignación de recursos, protección y recuperación de forma objetiva, basada en niveles de importancia, criticidad y valor previamente establecidos.

e) Debe utilizarse un sistema de clasificación que permita la asignación automática o semiautomática de prioridades a los recursos, apoyado en herramientas tecnológicas y políticas formales, integrando dicha clasificación con los procesos de gestión de activos, riesgos y continuidad de operaciones.

Subsección 2.01.6. Seguimiento y clasificación de datos

a) Debe mantenerse una lista oficial de los tipos de datos que han sido designados como de interés institucional, incluyendo, pero no limitándose a: información de identificación personal (PII), información de salud protegida (PHI), datos financieros o contables, propiedad intelectual, y datos vinculados a sistemas de tecnología operativa (OT).

b) Debe establecerse un proceso continuo de descubrimiento y análisis de datos distribuidos en los sistemas de información del Organismo, para identificar nuevas instancias o ubicaciones donde se almacenen, procesen o transmitan tipos de datos designados, incluso cuando no hayan sido formalmente registrados.

c) Los datos identificados deben clasificarse de manera formal

utilizando esquemas de etiquetado o marcación que especifiquen su nivel de sensibilidad, requisitos de protección, y condiciones de uso, conforme a las políticas institucionales de seguridad y cumplimiento normativo.

d) Debe mantenerse información actualizada sobre la procedencia (origen), propiedad (responsable funcional), ubicación física o lógica (geolocalización) y flujo de cada tipo de dato identificado, de forma que se facilite su trazabilidad, protección y auditoría.

Sección 2.02. Análisis y tratamiento de riesgos cibernéticos

Esta sección detalla los controles operativos para la identificación de amenazas y vulnerabilidades, así como los procedimientos para el análisis, evaluación y tratamiento del riesgo cibernético, en consonancia con las metodologías definidas en la NORTIC A9.

Subsección 2.02.1. Gestión de vulnerabilidades técnicas

a) Debe utilizarse una herramienta de escaneo y análisis de vulnerabilidades que permita detectar proactivamente debilidades técnicas en sistemas operativos, aplicaciones, configuraciones, dispositivos de red y otros componentes tecnológicos relevantes. La herramienta debe estar actualizada con fuentes confiables de inteligencia de vulnerabilidades (por ejemplo, CVE, NVD).

b) Deben realizarse escaneos de vulnerabilidades con una frecuencia definida, incluyendo análisis programados y análisis bajo demanda ante cambios significativos en la infraestructura, incorporación de nuevos activos o detección de incidentes de seguridad.

c) Las vulnerabilidades identificadas deben ser registradas en un repositorio institucional, documentando su naturaleza

técnica, nivel de severidad, activo afectado, fecha de detección, clasificación según criticidad, riesgo potencial asociado, y acciones recomendadas.

d) El análisis de vulnerabilidades debe estar integrado con la gestión de riesgos de ciberseguridad, de forma que las debilidades detectadas se prioricen y se asignen responsabilidades para su tratamiento dentro de plazos definidos, conforme a su nivel de riesgo.

Subsección 2.02.2. Gestión de inteligencia de amenazas

a) Debe mantenerse evidencia de la afiliación o participación del Organismo en foros, redes y plataformas de intercambio de inteligencia de amenazas, tales como el CSIRT Nacional, centros sectoriales, alianzas regionales o mecanismos multilaterales de ciberseguridad.

b) La inteligencia de amenazas debe incorporarse a los procesos de evaluación de riesgos, priorización de controles, ajustes en reglas de detección, aplicación de parches, revisión de configuraciones y planificación de medidas preventivas.

c) Debe documentarse el ciclo de vida de la información procesada, incluyendo su fuente, análisis realizado, decisiones adoptadas y medidas de protección derivadas. Este procedimiento debe incluir alertas internas, generación de reportes y comunicación con unidades técnicas involucradas.

Subsección 2.02.3. Análisis de fuentes y actores de amenazas

a) Deben analizarse fuentes internas de amenazas, como colaboradores descontentos, errores humanos, accesos privilegiados mal gestionados o proveedores con control sobre infraestructura crítica, evaluando sus capacidades, niveles de acceso y posibles motivaciones.

b) Deben evaluarse también fuentes externas de amenazas, incluyendo actores como grupos de amenazas persistentes avanzadas (APT), ciberdelincuentes, hacktivistas, actores patrocinados por Estados, competidores maliciosos y amenazas emergentes del ecosistema digital.

c) Las amenazas identificadas deben ser documentadas de manera estructurada, incluyendo su origen (interno o externo), nivel de sofisticación, motivaciones (económicas, políticas, ideológicas), objetivos potenciales, vectores de ataque comúnmente utilizados y ejemplos de campañas previas.

d) Esta documentación debe ser parte de una base de datos de inteligencia operativa del Organismo, y debe ser actualizada de forma periódica o cuando se reciban alertas relevantes a través de fuentes externas confiables (por ejemplo, CSIRT nacional, proveedores de inteligencia, informes sectoriales).

Subsección 2.02.4. Análisis del riesgo cibernético

a) Una vez identificadas las amenazas y vulnerabilidades, el organismo debe evaluar el riesgo cibernético utilizando la metodología de análisis, evaluación y priorización definida en la NORTIC A9, Capítulos 2.2 y 2.3.

b) La evaluación del impacto debe utilizar como insumo principal los resultados del Análisis de Impacto al Negocio (BIA), realizado conforme a la NORTIC A9.

Subsección 2.02.5. Tratamiento del riesgo cibernético

a) Para cada riesgo cibernético que supere la tolerancia definida, el Organismo debe seleccionar una de las estrategias de tratamiento (mitigar, transferir, aceptar, evitar) conforme a la metodología definida en la NORTIC A9, Capítulo 2.4.

b) Las decisiones de tratamiento deben documentarse en la Declaración de Aplicabilidad, como se exige en la NORTIC A7.

Subsección 2.02.6. Gestión de cambios y excepciones de riesgo

a) Deben implementarse y cumplirse procedimientos documentados que regulen la gestión de cambios en los controles, procesos o configuraciones vinculadas a las respuestas al riesgo, incluyendo su revisión técnica, pruebas previas, justificación, aprobación formal y documentación.

b) Cada cambio propuesto debe venir acompañado de una evaluación de riesgos asociada, que identifique los impactos potenciales de ejecutar o no ejecutar dicho cambio, así como orientaciones claras para su reversión segura en caso de fallos o resultados no esperados.

c) Toda solicitud de excepción a controles establecidos debe incluir una justificación técnica o de negocio, una evaluación formal del riesgo que implica su aprobación, y un plan de tratamiento o respuesta para mitigar o monitorear el riesgo aceptado.

d) Debe mantenerse un registro centralizado y actualizado de todas las excepciones otorgadas, incluyendo fechas de aprobación, responsables, condiciones, duración y compromisos asociados.

e) Los riesgos aceptados temporalmente deben ser revisados de forma periódica conforme a los hitos definidos en los planes de acción, verificando si las condiciones originales se mantienen, si se requiere extender la excepción o si se deben aplicar controles definitivos.

Subsección 2.02.7. Intercambio de información de seguridad

a) Deben establecerse reglas y protocolos formales, incluidos en acuerdos contractuales, para el intercambio de información sobre vulnerabilidades entre el Organismo y sus proveedores, asegurando canales seguros, tiempos de notificación definidos, clasificación de la información y condiciones de confidencialidad.

b) Las responsabilidades para la recepción, análisis y respuesta a divulgaciones de amenazas, vulnerabilidades o incidentes reportadas por terceros deben ser asignadas explícitamente dentro del Organismo, y acompañadas de procedimientos claros que definan los pasos para evaluar impacto, priorizar acciones y emitir retroalimentación.

c) La comunicación debe mantenerse activa con el CSIRT Nacional del Centro Nacional de Ciberseguridad, y otros actores del ecosistema, facilitando la coordinación en la contención de amenazas comunes, la aplicación de parches, y la mitigación de vulnerabilidades explotables.

d) Debe mantenerse evidencia documental de los intercambios realizados, las acciones tomadas como resultado, los reportes emitidos a terceros y la validación de las respuestas implementadas.

Subsección 2.02.8. Evaluación de seguridad en adquisiciones

a) Debe establecerse un procedimiento formal de evaluación de ciberseguridad para todos los productos tecnológicos que serán utilizados en funciones críticas del Organismo, incluyendo hardware, software, soluciones en la nube, plataformas de control y otros activos digitales.

b) La evaluación debe verificar la autenticidad del origen del producto (fabricante, integrador o canal autorizado), así como su integridad física y lógica, descartando la existencia de componentes alterados, puertas traseras o modificaciones maliciosas.

c) Debe incluirse la revisión de certificaciones, historial de vulnerabilidades, resultados de pruebas de seguridad, cuando estén disponibles, y cumplimiento con estándares reconocidos.

d) Este control debe aplicarse antes de la adquisición y como

condición para el uso en entornos productivos, especialmente en sistemas que manejen información sensible o formen parte de infraestructuras críticas.

e) Las evaluaciones deben documentarse y formar parte del expediente técnico de cada adquisición, incluyendo responsables, hallazgos, decisiones y medidas adoptadas.

Subsección 2.02.9. Evaluación de riesgos de proveedores

a) Deben establecerse procedimientos formales para evaluar el riesgo cibernético que representan los proveedores, tomando en consideración su rol dentro de la operación del Organismo, el tipo de acceso otorgado, la criticidad del servicio prestado y su nivel de madurez en ciberseguridad.

b) Las evaluaciones deben incluir tanto criterios comerciales como técnicos, tales como cumplimiento con políticas de seguridad, existencia de programas de gestión de vulnerabilidades, antecedentes de incidentes, uso de terceros subcontratados, y dependencias tecnológicas críticas.

c) Las evaluaciones deben realizarse previo a la contratación, y actualizarse periódicamente según el nivel de riesgo del proveedor, la evolución de amenazas y el grado de exposición.

d) Deben mantenerse registros documentados de los resultados de las evaluaciones, acciones derivadas, criterios utilizados y planes de mejora o mitigación acordados.

Sección 2.03. Mejora continua del programa de ciberseguridad

Esta sección establece los controles para la validación periódica, el monitoreo del desempeño y la implementación de mejoras basadas en lecciones aprendidas, asegurando que las defensas del organismo se mantengan vigentes y efectivas.

