Presidencia de la República

OFICINA PRESIDENCIAL DE TECNOLOGÍAS
DE LA INFORMACIÓN Y COMUNICACIÓN

OPTIC

NORTIC A7 2016

GOBIERNO ELECTRÓNICO
REPÚBLICA DOMINICANA

NORMA PARA LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN EN EL ESTADO DOMINICANO

Santo Domingo, República Dominicana
Abril 2016

Presidencia de la República

OFICINA PRESIDENCIAL DE TECNOLOGÍAS
DE LA INFORMACIÓN Y COMUNICACIÓN

NORTIC A7 2016

NORMA PARA LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN EN EL ESTADO DOMINICANO

Santo Domingo, República Dominicana
Abril, 2016

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

Edición: 1era

Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC)
Departamento de Estandarización, Normativas y Auditoría Técnica

Fecha de aprobación: 22 de Enero de 2015
Fecha de lanzamiento: 15 de Abril de 2016

Categoría: A
Serie de documento: 7
Año de publicación: 2016
Versión 0.1.0

Diagramado y Diseñado por el Departamento de Multimedia, OPTIC
Impreso en República Dominicana

CONTENIDO

PRÓLOGO

La Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC), es el organismo del Estado Dominicano responsable de fomentar el uso de las Tecnologías de la Información y Comunicación (TIC), creado mediante el decreto No. 1090-04, en fecha 3 de septiembre de 2004, como dependencia directa del Poder Ejecutivo, con autonomía financiera, estructural y funcional, a fin de garantizar eficiencia, transparencia, servicios en línea y mecanismos para rendición de cuentas disponibles a favor de la ciudadanía.

Para el aseguramiento del correcto uso e implementación de las TIC en el Estado, la OPTIC elabora y establece las normas y estándares tecnológicos que impulsen el gobierno electrónico en el país.

Estas normas sobre TIC, denominadas NORTIC, son creadas desde el año 2013 por el departamento de Estandarización, Normativas y Auditoría Técnica, bajo el mandato del Ing. Armando García, director general de la OPTIC, y en el gobierno del Presidente de la República Dominicana, Lic. Danilo Medina.

Las NORTIC fueron concebidas para normalizar, estandarizar y tener una herramienta de auditoría para el efectivo uso e implementación de las TIC en la administración pública, con el fin de llegar a la completa homogeneidad y mejora de los procesos entre los organismos gubernamentales.

En este contexto, se han definido 5 categorías o tipos de NORTIC, según el alcance de estas, para ser difundidas e implementadas en toda la administración pública, como se presenta a continuación:

1. **Categoría A** (normas universales), para los aspectos normativos que aplican a todos los organismos gubernamentales.

2. **Categoría B** (normas para los departamentos de TIC), para aquellas normas necesarias y exclusivas a la efectiva gestión de los departamentos o áreas de TIC, dentro de los distintos organismos del Estado Dominicano.
3. **Categoría C** (normas municipales), para las normas que aplican a las iniciativas de TIC en los ayuntamientos o municipios.
4. **Categoría D** (normas para embajadas), para las normas que aplican únicamente a las iniciativas de TIC de las embajadas, consulados o misiones en el extranjero.
5. **Categoría E** (normas especiales), para las normas que aplican a organismos gubernamentales con características específicas dependiendo de sus funciones y estructura orgánica, así como para iniciativas, proyectos o programas de Gobierno, en el cual se haga uso de las TIC.

De modo, que esta Norma sobre Seguridad de las tecnologías de la información y comunicación en el Estado Dominicano, por tener un alcance universal, pertenece a la categoría A; mientras que por ser la séptima NORTIC elaborada en esta categoría, su denominación sería NORTIC A7:2016, siendo los últimos 4 dígitos los referidos al año de lanzamiento de esta norma.

En algunos casos, esta normativa puede presentarse de la forma siguiente: NORTIC A7-1:2016, seguida de trece caracteres (#####-##-######), donde el número "1" que aparece después del guion (-) especifica la serie del documento (1 para directrices, 2 para guías de implementación, 3 para código de buenas prácticas, entre otros) y los demás caracteres, el Número de Identificación Único (NIU) para cada organismo del Estado.

La evaluación de cada NORTIC es realizada por dos comités, la primera evaluación es ejecutada por el Comité Interno para Evaluación de las Normas (CIEN), el cual está conformado por expertos en TIC dentro de la OPTIC, mientras que la segunda evaluación es realizada por el Comité de Estándares de Tecnologías de la Información y Comunicación (COETIC), el cual está conformado por los responsables de TIC de cada organismo gubernamental, o a quienes la máxima autoridad de cada organismo designe.