Subsección 2.03.1. Evaluaciones continuas del programa de ciberseguridad

a) Deben realizarse autoevaluaciones periódicas sobre los servicios críticos del Organismo, considerando amenazas actualizadas, así como tácticas, técnicas y procedimientos (TTP) conocidos que puedan ser utilizados por actores maliciosos contra dichos servicios.

b) Debe contemplarse la contratación de auditorías externas independientes o evaluaciones de terceros para validar la madurez del programa de ciberseguridad, verificar el cumplimiento de controles y descubrir vulnerabilidades o debilidades que no hayan sido detectadas internamente.

c) Deben implementarse herramientas automatizadas para la evaluación continua del cumplimiento de los requisitos de ciberseguridad establecidos, incluyendo revisiones de configuración, parches aplicados, controles de acceso, cumplimiento normativo y desviaciones de políticas.

d) Los hallazgos de estas evaluaciones deben documentarse, priorizarse según su nivel de riesgo, y traducirse en planes de acción concretos con responsables, plazos definidos y seguimiento periódico.

Subsección 2.03.2. Implementación de mejoras basadas en lecciones aprendidas

a) Debe mantenerse un proceso estructurado para revisar los hallazgos de simulaciones, ejercicios de mesa, pruebas técnicas, revisiones internas o auditorías independientes, a fin de identificar lecciones aprendidas y traducirlas en acciones de mejora para futuras respuestas a incidentes.

b) Las pruebas deben involucrar, cuando corresponda, a partes interesadas internas clave como la alta dirección, las unidades legales, recursos humanos, adquisiciones, comunicaciones

y otras funciones institucionales estratégicas, para asegurar la coordinación y la eficacia en la toma de decisiones ante cibercrisis.

c) Deben ejecutarse pruebas de penetración autorizadas sobre sistemas de alto riesgo, previamente aprobadas por la dirección, con el objetivo de identificar brechas explotables, validar controles y reforzar la seguridad.

d) Deben existir planes de contingencia para responder a la detección de productos o servicios adulterados o no auténticos, especialmente cuando provienen de proveedores externos, incluyendo procedimientos de aislamiento, notificación y reemplazo.

e) Se deben recopilar, analizar y utilizar métricas de rendimiento de herramientas y servicios de seguridad para tomar decisiones sobre inversiones, rediseños y ajustes del programa de ciberseguridad institucional.

Subsección 2.03.3. Monitoreo del desempeño y métricas de seguridad (KPIs/KRIs)

a) Deben organizarse sesiones colaborativas de revisión postincidente o postejercicio junto con proveedores y otras partes involucradas, con el objetivo de identificar fallas, éxitos, brechas de coordinación y oportunidades de mejora mutua.

b) Deben establecerse métricas operativas de ciberseguridad (KPIs/KRIs) que permitan medir el desempeño de los controles, la madurez de las capacidades implementadas, y el cumplimiento de objetivos definidos. Estas métricas deben analizarse en series temporales para identificar tendencias y patrones.

c) La información obtenida a través de estos procesos debe ser utilizada para justificar cambios normativos, reasignación de recursos, adquisición de nuevas herramientas o fortalecimiento de capacidades internas.

a) Debe desarrollarse y mantenerse un plan específico de gestión de vulnerabilidades, que establezca mecanismos para identificar, evaluar, clasificar, priorizar, probar y tratar todas las vulnerabilidades conocidas en los activos tecnológicos del Organismo.

b) Los planes de ciberseguridad deben ser comunicados de manera clara a todos los responsables de su ejecución, así como a las partes afectadas interna o externamente, incluyendo socios estratégicos, unidades de soporte y autoridades competentes.

CAPÍTULO 3

ARQUITECTURA Y CONTROLES DE PROTECCIÓN

Este capítulo detalla el conjunto de controles preventivos y las medidas de protección que constituyen la primera línea de defensa de la organización. Su objetivo es establecer una arquitectura de seguridad robusta para salvaguardar los activos de información y la infraestructura tecnológica contra accesos no autorizados y otras ciberamenazas.

Sección 3.01. Gestión de identidades, autenticación y control de acceso

Esta sección establece los controles para el ciclo de vida de las identidades digitales, los mecanismos de autenticación y la aplicación del principio de mínimo privilegio.

Subsección 3.01.1. Gestión de identidades y credenciales de acceso

a) Deben establecerse procedimientos formales para la emisión inicial de identidades y credenciales, que aseguren la validación previa de la identidad del solicitante y el principio de menor privilegio, según las funciones asignadas.

b) La gestión de identidades debe mantenerse de forma continua mediante un sistema centralizado (IAM – Identity and Access Management), que permita la administración eficiente de altas, bajas, modificaciones, delegaciones temporales y actualizaciones

asociadas a cambios organizativos.

c) Deben realizarse verificaciones periódicas y auditorías internas para garantizar que todas las identidades y credenciales activas siguen siendo válidas, necesarias y autorizadas, identificando accesos obsoletos o indebidos.

d) Debe establecerse un proceso de revocación inmediata de credenciales ante eventos como desvinculación laboral, transferencia de funciones, pérdida de dispositivos o incidentes de seguridad. Este proceso debe ser automático o manual con tiempos de ejecución definidos y supervisión posterior.

e) Todos los eventos relacionados con la emisión, modificación, verificación y revocación de credenciales deben registrarse en sistemas de auditoría que permitan trazabilidad, monitoreo y cumplimiento de políticas.

Subsección 3.01.2. Mecanismos de autenticación basados en riesgo

a) Debe realizarse una evaluación de riesgos para cada categoría de transacción, servicio o recurso, con el fin de determinar el nivel mínimo requerido de autenticación. Esta evaluación debe considerar la sensibilidad de la información, el impacto potencial en caso de compromiso, y el contexto operacional.

b) Debe adoptarse autenticación multifactor (MFA) para transacciones de alto riesgo, como acceso a sistemas críticos, datos personales o financieros, y tareas con privilegios elevados. El uso de MFA debe seguir estándares de seguridad robustos y contemplar factores independientes (algo que el usuario sabe, tiene o es).

c) Deben implementarse mecanismos de autenticación adaptativa que ajusten dinámicamente el nivel de autenticación requerido según condiciones contextuales como ubicación, dispositivo, comportamiento, horario o nivel de amenaza detectado.

d) La selección de métodos de autenticación debe incluir un análisis del impacto en la privacidad del usuario, evitando mecanismos excesivamente intrusivos o que recolecten más información de la necesaria para cumplir con el propósito de autenticación.

e) Los niveles de autenticación deben ser documentados, revisados periódicamente y actualizados ante cambios en el entorno tecnológico, normativo o en el nivel de amenaza.

Subsección 3.01.3. Medidas de autenticación reforzada para recursos críticos

a) Debe requerirse el uso obligatorio de autenticación multifactor (MFA) para accesos a recursos críticos, sistemas con información sensible, administración de infraestructuras y servicios expuestos externamente, conforme al principio de defensa en profundidad.

b) Los mecanismos de autenticación deben incluir procesos de reautenticación periódica basados en el nivel de riesgo y el tipo de recurso, especialmente en contextos de arquitecturas de confianza cero, sesiones prolongadas o accesos sensibles desde ubicaciones no confiables.

c) Deben establecerse mecanismos de emergencia que permitan al personal autorizado acceder a cuentas críticas o recursos esenciales durante situaciones excepcionales, asegurando trazabilidad, controles compensatorios y registro de todas las acciones realizadas.

Subsección 3.01.4. Aseguramiento de la legitimidad de identidades digitales

a) Deben implementarse procesos formales de verificación de identidad antes de emitir credenciales de acceso, asegurando que toda identidad corresponda a un usuario o sistema legítimamente autorizado, mediante validación documental, confirmación de datos personales u otros métodos de validación apropiados.

b) Las identidades deben estar vinculadas de manera segura a credenciales únicas, tales como contraseñas robustas, certificados digitales, tokens criptográficos o factores biométricos, evitando duplicaciones o reutilizaciones.

c) Debe garantizarse la afirmación continua de la identidad durante las interacciones, a través de mecanismos confiables como el uso de tokens de autenticación, autenticadores físicos, biometría o autenticación basada en certificados.

d) La autenticación multifactor (MFA) debe ser implementada obligatoriamente para accesos sensibles o privilegiados, incorporando al menos dos factores independientes entre sí (por ejemplo, contraseña + token, o biometría + PIN).

e) Deben adoptarse mecanismos de monitoreo continuo de las sesiones y autenticaciones para detectar patrones de comportamiento anómalos, intentos de suplantación, accesos no autorizados o desviaciones de las políticas establecidas.

Subsección 3.01.5. Control de acceso lógico, privilegio mínimo y separación de funciones

a) Debe asignarse a cada usuario únicamente el nivel de acceso y privilegios necesarios para el desempeño de sus responsabilidades, evitando permisos excesivos, genéricos o sin justificación documental.

b) Deben establecerse mecanismos de separación de funciones, asegurando que las tareas críticas en los procesos de negocio (como aprobación y ejecución de pagos, o gestión y auditoría de accesos) no sean realizadas por una misma persona o rol sin controles compensatorios.

c) Las autorizaciones de acceso deben revisarse de forma periódica (al menos semestralmente o ante cambios de función) para validar su vigencia, necesidad y adecuación al rol funcional, con evidencia de la revisión realizada y su aprobación.

d) Debe mantenerse un registro detallado de actividades de acceso, incluyendo autenticaciones, uso de privilegios, intentos de escalamiento y modificaciones de permisos, que permita auditar y detectar actividades indebidas o violaciones de política.

e) Deben ofrecerse programas de capacitación orientados a los usuarios, sobre la importancia de adherirse al principio de mínimo privilegio y de no acumular funciones críticas que comprometan la seguridad institucional.

Subsección 3.01.6. Controles de acceso físico a áreas críticas

a) Deben implementarse medidas de control físico que incluyan el uso de cerraduras electrónicas o mecánicas, sistemas de tarjetas de proximidad, lectores biométricos, y sistemas de videovigilancia en áreas críticas tales como centros de datos, salas de comunicaciones, archivos sensibles, entre otros.

b) Deben utilizarse métodos de identificación y autenticación personal (como credenciales, biometría o PIN) que permitan verificar la legitimidad del acceso y registrar adecuadamente cada ingreso o salida de personal autorizado.

c) Deben mantenerse registros de acceso físico actualizados, que incluyan fecha, hora, identidad del usuario, área accedida y duración de la estancia, con trazabilidad suficiente para realizar auditorías y responder ante incidentes.

Sección 3.02. Capacitación y concienciación en seguridad cibernética

Esta sección define los requisitos para el desarrollo de programas de concienciación y capacitación continua, garantizando que todos los colaboradores comprendan su rol y responsabilidad en la protección de los activos digitales del Estado.

Subsección 3.02.1. Programa de concienciación y capacitación continua

a) Deben establecerse programas de concientización formalizados que aborden temáticas fundamentales como el uso seguro de contraseñas, prevención de malware, protección de información sensible, identificación de amenazas comunes y uso seguro de tecnologías de la información.

b) Debe garantizarse la capacitación continua del personal, con actualizaciones periódicas sobre amenazas emergentes, cambios normativos, mejores prácticas de ciberhigiene y nuevos procedimientos internos.

c) Debe realizarse simulaciones de ataques de ingeniería social, tales como campañas simuladas de phishing, que permitan medir la respuesta de los usuarios, generar retroalimentación y ajustar las estrategias educativas.

d) Deben comunicarse de forma clara y accesible las políticas institucionales de seguridad de la información, asegurando que todos los usuarios comprendan sus obligaciones y las consecuencias del incumplimiento.

e) El Organismo debe proveer materiales educativos complementarios, como guías prácticas, infografías, cápsulas informativas y recursos digitales, disponibles en formatos accesibles y adaptados al nivel de conocimiento del personal.

a) Deben identificarse los roles especializados dentro del Organismo que requieren formación adicional en materia de ciberseguridad, tales como: personal de tecnologías de la información, seguridad física, unidades financieras, jurídicos, directivos, así como usuarios con acceso a datos sensibles o infraestructuras críticas.

b) La formación debe ser adaptada al nivel de riesgo y responsabilidad de cada rol, e incluir conocimientos específicos sobre gestión de incidentes, uso seguro de privilegios, controles regulatorios, gestión de proveedores, protección de datos personales y cumplimiento normativo.

c) El Organismo debe garantizar que los terceros con acceso autorizado, incluyendo contratistas, socios y proveedores clave, también participen en programas de formación adecuados a los servicios que prestan.

d) Deben establecerse mecanismos para evaluar periódicamente la comprensión de las prácticas de seguridad requeridas para cada rol, utilizando pruebas, ejercicios prácticos o simulaciones que permitan medir el nivel de madurez del personal.

e) Las capacitaciones deben actualizarse al menos una vez al año, incluyendo módulos que refuercen prácticas existentes, informen sobre amenazas emergentes, cambios normativos o tecnológicos, y actualicen los procedimientos institucionales aplicables.

f) El programa de concienciación y sus materiales deben ser revisados y actualizados, como mínimo, de forma anual.

Sección 3.03. Protección de datos en reposo, en uso y en tránsito

Esta sección establece los controles técnicos y procedimentales para proteger la confidencialidad, integridad y disponibilidad de la información en todos sus estados: en reposo (almacenada), en tránsito (en comunicación) y en uso (en procesamiento).

Subsección 3.03.1. Protección de datos en reposo

a) Deben implementarse mecanismos de cifrado de datos almacenados, tanto en reposo como en soportes de respaldo, utilizando algoritmos robustos y estándares reconocidos, a fin de proteger su confidencialidad e integridad.

b) Deben establecerse procedimientos seguros de gestión del ciclo de vida de las claves criptográficas, incluyendo su generación, almacenamiento, uso, rotación, distribución y destrucción, garantizando su confidencialidad y disponibilidad únicamente para usuarios autorizados.

c) Deben aplicarse controles de acceso basados en roles, que aseguren que solo personas o sistemas con autorización explícita puedan acceder, modificar o eliminar datos almacenados. Estos controles deben estar documentados y alineados con el principio de mínimo privilegio.

d) Los sistemas deben incluir capacidades de monitoreo y registro para detectar y alertar sobre actividades anómalas o sospechosas relacionadas con los datos almacenados, tales como accesos fuera de horario, intentos de lectura masiva o cambios no autorizados.

e) Deben establecerse procedimientos formales para el borrado seguro de los datos, que garanticen su eliminación permanente cuando estos ya no sean necesarios para fines operativos, legales o normativos, mediante técnicas como sobreescritura múltiple o destrucción física.

f) La integridad de los datos almacenados debe ser preservada mediante mecanismos de detección de manipulaciones no autorizadas, como firmas digitales, sumas de verificación (hashes) o controles de integridad basados en hardware.

Subsección 3.03.2. Protección de datos en tránsito

a) Debe implementarse el cifrado de las comunicaciones para proteger los datos transmitidos entre usuarios, sistemas, servicios y ubicaciones remotas, garantizando que no puedan ser interceptados o alterados por actores no autorizados.

b) Se deben utilizar protocolos criptográficos seguros y reconocidos, como TLS 1.2 o superior o IPsec, para proteger las comunicaciones, incluyendo las sesiones web (HTTPS) y las transferencias de archivos.

c) Deben establecerse mecanismos de autenticación de extremo a extremo, que validen la identidad tanto del emisor como del receptor de la información, asegurando que los datos solo sean accesibles para las partes autorizadas.

d) Los Organismos deben aplicar controles de acceso sobre las interfaces de red y los sistemas de comunicación, restringiendo quién puede emitir o recibir información, y documentando los permisos asociados.

e) Deben implementarse sistemas de monitoreo de red capaces de detectar accesos indebidos, intentos de intercepción, anomalías en la transmisión de datos, o fallos en la aplicación de cifrado.

f) Las claves criptográficas utilizadas para proteger los datos en tránsito deben ser generadas, distribuidas, almacenadas y rotadas de manera segura, conforme a las políticas de gestión de claves establecidas en la institución.

Subsección 3.03.3. Protección de datos en uso

a) Deben implementarse mecanismos de limpieza inmediata de datos confidenciales almacenados temporalmente en la memoria o registros del procesador (como contraseñas, claves privadas, o información sensible), tan pronto como dejen de ser necesarios para la operación.

b) Los sistemas deben garantizar que los datos en uso no puedan ser accedidos por usuarios o procesos no autorizados que operen en la misma plataforma, especialmente en entornos de cómputo compartido, virtualización o ejecución simultánea.

c) El Organismo debe utilizar funcionalidades de aislamiento de procesos y gestión segura de memoria, evitando que procesos legítimos puedan ser explotados para acceder a datos sensibles activos.

d) Deben aplicarse técnicas de protección de datos en uso tales como la encriptación de memoria, entornos de ejecución confiables, y verificación de integridad del sistema operativo y aplicaciones.

Sección 3.04. Protección de plataformas y software

Esta sección define los controles operativos y de gestión para el ciclo de vida completo de las plataformas y el software, desde la gestión de cambios y la configuración segura, hasta el desarrollo de aplicaciones (SDLC) y la generación de registros de auditoría.

Subsección 3.04.1. Gestión de cambios en configuraciones

a) Debe establecerse un proceso formal de solicitud y autorización de cambios, que incluya plantillas normalizadas, criterios de

prioridad, asignación de responsables y trazabilidad completa del ciclo de vida del cambio.

b) Todo cambio propuesto en configuraciones que afecten la infraestructura tecnológica debe ser precedido por una evaluación de riesgos, considerando los impactos potenciales en la seguridad, la operación de servicios críticos y la disponibilidad de los sistemas.

c) La aprobación de cambios debe estar restringida a personal autorizado, y especialmente controlada en los casos que involucren sistemas críticos, controladores de red, plataformas de autenticación, o configuración de seguridad.

d) Debe mantenerse un registro detallado de los cambios realizados, incluyendo la justificación, autorizaciones, fechas, responsables, pruebas realizadas, y cualquier impacto detectado posterior a la implementación.

e) Los cambios deben ser revisados posteriormente, verificando su correcta ejecución, validando que no se hayan introducido nuevas vulnerabilidades y asegurando el cumplimiento de las políticas de seguridad establecidas.

f) El proceso debe contemplar la capacidad de reversión o restauración de configuraciones anteriores en caso de errores, fallos operativos o deterioro en los controles de seguridad.

g) Debe establecerse un sistema de gestión de versiones que permita el seguimiento histórico de la configuración de cada sistema y la recuperación de estados anteriores.

Subsección 3.04.2. Retención y destrucción segura de datos

a) La retención y destrucción de datos debe regirse por la política de retención de la institución, la cual debe establecer los períodos de conservación aplicables a cada tipo de información, en función de su categoría, valor legal, utilidad operativa y

requisitos normativos, incluyendo los criterios y plazos para su eliminación.

b) El Organismo debe establecer procedimientos detallados para la destrucción segura de datos, tanto en medios digitales como físicos, mediante métodos aprobados tales como sobreescritura múltiple, desmagnetización, trituración o eliminación criptográfica.

c) Deben garantizarse procedimientos de eliminación segura de medios de almacenamiento, tales como discos duros, unidades USB, cintas magnéticas, SSD, CDs, o cualquier otro dispositivo, antes de su desecho, reutilización o donación.

d) Debe mantenerse un registro detallado de todas las operaciones de destrucción de datos, incluyendo la fecha de eliminación, responsable, método utilizado, tipo de datos destruidos y justificación del proceso.

e) El personal involucrado en tareas de destrucción de datos debe recibir formación específica, que asegure el conocimiento de las políticas vigentes, el uso de herramientas aprobadas y las responsabilidades asociadas al manejo de información confidencial.

f) Deben realizarse revisiones y auditorías periódicas para verificar el cumplimiento de las políticas de retención y destrucción, identificando oportunidades de mejora y documentando los hallazgos y acciones correctivas.

Subsección 3.04.3. Generación y gestión de registros de auditoría (logs)

a) Todos los sistemas operativos, aplicaciones, servicios internos y servicios contratados en la nube deben estar configurados para generar registros (logs) de auditoría, con información suficiente para apoyar actividades de monitoreo, investigación y respuesta ante incidentes.

b) Los generadores de registros deben estar configurados para compartir de forma segura sus registros con los sistemas de centralización de eventos (por ejemplo, SIEM, syslog centralizado, lagos de datos de seguridad), utilizando canales autenticados, cifrados y con validación de integridad.

c) Los registros deben incluir los datos mínimos requeridos, tales como: fecha/hora del evento, usuario, dispositivo, ubicación, tipo de acceso, recurso, resultado del intento y otros metadatos necesarios para evaluar el contexto.

d) La integración de registros debe abarcar tanto infraestructura local como servicios en la nube, entornos híbridos, redes internas, redes virtuales privadas (VPN), y aplicaciones críticas que manejen información sensible o de misión institucional.

e) Deben mantenerse políticas documentadas de retención, clasificación y protección de registros, asegurando que estén disponibles para análisis de incidentes y cumplan los requisitos legales o regulatorios aplicables.