En vista de la responsabilidad de la OPTIC en la elaboración de políticas, estrategias y controles de TIC y de los avances en el uso de las tecnologías, de los cuales los organismos gubernamentales no quedan al margen, surge esta normativa con las directrices para garantizar la seguridad de la información en las plataformas y los procesos tecnológicos que son implementados por los organismos.

MARCO LEGAL

La OPTIC, en su rol de entidad normalizadora sobre el uso e implementación de TIC en la administración pública, ha establecido las directrices por las cuales debe regirse todo organismo gubernamental del Estado Dominicano, tanto para aquellos que están físicamente dentro del país, como para los organismos que se encuentran fuera, como son las embajadas, consulados y misiones en el extranjero.

El marco legal que soporta esta norma está compuesto por las leyes y decretos presidenciales presentados a continuación:

1. El **Decreto 1090-04**, a través del cual se constituye la OPTIC como dependencia directa del poder ejecutivo, donde se establece lo siguiente:

    - **Artículo 3.-** Serán funciones de la Oficina Presidencial de Tecnologías de la Información y Comunicación, diseñar, proponer y definir las políticas, establecer los lineamientos y elaborar las estrategias, planes de acción y programas para promover, desarrollar y garantizar mayor acceso, conectividad e implantación de nuevas tecnologías de la información y comunicación, con el fin de fomentar su uso, como soporte del crecimiento económico y competitividad hacia la sociedad de la información, gestionando los proyectos conforme a tales directrices; y que garanticen el acceso equitativo a los mercados y al sector productivo como esfuerzo para la política de generación de empleo, para mejorar la calidad de vida, crear oportunidades de educación, trabajo, justicia, cultura y recreación, y otros.

- **Artículo 5.-** La Oficina Presidencial de Tecnologías de la Información y Comunicación será responsable de la formulación de políticas y la implementación del proceso de desarrollo e innovación tecnológica para la transformación y modernización del Estado hacia la sociedad de la información, promoviendo la integración de nuevas tecnologías, su compatibilidad, interoperabilidad y estandarización en materia de TIC.
- **Artículo 7.-** La Oficina Presidencial de Tecnologías de la Información y Comunicación podrá proponer políticas para difundir y promover la generación de una cultura de TIC en el país.
- **Artículo 9.-** La Oficina Presidencial de Tecnologías de la Información y Comunicación deberá velar, asistir y supervisar en los aspectos y políticas relativas a la seguridad y privacidad de la información digitalizada y electrónica en el ámbito del sector público.

2. Para el tratamiento de los derechos sobre la protección de datos personales, esta norma se ampara en la propia **Constitución de la República Dominicana** del 26 de enero de 2010.

- **Artículo 44.-** Derecho a la intimidad y el honor personal. Toda persona tiene derecho a la intimidad. Se garantiza el respeto y la no injerencia en la vida privada, familiar, el domicilio y la correspondencia del individuo. Se reconoce el derecho al honor, al buen nombre y a la propia imagen. Toda autoridad o particular que los viole está obligado a resarcirlos o repararlos conforme a la ley. Por tanto:
    - Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus

bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos.

- Se reconoce la inviolabilidad de la correspondencia, documentos o mensajes privados en formatos físico, digital, electrónico o de todo otro tipo. Sólo podrán ser ocupados, interceptados o registrados, por orden de una autoridad judicial competente, mediante procedimientos legales en la sustanciación de asuntos que se ventilen en la justicia y preservando el secreto de lo privado, que no guarde relación con el correspondiente proceso. Es inviolable el secreto de la comunicación telegráfica, telefónica, cablegráfica, electrónica, telemática o la establecida en otro medio, salvo las autorizaciones otorgadas por juez o autoridad competente, de conformidad con la ley.
- El manejo, uso o tratamiento de datos e informaciones de carácter oficial que recaben las autoridades encargadas de la prevención, persecución y castigo del crimen, sólo podrán ser tratados o comunicados a los registros públicos, a partir de que haya intervenido una apertura a juicio, de conformidad con la ley.

3. La **Ley 53-07** contra Crímenes y Delitos de Alta Tecnología.
   - **Artículo l.-** Objeto de la Ley. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de la información y comunicación, y su contenido, así como la prevención y sanción de los delitos cometidos contra estos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas física o morales, en los términos previstos en esta ley. La integridad de

los sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten a través de estos, las transacciones y acuerdos comerciales o de cualquier otra índole que se llevan a cabo por su medio y la confidencialidad de estos, son todos bienes jurídicos protegidos.