Subsección 3.04.4. Ciclo de vida de desarrollo seguro (SDLC)

a) Debe elaborarse, implementarse y mantenerse un SDLC institucional que abarque formalmente las fases de planificación, diseño, desarrollo, pruebas, implementación, operación y mantenimiento, integrando controles de seguridad desde el inicio del proceso.

b) En cada fase del SDLC deben realizarse evaluaciones de riesgos, identificando amenazas potenciales, vulnerabilidades técnicas, fallas de diseño y dependencias críticas que puedan comprometer la confidencialidad, integridad o disponibilidad de la solución.

c) Debe incorporarse un conjunto de pruebas de seguridad específicas como parte de la validación funcional, incluyendo

análisis de código estático, pruebas dinámicas, escaneos de vulnerabilidades y validaciones de cumplimiento de controles de seguridad.

d) Los equipos de desarrollo, diseño y gestión de proyectos deben recibir formación periódica y concientización en desarrollo seguro, abordando principios, amenazas comunes (por ejemplo, OWASP Top 10), y buenas prácticas aplicables al contexto institucional.

e) Deben implementarse revisiones sistemáticas de código fuente, con especial énfasis en asegurar el uso de librerías confiables, validaciones de entrada/salida y la ausencia de funciones inseguras o desactualizadas.

f) Debe mantenerse documentación completa del SDLC, incluyendo decisiones de arquitectura, diseño, dependencias, evaluaciones de seguridad, bitácoras de cambios, pruebas realizadas y lecciones aprendidas.

Sección 3.05. Seguridad y resiliencia de la infraestructura de red

Esta sección establece los controles para asegurar su protección y resiliencia, abarcando desde la seguridad perimetral, la segmentación y los controles de comunicaciones, hasta la protección física y ambiental de los centros de datos y salas de comunicaciones.

Subsección 3.05.1. Seguridad y resiliencia de la infraestructura de red

a) Debe implementarse cifrado robusto para todas las comunicaciones sensibles que transiten por redes institucionales, privadas o públicas, utilizando protocolos criptográficos modernos y certificados válidos (por ejemplo, TLS 1.2 o superior, IPsec, VPN).

b) El acceso a las redes de control, sistemas de comunicación y plataformas críticas debe estar restringido mediante mecanismos de autenticación fuerte, como autenticación multifactor (MFA) o certificados digitales individuales.

c) Se deben establecer y aplicar controles de acceso basados en privilegios mínimos, que limiten el acceso a recursos, configuraciones y datos únicamente a personal autorizado conforme a sus funciones.

d) El Organismo debe implementar sistemas de monitoreo continuo (como IDS/IPS, SIEM o sondas de red) para la detección temprana de comportamientos anómalos, actividades sospechosas, intentos de intrusión o uso indebido de recursos.

e) Debe garantizarse la segmentación de redes, dividiendo y aislando las zonas críticas (por ejemplo, redes administrativas, operacionales, servicios públicos, DMZ) mediante firewalls, VLANs y arquitecturas de microsegmentación.

f) Todos los componentes de infraestructura deben mantenerse actualizados y parcheados periódicamente, conforme a un plan de gestión de vulnerabilidades que evalúe su nivel de exposición y criticidad operativa.

g) Deben aplicarse medidas de resiliencia ante ataques de denegación de servicio (DoS o DDoS), como filtros de tráfico, sistemas de mitigación, balanceadores de carga y planes de contingencia de conectividad.

h) Para cumplir con los Objetivos de Tiempo de Recuperación (RTO) definidos en la NORTIC A9, deben implementarse mecanismos de resiliencia tecnológica, tales como balanceadores de carga, arquitecturas de conmutación por error (failover), virtualización redundante y sistemas tolerantes a fallos.

a) Deben realizarse auditorías periódicas de cumplimiento para verificar que las instalaciones físicas y los controles implementados se ajustan a las políticas internas de seguridad y a los requisitos legales y regulatorios aplicables.

b) El acceso a las áreas críticas y centros de datos debe ser controlado mediante mecanismos de acceso físico restringido, tales como tarjetas electrónicas, controles biométricos, guardias de seguridad y registros de entrada/salida, permitiendo el ingreso únicamente a personal debidamente autorizado.

c) Se deben implementar medidas de protección contra amenazas ambientales, incluyendo sensores de humo, detectores de inundación, sistemas de supresión de incendios, unidades de climatización redundantes y mecanismos de protección contra sobretensiones eléctricas.

d) Las instalaciones que albergan infraestructuras críticas deben cumplir con las normativas de construcción y códigos aplicables, garantizando que los espacios físicos estén diseñados y construidos con criterios de seguridad estructural, acceso controlado y resistencia ambiental.

e) Deben establecerse procesos formales para la gestión de instalaciones, que aseguren el mantenimiento preventivo y correctivo de los equipos físicos, la supervisión continua del entorno y la disponibilidad de recursos de respaldo como generadores o UPS.

f) Deben desarrollarse y mantenerse actualizados planes de respuesta a emergencias físicas, que incluyan procedimientos de evacuación, manejo de incendios, continuidad operativa y comunicaciones en caso de eventos disruptivos.

g) La seguridad física de los equipos debe estar garantizada mediante su anclaje, almacenamiento seguro, etiquetado, inventariado, y protección contra robo, sabotaje o acceso indebido.

Subsección 3.05.3. Monitoreo y planificación de la capacidad de recursos

a) Deben establecerse procedimientos para el monitoreo constante del uso de recursos tecnológicos, incluyendo indicadores de almacenamiento, capacidad de procesamiento (CPU/RAM), consumo energético, uso de ancho de banda, espacio en disco y utilización de plataformas de virtualización o servicios en la nube.

b) El Organismo debe prever proactivamente las necesidades futuras de recursos tecnológicos, utilizando tendencias históricas, métricas de desempeño y análisis de proyección de carga, de modo que puedan anticiparse aumentos de demanda y garantizar la continuidad del servicio.

c) Deben integrarse capacidades de alerta temprana y monitoreo automatizado, que notifiquen al personal técnico sobre niveles de utilización cercanos al umbral crítico, permitiendo acciones preventivas antes de que se afecte la operación institucional.

d) Las plataformas tecnológicas deben estar diseñadas con capacidad de escalamiento, ya sea vertical (mayor capacidad de hardware) u horizontal (adición de instancias o nodos), permitiendo aumentar los recursos sin afectar la disponibilidad.

e) El monitoreo de recursos debe mantenerse documentado y revisado periódicamente, de forma que se tomen decisiones de adquisición, redimensionamiento o migración tecnológica con base en evidencia.

CAPÍTULO 4

DETECCIÓN Y MONITOREO DE SEGURIDAD

Este capítulo detalla los controles y capacidades para el monitoreo continuo de la infraestructura, la identificación de anomalías y la detección temprana de eventos de seguridad, permitiendo una respuesta oportuna ante posibles incidentes.

Sección 4.01. Identificación y evaluación de eventos de seguridad

Esta sección establece los requisitos para analizar anomalías, indicadores de compromiso y otros eventos potencialmente adversos. Su objetivo es caracterizar dichos eventos para detectar formalmente los incidentes de ciberseguridad, evaluar su impacto inicial y priorizar la respuesta.

Subsección 4.01.1. Establecimiento de líneas base operacionales

a) Debe definirse una línea base de operaciones normales que describa los patrones típicos de tráfico, autenticación, uso de servicios y flujos de datos entre usuarios, sistemas y redes, tomando como referencia periodos operativos estables.

b) La línea base debe ser documentada y validada con las unidades de tecnología y seguridad, y mantenerse actualizada conforme

a las modificaciones de infraestructura, cambios en los sistemas o actualizaciones operativas relevantes.

c) Debe implementarse un sistema de monitoreo continuo, utilizando herramientas de detección de anomalías o sondas de red, que permita comparar las operaciones actuales con la línea base establecida.

d) El Organismo debe desarrollar mecanismos de alerta y detección temprana para notificar cuando se produzcan desviaciones significativas, ya sea en volumen, frecuencia, origen o tipo de tráfico, así como accesos atípicos o uso no autorizado de recursos.

e) La línea base y sus desviaciones deben ser revisadas regularmente, al menos de forma semestral o después de eventos significativos, para garantizar que refleje adecuadamente el entorno actual.

Subsección 4.01.2. Capacidades de integración y correlación de eventos

a) Deben integrarse fuentes de datos heterogéneas incluyendo eventos de sistemas operativos, redes, aplicaciones empresariales, controladores de dominio, soluciones antimalware, firewalls, autenticación, VPN, entre otros.

b) Se requiere la implementación de un sistema de centralización de eventos de seguridad o plataforma equivalente que permita la correlación automática de eventos, con reglas o casos de uso diseñados para identificar patrones de comportamiento sospechoso, actividades anómalas y señales tempranas de amenazas persistentes.

c) Los datos de eventos deben ser normalizados para mantener un formato común y facilitar su análisis automatizado, evitando la pérdida de contexto entre diferentes tipos de registros.

d) Deben aplicarse técnicas de análisis multidimensional, correlacionando dimensiones como el tiempo, el origen geográfico, el tipo de evento, los usuarios involucrados y los activos afectados, para detectar comportamientos encadenados o ataques multivectoriales.

e) Se debe habilitar la detección de amenazas avanzadas mediante reglas de correlación, inteligencia de amenazas e integración con plataformas de análisis de comportamiento (UEBA) o detección basada en indicadores de compromiso (IoCs) y Técnicas, Tácticas y Procedimientos (TTPs).

f) Las correlaciones identificadas deben desencadenar acciones automáticas de contención y alerta, cuando se trate de amenazas conocidas, permitiendo respuestas rápidas y coordinadas.

Subsección 4.01.3. Evaluación del impacto de incidentes de seguridad

a) Debe realizarse un análisis detallado del incidente que identifique el tipo de evento, su vector de ataque, los activos comprometidos, y las actividades maliciosas ejecutadas o intentadas.

b) La evaluación debe incluir una estimación de pérdidas potenciales, considerando impactos financieros, interrupciones de operaciones críticas, afectación a la disponibilidad de servicios, daño reputacional, impacto en la confianza institucional y riesgos legales o regulatorios.

c) Deben definirse y aplicarse criterios de clasificación del impacto que permitan categorizar los incidentes en niveles, tomando como referencia la naturaleza de los activos afectados y la criticidad de las funciones que soportan.

d) Los incidentes de seguridad cibernética y de la información deberán agruparse conforme a su nivel de criticidad e impacto.

Para ello, se debe utilizar la clasificación detallada en el Anexo A: Tabla No.1 - Niveles de Criticidad de Incidentes de Seguridad.

e) La información sobre el impacto debe ser comunicada de manera efectiva a los responsables de la toma de decisiones, incluyendo la alta dirección, el equipo de respuesta a incidentes, el CSIRT Nacional y otros actores relevantes según el tipo de incidente.

f) La clasificación de impacto debe utilizarse como base para priorizar las acciones de respuesta, asignar recursos de contención y recuperación, y definir la necesidad de activar procedimientos de escalamiento o declaración de cibercrisis.

g) Los organismos deben utilizar los resultados del análisis de impacto para alimentar los procesos de lecciones aprendidas, revisión de controles de seguridad y actualización de los planes de continuidad, respuesta y recuperación.

Subsección 4.01.4. Generación y gestión de alertas de ciberseguridad

a) Deben utilizarse herramientas de ciberseguridad capaces de generar alertas automáticas ante la detección de comportamientos anómalos, indicadores de compromiso (IoCs), patrones conocidos de amenazas o desviaciones relevantes respecto a la línea base operativa.

b) Las alertas generadas en los sistemas e infraestructura tecnológica del Organismo gubernamental deben ser procesadas y transmitidas automáticamente hacia el Centro de Operaciones de Seguridad (SOC) del CSIRT Nacional del Centro Nacional de Ciberseguridad, los equipos de respuesta a incidentes sectoriales, y las herramientas de orquestación, automatización y respuesta internas, cuando estén disponibles.

c) Debe garantizarse que el personal autorizado, incluyendo los analistas del SOC, respondientes de incidentes y responsables técnicos, tenga acceso permanente a los registros de alertas

y hallazgos de análisis, a través de plataformas integradas y auditables.

d) Los Organismos deben contar con un sistema de gestión de tickets que permita registrar, clasificar, asignar y monitorear las alertas y hallazgos derivados de las herramientas de seguridad. La creación de tickets puede ser automática o manual, dependiendo del origen del hallazgo.

e) Las alertas deben estar vinculadas a flujos de respuesta específicos, permitiendo su priorización, asignación de responsables, trazabilidad de las acciones ejecutadas, y cierre documentado con base en evidencia técnica.

Subsección 4.01.5. Integración de inteligencia de amenazas en la detección

a) Deben implementarse mecanismos seguros para integrar fuentes de inteligencia de amenazas cibernéticas (como IoCs, TTPs, firmas de malware, campañas activas y perfiles de adversarios) en las tecnologías de detección de la organización, así como en los procedimientos y la capacitación del personal.

b) La información proveniente del inventario actualizado de activos tecnológicos debe ser proporcionada a las plataformas de detección, con el fin de correlacionar amenazas con sistemas críticos, dispositivos vulnerables y servicios expuestos.

c) Deben establecerse procesos automatizados o manuales para adquirir y analizar divulgaciones de vulnerabilidades provenientes del CSIRT Nacional del Centro Nacional de Ciberseguridad, proveedores de tecnología, fabricantes, CSIRTs sectoriales y organismos de seguridad cibernética, a fin de evaluar su impacto en la infraestructura institucional y activar acciones de mitigación cuando corresponda.

d) La integración de esta información debe permitir refinar las

reglas de detección, priorizar alertas y mejorar la eficacia de las herramientas de detección y escáneres de vulnerabilidades.

e) Los procesos de detección deben adaptarse de forma dinámica conforme se recibe nueva información sobre amenazas emergentes, configuraciones inseguras o debilidades en software y hardware institucional.

Subsección 4.01.6. Establecimiento de umbrales de monitoreo

a) Deben desarrollarse procesos para el análisis del historial de eventos, tales como registros de red, sistemas de autenticación, uso de aplicaciones y comportamiento de usuarios, con el propósito de identificar patrones normales y anomalías relevantes.

b) A partir de dicho análisis, deben establecerse umbrales técnicos y operacionales para métricas clave como volumen de tráfico, tasa de errores, número de intentos fallidos de autenticación, cambios en archivos críticos, conexiones remotas inusuales, entre otros.

c) Los umbrales definidos deben ser documentados y ajustados periódicamente, en respuesta a cambios en la infraestructura tecnológica, la criticidad de los activos, actualizaciones en los modelos de amenazas o comportamiento adaptativo del adversario.

d) Deben utilizarse soluciones tecnológicas que permitan la automatización de alertas en caso de que se superen los umbrales definidos, notificando de inmediato al CSIRT Nacional del Centro Nacional de Ciberseguridad, al personal interno o tercerizado de respuesta a incidentes, responsables de ciberseguridad u otros actores designados.

e) Se deben establecer canales de colaboración con otras instituciones y comunidades de ciberseguridad, como el

CSIRT Nacional del Centro Nacional de Ciberseguridad, para compartir umbrales efectivos, lecciones aprendidas y datos sobre comportamiento anómalo detectado en el ecosistema gubernamental.

Sección 4.02. Monitoreo continuo y correlación de eventos

Esta sección establece los requisitos para la supervisión constante de los activos tecnológicos. Detalla los controles para el monitoreo de redes, sistemas, actividad de personal y proveedores, así como la integración y correlación de los eventos de seguridad generados para identificar patrones de ataque y actividades maliciosas.

Subsección 4.02.1. Monitoreo de redes y servicios

a) Deben desplegarse herramientas especializadas de monitoreo de red, tales como sistemas de detección de intrusiones (IDS/IPS), sensores de tráfico, analizadores de flujo, o plataformas NDR (Network Detection and Response), que permitan inspeccionar el tráfico, identificar comportamientos inusuales y generar alertas.

b) Se debe establecer métricas clave que definan el comportamiento normal de la red, incluyendo volumen de tráfico, frecuencia de conexiones, tipos de protocolo utilizados, número de errores de autenticación o cambios de configuración no autorizados.

c) El tráfico de red debe ser analizado regularmente, tanto de forma automatizada como manual, para identificar indicadores de compromiso, movimientos laterales, actividades de comando y control (C2), exfiltración de datos, escaneo de puertos u otros patrones maliciosos.

d) Deben configurarse alertas automatizadas en las plataformas de monitoreo que notifiquen al personal de ciberseguridad en tiempo real cuando se detecten desviaciones significativas, patrones sospechosos o violaciones a las políticas de red establecidas.

e) Los Organismos deben implementar esquemas de supervisión continua que garanticen la cobertura de todas las redes y segmentos críticos, incluyendo conexiones internas, redes perimetrales, servicios de nube, VPNs y entornos OT, cuando corresponda.

f) El personal técnico debe estar capacitado para interpretar alertas y eventos, y aplicar procedimientos de contención, análisis o escalamiento, según los protocolos establecidos.

Subsección 4.02.2. Monitoreo de seguridad física

a) Deben desplegarse sistemas de vigilancia física, tales como cámaras de videovigilancia (CCTV), sensores de movimiento, controles de acceso biométrico, sensores de apertura y alarmas en puntos de entrada, de manera que se cubran todas las áreas clasificadas como críticas o sensibles.

b) Debe establecerse un sistema de monitoreo físico en tiempo real, operado por personal de seguridad institucional o mediante integración con un centro de control o monitoreo de seguridad centralizado.

c) Las soluciones implementadas deben permitir la configuración de alertas automatizadas ante eventos definidos como sospechosos (por ejemplo, accesos fuera de horario, intentos fallidos de ingreso, movimientos en áreas restringidas sin autorización).

d) Se debe contar con un procedimiento para el análisis de eventos registrados, que permita identificar patrones anómalos,

reconstruir incidentes, preservar evidencia y apoyar la respuesta ante eventos físicos no autorizados.

e) El acceso físico a salas de servidores, centros de datos, oficinas de alta confidencialidad y otros entornos críticos debe ser estrictamente controlado y limitado solo a personal autorizado, con registros de ingreso y egreso.

f) Deben establecerse mecanismos de integración entre el monitoreo físico y lógico, de modo que eventos físicos sospechosos puedan correlacionarse con eventos cibernéticos (por ejemplo, acceso físico a un servidor coincidiendo con intentos de intrusión en la red).

Subsección 4.02.3. Monitoreo de la actividad del personal

a) Debe establecerse perfiles base de comportamiento normal para los diferentes tipos de usuarios (por ejemplo: personal administrativo, técnicos, usuarios con privilegios, contratistas) a fin de identificar desviaciones relevantes que indiquen actividad maliciosa o negligente.

b) Se deben configurar alertas automatizadas que notifiquen al personal de ciberseguridad ante actividades atípicas, como accesos fuera del horario laboral, uso de credenciales en múltiples dispositivos simultáneamente, cambios no autorizados en configuraciones o intentos reiterados de acceso fallido.

c) Los Organismos deben implementar procedimientos de análisis de comportamiento de usuarios, a través de mecanismos automatizados o revisión periódica, para detectar señales tempranas de abuso de privilegios, movimientos laterales o preparación de ataques internos.

d) El acceso a los sistemas debe estar basado en roles y alineado al principio de menor privilegio, asegurando que cada colaborador cuente únicamente con los permisos estrictamente necesarios para desempeñar sus funciones.

a) Deben implementarse sistemas de monitoreo de acceso y actividad que registren e informen sobre las acciones realizadas por los proveedores externos dentro del entorno tecnológico del Organismo, incluyendo accesos remotos, modificaciones en sistemas, transferencia de archivos o uso de credenciales privilegiadas.

b) Se debe realizar auditorías de seguridad periódicas a los servicios prestados por terceros, incluyendo revisiones del cumplimiento de políticas, niveles de servicio y controles establecidos.

c) Los contratos establecidos con proveedores deben incluir cláusulas de ciberseguridad específicas, tales como requisitos de monitoreo, conservación de registros, obligaciones de reporte de incidentes, medidas de mitigación y derechos de auditoría por parte del Organismo.

d) Debe establecerse un procedimiento formal para responder a incidentes que involucren a proveedores externos, incluyendo la notificación oportuna, coordinación para la investigación y mitigación de impactos, y documentación de hallazgos.

e) Los Organismos deben verificar de manera periódica el cumplimiento de los acuerdos de seguridad por parte de los proveedores, mediante revisiones técnicas, evaluaciones de cumplimiento contractual o controles automatizados.

Subsección 4.02.5. Monitoreo de integridad de hardware y software

a) Deben implementarse soluciones detección y protección en todos los equipos de cómputo, servidores, dispositivos móviles y demás activos tecnológicos, asegurando su cobertura y efectividad mediante políticas de instalación obligatoria.

b) Se debe garantizar que las firmas de detección y bases de datos de amenazas estén actualizadas periódicamente, de forma automatizada, asegurando la protección frente a amenazas emergentes.

c) Se debe establecer capacidades de monitoreo del tráfico de red, especialmente salidas no autorizadas, conexiones sospechosas o comunicaciones asociadas con infraestructura maliciosa.

d) Debe aplicarse un esquema de inspección de archivos adjuntos y descargas, especialmente en los canales de correo electrónico, almacenamiento en la nube y plataformas de mensajería, mediante mecanismos automáticos de análisis en sandbox o motores heurísticos.

CAPÍTULO 5

GESTIÓN Y RESPUESTA A INCIDENTES

Este capítulo establece el marco formal para la gestión de incidentes, detallando los procesos para contener el impacto, erradicar la amenaza y restaurar las operaciones de manera coordinada y eficaz.

Sección 5.01. Proceso de gestión de incidentes

La eficacia de la respuesta a incidentes depende de un proceso estructurado y predefinido. Esta sección define los requisitos para el ciclo de vida de la gestión de incidentes, abarcando desde su categorización y priorización inicial hasta la selección de estrategias, el seguimiento y la escalada.

Subsección 5.01.1. Esquema de categorización de incidentes

a) Deben definirse categorías claras y específicas para la clasificación de incidentes en alineación con las directrices del CSIRT Nacional de Centro Nacional de Ciberseguridad, basadas en su naturaleza, origen, tipo de afectación, impacto operacional y nivel de criticidad de los activos comprometidos.

b) Los Organismos deben elaborar criterios objetivos y documentados para asignar incidentes a cada una de las

categorías definidas, considerando factores como la pérdida de confidencialidad, integridad o disponibilidad, el alcance del incidente, y el tiempo estimado de interrupción.

c) La categorización debe permitir la priorización eficiente de la respuesta y la asignación proporcional de recursos humanos, técnicos y logísticos en función del nivel de gravedad e impacto del incidente clasificado.

d) Deben establecerse mecanismos de comunicación formal para informar a los equipos de respuesta nacionales o sectoriales y partes interesadas sobre la categoría asignada a cada incidente y las acciones previstas según dicha clasificación.

e) Esta categorización debe integrarse a los procedimientos operativos estándar del plan de respuesta institucional y estar sujeta a revisiones periódicas en alineación con los criterios definidos por el CSIRT Nacional del Centro Nacional de Ciberseguridad, en función de la evolución de las amenazas y la experiencia adquirida en la gestión de incidentes.

f) Cuando un sistema maneje diferentes informaciones y/o preste diferentes servicios, el nivel de criticidad en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

Subsección 5.01.2. Priorización y selección de estrategias de respuesta

a) Deben establecerse criterios para priorizar la atención de incidentes en función de su alcance operativo, impacto potencial sobre servicios críticos, tiempo de exposición, y amenazas a la integridad o continuidad institucional.

b) La estrategia de respuesta seleccionada debe equilibrar la necesidad de contener y recuperar rápidamente los servicios

con la necesidad de preservar evidencia.

c) Los Organismos deben realizar análisis forense detallado cuando el contexto lo amerite de acuerdo con lo establecido en el marco legal vigente sobre ciberdelito.

d) Deben definirse procedimientos que guíen la selección de la estrategia de respuesta más efectiva frente a un incidente activo, en coordinación con los equipos técnicos, la MAE, con proveedores de servicios terceros, con el CSIRT nacional del Centro Nacional de Ciberseguridad, y con autoridades judiciales cuando el caso lo amerite.

e) La priorización y estrategia deben quedar documentadas en los registros del incidente como parte del proceso de gestión, y servir como insumo para la evaluación posterior de la respuesta realizada, en coordinación con la autoridad nacional de respuesta a incidentes.

Subsección 5.01.3. Seguimiento y escalada de incidentes

a) Debe implementarse un proceso para realizar seguimiento continuo al estado de todos los incidentes activos, verificando su progreso, acciones ejecutadas, responsables asignados y cumplimiento de los tiempos de respuesta establecidos en los procedimientos internos.

b) Los Organismos deben mantener registros actualizados del ciclo de vida del incidente, desde su detección hasta su resolución y cierre, utilizando sistemas de gestión de incidentes que permitan trazabilidad, control y auditoría.

c) En función de la evolución y gravedad del incidente, debe existir un protocolo para coordinar su escalada o elevación ante las partes interesadas previamente definidas, incluyendo dirección institucional, áreas críticas, organismos reguladores, CSIRT Nacional del Centro Nacional de Ciberseguridad u otros

terceros relevantes.

d) La escalada debe realizarse conforme a criterios previamente establecidos, que consideren el nivel de impacto, tiempo de interrupción, sensibilidad de la información comprometida, o indicios de actividad persistente o coordinada.

e) El proceso debe contemplar la asignación de responsables para la coordinación con cada parte interesada, y garantizar que la comunicación sea oportuna, precisa y con los niveles adecuados de clasificación y autorización.

Subsección 5.01.4. Criterios para la activación de la recuperación

a) Deben definirse criterios técnicos y operativos para la activación de la respuesta, los cuales deben basarse en las características del incidente detectado, su alcance, tiempo de exposición, impacto sobre los activos críticos, y la imposibilidad de contener el incidente sin interrumpir operaciones.

b) La evaluación de estos criterios debe realizarse en conjunto entre el equipo de respuesta a incidentes y el equipo de recuperación, considerando la naturaleza del ataque y los riesgos asociados a la ejecución temprana o tardía de las acciones de restauración.

c) En el proceso de decisión debe tenerse en cuenta si la ejecución de la respuesta puede provocar interrupciones operativas mayores, afectar la continuidad de servicios esenciales o comprometer la integridad de evidencias necesarias para análisis forense o investigaciones legales.

d) El proceso de activación debe documentarse formalmente, estableciendo quién toma la decisión, bajo qué criterios y en qué momento se hace efectiva la transición de la fase de respuesta a la de recuperación.

e) Una vez que se toma la decisión de activar la recuperación, se deben invocar los procedimientos y planes correspondientes

definidos en la **NORTIC A9 – Norma para la Gestión de Riesgos Tecnológicos y Continuidad Operativa.**

Sección 5.02. Análisis técnico y forense de incidentes

Esta sección establece los requisitos para la investigación técnica y el análisis forense, así como los procedimientos para la recolección, preservación y manejo de la evidencia digital.

Subsección 5.02.1. Análisis técnico de incidentes

a) Debe realizarse la asignación clara de responsabilidades, especificando quién es responsable de la validación inicial, la recopilación de evidencia, el análisis técnico y la elaboración del informe de hallazgos, incluyendo personal interno o proveedores de servicios gestionados.

b) Deben disponerse herramientas especializadas de análisis y respuesta de incidentes, incluyendo tecnologías para la correlación de eventos, soluciones de protección de puntos finales, plataformas de cacería de amenazas, y herramientas forenses digitales, para apoyar el trabajo de los equipos de respuesta.

c) Todos los pasos de la investigación y respuesta de incidentes deben ser documentados en registros estructurados, incluyendo los datos recopilados, las técnicas empleadas, el análisis de la causa raíz, las acciones tomadas, los errores identificados y las lecciones aprendidas.

Subsección 5.02.2. Capacidades y procedimientos de análisis forense

a) Debe contarse con recursos forenses internos capacitados o establecer acuerdos con externos especializados que

garanticen la capacidad de ejecutar análisis forense digital de forma oportuna y profesional.

b) La adquisición de evidencia debe realizarse aplicando técnicas forenses que aseguren su integridad, autenticidad y trazabilidad, utilizando métodos estandarizados y herramientas reconocidas internacionalmente.

c) Deben analizarse los artefactos digitales disponibles, tales como registros del sistema, archivos de memoria, discos duros, dispositivos móviles y flujos de red, con el propósito de reconstruir la cronología de los eventos, identificar vectores de ataque y delimitar la magnitud del compromiso.

d) Debe asegurarse la colaboración con las autoridades legales competentes y con las unidades jurídicas internas del Organismo para garantizar que los procedimientos de adquisición, análisis y custodia de evidencia se ajusten a los marcos legales aplicables y sean admisibles en instancias judiciales si fuese necesario.

e) Debe elaborarse un informe forense por cada incidente investigado, el cual debe contener los hallazgos técnicos, las acciones ejecutadas, las vulnerabilidades detectadas, las recomendaciones de mejora y, cuando corresponda, los elementos que apoyen la atribución o remediación.

Subsección 5.02.3. Preservación y manejo de evidencia digital

a) Deben recopilarse todos los datos pertinentes al incidente, incluyendo registros de eventos, capturas de tráfico, alertas de seguridad, configuraciones de sistemas, correos electrónicos, archivos afectados y cualquier otro dato relevante que permita reconstruir el incidente.

b) Deben preservarse los metadatos asociados a los datos recopilados, tales como el origen, la fecha y hora de recolección,

el custodio responsable y cualquier transformación o acceso posterior, siguiendo los principios de cadena de custodia.

c) Deben implementarse procedimientos técnicos y administrativos para proteger la integridad de los datos de incidentes y garantizar que no sean alterados, sobrescritos o eliminados de manera accidental o intencional durante el proceso de investigación.

d) Toda la información preservada debe estar disponible para análisis interno, apoyo a acciones correctivas, revisiones de cumplimiento normativo y, de ser requerido, como evidencia válida ante autoridades competentes o procesos judiciales.

e) Los procedimientos de preservación de evidencia deben estar alineados con buenas prácticas internacionales y contemplar el uso de herramientas especializadas de adquisición forense, almacenamiento seguro y documentación formal.

Subsección 5.02.4. Evaluación de daños y análisis de impacto post-incidente

a) Debe realizarse un análisis detallado del impacto del incidente sobre los sistemas de información, los datos institucionales, los procesos operativos, los servicios prestados y las funciones críticas, considerando tanto el grado de afectación como la duración del evento.

b) La evaluación de impacto debe ser comunicada de forma clara y oportuna a las partes interesadas internas pertinentes, incluyendo la dirección ejecutiva, el equipo de respuesta a incidentes, las unidades operativas afectadas y las instancias responsables de la continuidad institucional.

c) Deben identificarse, documentarse comunicarse a las autoridades internas y al CSIRT Nacional del Centro Nacional de Ciberseguridad las pérdidas reales y potenciales asociadas al incidente, incluyendo impactos financieros, deterioro de la imagen institucional, pérdida de confianza pública, sanciones

legales o interrupciones significativas de los servicios esenciales.

d) Deben evaluarse las consecuencias tanto a corto como a largo plazo, considerando la recuperación de sistemas, afectación de proyectos estratégicos, compromisos contractuales y riesgos de recurrencia si no se toman medidas correctivas efectivas.

e) Deben mantenerse registros detallados del proceso de evaluación del impacto, documentando los hallazgos, criterios utilizados, análisis realizados y las decisiones adoptadas como resultado de esta evaluación.

Sección 5.03. Notificación y comunicación de incidentes

Esta sección define los controles y protocolos para la notificación y comunicación con las partes interesadas internas y externas, incluyendo a las autoridades nacionales, conforme a las regulaciones vigentes.

Subsección 5.03.1. Notificación y comunicación interna y externa

a) Conforme al decreto 685-22 que establece la notificación de incidentes cibernéticos en la administración pública, los organismos gubernamentales deberán reportar sin demora los incidentes de ciberseguridad que les afecten, siguiendo las políticas y procedimientos de gestión de incidentes de su institución al CSIRT Nacional del Centro Nacional de Ciberseguridad (CNCS), al ente u órgano regulador sectorial competente o al CSIRT sectorial correspondiente. Deben comunicar el incidente dentro de las primeras veinticuatro (24) horas de haber sido detectado.

b) La notificación del incidente debe incluir toda la información necesaria para valorar su impacto institucional, sectorial o nacional, a fin de que se articulen desde el CSIRT Nacional del

Centro Nacional de Ciberseguridad o del CSIRT sectorial, según corresponda, las gestiones adecuadas tendientes a lograr la solución del incidente declarado.

c) Al margen de que el evento se haya subsanado o mitigado, debe ser comunicado, para alerta temprana a terceros y/o acciones de coordinación adicionales.

d) Los organismos gubernamentales deben realizar la notificación de incidentes al CSIRT-RD del Centro Nacional de Ciberseguridad a través del formulario web **https://cncs.gob.do/reportar-incidentes/** o a la dirección de correo electrónico **incidentes@csirt.gob.do**

e) Si un incidente cibernético constituye un delito, el organismo gubernamental debe reportarlo además al Ministerio Público y a la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de Investigaciones (DNI), conforme a lo establecido en la legislación vigente sobre ciberdelito.

f) Deben compartir la información relevante con las partes interesadas internas y externas designadas para garantizar una comunicación efectiva y oportuna.

g) Los responsables de seguridad de la información deberán cuidar que las medidas de mitigación y/o control del incidente no comprometan la evidencia o la información relevante para la investigación inmediata o a futuro de este.

h) Deben identificarse y documentarse todas las partes interesadas internas y externas que deben ser involucradas en los procesos de respuesta a incidentes, incluyendo unidades operativas, áreas legales, comunicaciones institucionales, reguladores, proveedores, clientes y otros terceros críticos.

i) Deben definirse canales formales de comunicación y coordinación, especificando protocolos, medios técnicos, frecuencia de actualizaciones y responsables designados para

cada tipo de parte interesada.

j) Deben desarrollarse y mantenerse actualizados los protocolos de coordinación que definan cómo debe intercambiarse la información, qué contenido debe comunicarse en cada fase del incidente, y cómo garantizar la colaboración sin comprometer la seguridad o la confidencialidad de los datos.

k) Debe promoverse la colaboración efectiva entre los distintos equipos internos y externos involucrados en la respuesta, asegurando que todos comprendan sus responsabilidades, niveles de autoridad y puntos de contacto para la ejecución coordinada de acciones.

l) Deben realizarse simulacros y ejercicios periódicos que incluyan a las partes interesadas, con el propósito de poner a prueba la coordinación real, validar los procedimientos establecidos y realizar ajustes necesarios para mejorar la eficiencia de la respuesta conjunta.

Subsección 5.03.2. Intercambio de información con partes externas autorizadas

a) Deben identificarse las partes interesadas externas relevantes con las que se requiere o se desea compartir información de ciberseguridad, incluyendo agencias gubernamentales, centros de respuesta a incidentes sectoriales, entidades reguladoras, organismos internacionales, socios estratégicos y miembros del ecosistema nacional de ciberseguridad.

b) Debe definirse con claridad qué tipos de información será compartida de forma voluntaria, en qué condiciones, con qué niveles de clasificación y cómo se estructurará la información para facilitar su uso y protección (por ejemplo, indicadores de compromiso, tácticas de adversarios, contexto del incidente, medidas adoptadas).

c) Deben implementarse mecanismos de comunicación seguros y confiables, que incluyan canales cifrados, protocolos formales de intercambio, registros de auditoría y verificación de identidad de las partes participantes.

d) El Organismo debe participar activamente en foros de intercambio de información de ciberseguridad a nivel sectorial, nacional o regional, aprovechando estas plataformas para fortalecer su capacidad de detección temprana, análisis de amenazas e implementación de respuestas coordinadas.

Sección 5.04. Contención y remediación de incidentes

Esta sección establece los controles y procedimientos para la contención inmediata del incidente, la mitigación de sus efectos y la remediación de las causas subyacentes.

Subsección 5.04.1. Medidas de contención y mitigación de amenazas

a) Deben establecerse mecanismos de respuesta rápida que permitan aplicar medidas de contención en cuanto se detecte un incidente, con el fin de limitar su alcance y evitar que se propague a otros sistemas o servicios críticos.

b) Deben aplicarse procedimientos para aislar los sistemas afectados, incluyendo el cierre de sesiones, la segmentación lógica o física y la revocación de credenciales comprometidas, con el objetivo de evitar la propagación de malware, accesos no autorizados o corrupción de datos.

c) Cuando corresponda, deben desconectarse de forma segura los recursos críticos o vulnerables de la red institucional, garantizando que no sean utilizados como vectores de ataque o medios de exfiltración de información.

d) Deben implementarse controles de red para bloquear o limitar el tráfico malicioso, empleando listas de control de acceso, filtrado de contenido, análisis de comportamiento y otras tecnologías que reduzcan el riesgo de comunicación entre sistemas comprometidos.

e) Debe reforzarse la arquitectura de seguridad perimetral y segmentar la red de manera que se limite la capacidad de las amenazas de moverse lateralmente entre los diferentes segmentos de infraestructura.

Subsección 5.04.2. Procedimientos de remediación y análisis de causa raíz

a) Debe realizarse un análisis técnico y contextual detallado que identifique la causa raíz del incidente, determinando con precisión las vulnerabilidades explotadas, los controles fallidos, los factores humanos o tecnológicos implicados y las brechas de procedimiento asociadas.

b) Deben desarrollarse y aplicarse de forma priorizada parches de seguridad, actualizaciones de software o soluciones correctivas que mitiguen los vectores de ataque utilizados, en coordinación con los equipos técnicos, proveedores y responsables de los sistemas afectados.

c) Deben implementarse mejoras en los procesos, procedimientos o flujos operativos relacionados con el incidente, con el propósito de cerrar brechas organizacionales, reducir errores recurrentes y fortalecer la postura preventiva del Organismo.

d) Deben reevaluarse los controles de seguridad relacionados con el incidente, verificando su idoneidad, cobertura y nivel de cumplimiento; y fortalecerse o rediseñarse aquellos que hayan demostrado ser insuficientes o inadecuados.

e) Los hallazgos sobre factores humanos en el incidente deben ser utilizados como insumo para actualizar y reforzar el programa de concienciación y capacitación en seguridad.

CAPÍTULO 6

SEGURIDAD EN LA RECUPERACIÓN

Este capítulo establece los controles de ciberseguridad obligatorios que deben implementarse durante la fase de recuperación de un incidente. Su objetivo es asegurar que la restauración de los servicios, dirigida por los planes definidos en la **NORTIC A9**, no reintroduzca amenazas y, a su vez, fortalezca la postura de seguridad del organismo.

Sección 6.01. Planificación de la recuperación segura

Esta sección establece los requisitos para integrar los controles de seguridad en los planes de recuperación y para definir los protocolos formales que validen la integridad de los activos de restauración antes de su uso, incluyendo:

a) Los planes de recuperación del organismo, definidos en la NORTIC A9, deben ser actualizados para incorporar puntos de control de seguridad específicos, derivados de las lecciones aprendidas de incidentes reales, auditorías y ejercicios de simulación.

b) Se debe establecer y documentar un protocolo formal para la validación de la integridad y seguridad de los activos de

restauración (tales como respaldos, imágenes de sistemas y archivos de configuración). Este protocolo debe ser un paso obligatorio dentro del plan de recuperación y ejecutarse antes de iniciar cualquier proceso de restauración.

c) El protocolo de validación de activos de restauración debe incluir, como mínimo, las siguientes actividades:

   (i) Una revisión exhaustiva de los activos de restauración en busca de indicadores de compromiso (IoCs), signos de corrupción, manipulaciones o cualquier anomalía que pueda comprometer la seguridad del proceso de recuperación.

   (ii) La ejecución de análisis mediante herramientas técnicas apropiadas, tales como escaneos de vulnerabilidades, análisis de programa maligno y validación de firmas de integridad de archivos (hashes).

   (iii) Según la criticidad del incidente y de los activos afectados, la realización de un análisis forense de los medios de respaldo para descartar la persistencia de la amenaza.

d) Cualquier activo de restauración que muestre signos de compromiso, manipulación o contenga programa maligno no debe ser utilizado para la recuperación de sistemas en producción. El plan debe definir un procedimiento de escalada para estos casos, que contemple, como mínimo:

   (i) La activación del protocolo para utilizar una copia de respaldo anterior y verificada como segura.

   (ii) O, en su defecto, proceder con la reconstrucción del sistema desde una fuente confiable, aplicando posteriormente la restauración de datos limpios.

Sección 6.02. Ejecución de la recuperación segura

Esta sección detalla los controles para la erradicación de artefactos maliciosos, la mitigación de la causa raíz del incidente, y el fortalecimiento (hardening) de los sistemas antes de su retorno a producción.

Subsección 6.02.1. Erradicación de la amenaza y mitigación de la causa raíz

a) Antes de que un sistema, aplicación o componente afectado por un incidente sea reconectado al entorno de producción, el organismo debe asegurarse de que todos los artefactos maliciosos (malware, puertas traseras, cuentas de usuario no autorizadas, etc.) han sido completamente erradicados.

b) El organismo debe identificar la causa raíz del incidente. Si esta corresponde a una vulnerabilidad técnica, debe aplicarse el parche de seguridad correspondiente o un control compensatorio validado antes del retorno a producción. La simple restauración del servicio sin remediar la vulnerabilidad subyacente está prohibida.

c) Debe realizarse un análisis para identificar si la misma vulnerabilidad o una similar existe en otros sistemas de la institución, y en caso afirmativo, se deben incluir en el plan de remediación.

Subsección 6.02.2. Fortalecimiento (Hardening) y configuración segura

a) Todos los sistemas que serán restaurados deben ser sometidos a una revisión de su configuración para asegurar que cumplen con las políticas de fortalecimiento (hardening) de la institución. Esto debe incluir la eliminación de servicios, puertos y cuentas de usuario innecesarias que no sean esenciales para la operación del sistema.

b) Las credenciales de acceso de todas las cuentas (usuarios y servicios) asociadas a los sistemas comprometidos deben ser revocadas y reemitidas de forma segura, incluyendo contraseñas, claves SSH, certificados digitales y tokens de acceso.

c) Se deben revisar y revalidar los permisos de acceso de los sistemas restaurados, asegurando que se aplique el principio de mínimo privilegio.

Subsección 6.02.3. Documentación de la remediación

a) a) Todas las acciones de remediación y fortalecimiento realizadas deben ser documentadas formalmente. Este registro debe incluir la vulnerabilidad identificada, la acción correctiva aplicada, la fecha de aplicación y el personal responsable.

b) b) Esta documentación debe formar parte del informe post-incidente y ser utilizada como insumo para actualizar los planes de respuesta y los procedimientos de configuración segura, en el marco del ciclo de mejora continua.

Sección 6.03. Verificación y cierre de la recuperación

Esta sección establece los requisitos para el proceso de verificación de seguridad formal, la autorización para el retorno a producción, el monitoreo intensificado post-recuperación y la documentación necesaria para el cierre del incidente y la mejora continua.

Subsección 6.03.1. Proceso de validación formal y retorno a producción

a) El organismo debe establecer un proceso formal de validación de seguridad que debe ser ejecutado antes de autorizar el retorno a producción de cualquier sistema recuperado de un incidente.

b) Esta validación debe ser realizada por personal del equipo de ciberseguridad o un tercero autorizado, distinto del equipo que realizó la restauración, para asegurar la independencia y objetividad de la prueba.

c) La validación debe incluir, como mínimo:

   (i) Pruebas técnicas para confirmar que las acciones de restauración y remediación fueron completas y correctas.

   (ii) Revisión de registros (logs) de los sistemas restaurados para detectar cualquier actividad anómala.

   (iii) Verificación de que el sistema cumple con la línea base de configuración segura (hardening) de la institución.

   (iv) Pruebas de funcionalidad en conjunto con los dueños del proceso de negocio para asegurar que el sistema opera como se espera.

d) No debe autorizarse el retorno a producción de ningún sistema hasta que la revisión de seguridad se haya completado satisfactoriamente. La decisión final debe ser documentada, indicando quién la tomó, la fecha y la evidencia que sustenta la decisión.

Subsección 6.03.2. Monitoreo post-implementación

a) Deben establecerse mecanismos de monitoreo intensificado sobre los sistemas recién reactivados por un período de tiempo definido (ej. 72 horas).

b) Este monitoreo intensificado debe enfocarse en detectar tempranamente desviaciones en el comportamiento, errores persistentes, actividad de red anómala o cualquier signo de reinfección.

a) Deben establecerse criterios objetivos para declarar el final del proceso de recuperación, tales como la restauración completa de los servicios y la validación de la integridad de los sistemas.

b) La declaración formal de cierre del incidente debe ser registrada y comunicada a las partes interesadas pertinentes, incluyendo la alta dirección y el CIGETIC.

c) Debe prepararse un informe post-incidente que documente detalladamente todo el ciclo de vida del evento, incluyendo las decisiones tomadas, las medidas implementadas y, fundamentalmente, las lecciones aprendidas.

d) El informe post-incidente y la declaración de cierre deben ser utilizados como insumos para actualizar y mejorar los planes de recuperación, los procedimientos de respuesta y los procesos de mejora continua institucional, conforme a lo establecido en la **NORTIC A7 – Norma para la Administración de la Seguridad de la Información.**

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. International Organization for Standardization. (2022). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.

4. International Organization for Standardization. (2022). ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls. ISO.

5. International Organization for Standardization. (2012). ISO/IEC 27032:2012 — Information technology — Security techniques — Guidelines for cybersecurity. ISO.

6. International Organization for Standardization. (2016). ISO/IEC 27035-1:2016 — Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management. ISO.

7. 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.

8. National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

ABREVIATURAS Y ACRÓNIMOS

No.	Abreviaturas y Acrónimos	Inglés	Español
1	APT	Advanced Persistent Threat	Amenaza Persistente Avanzada
2	BIA	Business Impact Analysis	Análisis de Impacto al Negocio
3	CCTV	Closed-Circuit Television	Circuito Cerrado de Televisión
4	CIGETIC	N/A	Comité de Implementación y Gestión de Estándares TIC
5	CIS	Center for Internet Security	Centro para la Seguridad de Internet
6	CNCS	N/A	Centro Nacional de Ciberseguridad
7	CSIRT	N/A	Equipo de Respuesta a Incidentes de Seguridad Informática
8	CVE	Common Vulnerabilities and Exposures	Vulnerabilidades y Exposiciones Comunes
9	DMZ	Demilitarized Zone	Zona Desmilitarizada
10	DoS/DDoS	Denial of Service / Distributed DoS	Denegación de Servicio / Denegación de Servicio Distribuida
11	IAM	IAM	Gestión de Identidad y Accesos
12	IDS	Intrusion Detection System	Sistema de Detección de Intrusos
13	IEC	International Electrotechnical Commission	Comisión Electrotécnica Internacional
14	IoC	Indicator of Compromise	Indicador de Compromiso
15	IPS	Intrusion Prevention System	Sistema de Prevención de Intrusos
16	ISO	International Organization for Standardization	Organización Internacional de Normalización
17	KPI/KRI	Key Performance/Risk Indicator	Indicador Clave de Desempeño/Riesgo
18	MFA	Multi-Factor Authentication	Autenticación Multifactor
19	NDR	Network Detection and Response	Detección y Respuesta de Red

CONT. ABREVIATURAS Y ACRÓNIMOS

20	NIST	National Institute of Standards and Technology	Instituto Nacional de Estándares y Tecnología
21	OGTIC	N/A	Oficina Gubernamental de Tecnologías de la Información y Comunicación
22	OT	Operational Technology	Tecnología Operacional
23	OWASP	Open Web Application Security Project	Proyecto Abierto de Seguridad de Aplicaciones Web
24	RPO	Recovery Point Objective	Objetivo de Punto de Recuperación
25	RTO	Recovery Time Objective	Objetivo de Tiempo de Recuperación
26	SDLC	Software Development Lifecycle	Ciclo de Vida de Desarrollo de Software
27	SIEM	Security Information and Event Management	Gestión de Información y Eventos de Seguridad
28	SOC	Security Operations Center	Centro de Operaciones de Seguridad
29	TIC	Information and Communication Technologies	Tecnologías de la Información y la Comunicación
30	TTP	Tactics, Techniques, and Procedures	Tácticas, Técnicas y Procedimientos
31	UEBA	User and Entity Behavior Analytics	Análisis de Comportamiento de Usuarios y Entidades
32	VLAN	Virtual Local Area Network	Red de Área Local Virtual
33	VPN	Virtual Private Network	Red Privada Virtual

ANEXOS

Anexo A: Tabla No.1 - Niveles de Criticidad de Incidentes de Seguridad

Nivel	Descripción General	Criterios de Clasificación
Crítico	Consecuencias que suponen un perjuicio muy grave o total para los objetivos de la organización, sus activos críticos o los individuos afectados	• Anulación en más del 90% de la capacidad organizacional para obligaciones fundamentales • Activos/sistemas utilizados por más de un servicio esencial del Estado • Interrupción del servicio superior a 8 horas • Daño muy grave e incluso irreparable de activos organizacionales • Daños reputacionales muy elevados con cobertura internacional • Afectación a la seguridad nacional y ciudadana • Incumplimiento de leyes o regulaciones
Alto	Consecuencias que suponen un perjuicio grave para los objetivos de la organización, sus activos críticos o los individuos afectados	• Anulación en más del 70% de la capacidad organizacional para obligaciones fundamentales • Interrupción del servicio superior a 1 hora • Daño grave de activos organizacionales • Daños reputacionales muy elevados con cobertura internacional • Perjuicio grave a individuos de difícil o imposible reparación • Incumplimiento de leyes o regulaciones
Medio	Consecuencias que suponen un perjuicio parcial sobre las funciones de la organización, sus activos o los individuos afectados	• Reducción parcial de más del 30% de la capacidad organizacional • Daño parcial de activos organizacionales (financieros, información, imagen) • Daño reputacional apreciable • Perjuicio moderado a individuos • Otros de naturaleza análoga
Bajo	Consecuencias que suponen un perjuicio mínimo o nulo sobre las funciones de la organización, sus activos o los individuos afectados	• Sin reducción de capacidad organizacional • Sin daño o daño mínimo de activos • Sin perjuicio a individuos • Funcionamiento normal de obligaciones corrientes

Anexo B: Tabla No. 2 - Ejemplo de Formato de Inventario de Activos

Nombre del Activo	**Servidor01**	**Firewall01**	**Aplicación CRM**
Descripción	Servidor de Base de Datos	Firewall principal de la red	Sistema de Gestión de Relación con Clientes
Ubicación	Data Center	Oficina Principal	Nube (AWS)
Propietario	Departamento de TI	Seguridad Informática	Ventas y Marketing
Valor	Muy alto	Alto	Muy alto
Fecha de Adquisición	01/01/2022	15/03/2021	20/07/2020
Estado	En uso	En uso	En uso
Configuración y Versiones	Producto 01	Producto 02	Producto 03
Dependencias	Red de almacenamiento, Sistema de respaldo	Conexión a Internet, VPN corporativa	Base de datos de clientes, Integración con ERP

Anexo C: Tabla No. 3 - 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