4. La **Ley No. 340-06** sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones, en donde se establecen los principios y normas generales que rigen la contratación pública, relacionada con los bienes, obras, servicios y concesiones del Estado.

5. La **Ley No. 126-02** sobre Comercio Electrónico, Documentos y Firma Digital.

6. La **Ley 65-00** sobre Derecho de Autor[1].

   - **Artículo 2.-** El derecho de autor comprende la protección de las obras literarias y artísticas, así como la forma literaria o artística de las obras científicas, incluyendo todas las creaciones del espíritu en los campos indicados, cualquiera que sea el modo o forma de expresión, divulgación, reproducción o comunicación, o el género, mérito o destino, incluyendo, pero no limitadas a:
     - Los programas de computadoras, en los mismos términos que las obras literarias, sean programas fuente o programas objeto, o por cualquier otra forma de expresión, incluidos la documentación técnica y los manuales de uso.
     - Las bases o compilaciones de datos u otros materiales, legibles por máquina o en cualquier otra forma, que por la selección o disposición de sus contenidos constituyan creaciones de carácter intelectual, pero no de los datos o materiales en sí mismos y sin perjuicio del derecho de autor existente sobre las obras que puedan ser objeto de la base o compilación.

[1] Es el conjunto de leyes y principios que provee protección a los autores, artistas y demás creadores para sus creaciones.

7. El **Decreto No. 229-07**, el cual es el instructivo de aplicación de Gobierno Electrónico, contentivo de las pautas generales para el desarrollo de la Estrategia de Gobierno Electrónico en la República Dominicana.

8. El **Decreto No. 709-07** sobre las normas y estándares elaboradas por la OPTIC.

    - **Artículo 1.-** Se instruye a toda administración pública del Estado Dominicano a cumplir con las normas y los estándares tecnológicos para: (i) el desarrollo de portales gubernamentales, (ii) conectividad interinstitucional, (iii) interoperabilidad tecnológica, (iv) de seguridad, auditoría e integridad electrónica, (v) digitalización de documentos; así como cualquier otra normativa que sea redactada, aprobada y coordinada por la Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC), en materia de tecnología de la información y la comunicación (TIC) y Gobierno Electrónico.

9. El **Decreto No. 615-07**, que Instruye a la OPTIC a coordinar el procedimiento para la elaboración de los inventarios[2] respecto a los programas incorporados a las computadoras y su licenciamiento.

10. La **Resolución Número 51-2013**, que aprueba los modelos de estructura organizativa permitidos para las unidades de TIC de todos los organismos del sector público.

[2] Es un registro organizado de los activos pertenecientes o bajo la responsabilidad de un organismo determinado.

INTRODUCCIÓN

La Norma para la Seguridad de las Tecnologías de la Información y Comunicación en el Estado Dominicano, establece las directrices que debe seguir cada organismo para la correcta implementación de la seguridad y continuidad de la misma, con el objetivo de salvaguardar y proteger los activos del organismo en una sociedad de la información que se encuentra en continua expansión.

Esta norma también conocida como NORTIC A7, indica desde el primer capítulo su alcance, el cual comprende todos los organismos gubernamentales de manera obligatorio. Además, se establecen las directrices que deben cumplir respecto al marco regulatorio, estructura organizativa y el desarrollo de las competencias, los cuales les permiten a cada organismo construir las bases para la implementación de la seguridad.

El capítulo II sobre Sistema para la Administración de la Seguridad de la Información, establece todas las pautas necesarias para la correcta implementación de los sistemas de seguridad que administran la información sensible del organismo, así como también, las políticas para la gestión, tratamiento y respaldo de la misma. Además por la importancia que representa la información para cualquier organismo, se ha agregado en la norma una sección para abordar los temas sobre el borrado seguro y recuperación de la información, de manera que se puedan evitar, o disminuir a un menor grado, las posibilidades de perder informaciones necesarias, permitiéndole a los organismos contar con procesos establecidos para estos casos.

El siguiente capítulo sobre la Administración de los Controles de Accesos, establece las directrices que apoyan los marcos regulatorios de acceso a los sistemas e instalaciones del organismo, garantizando que las informaciones sensitivas, contenidas en dichos medios, no

sean filtradas o manipuladas por personal no autorizado, todo esto regulado mediante la implementación de políticas para el acceso a la red, acceso a los sistemas que soportan las operaciones del organismo, y las políticas para la regulación de los accesos de los usuarios[3].

El capítulo IV, aborda los planes de disponibilidad y continuidad estableciendo las metodologías y procedimientos necesarios para mantener las operaciones del organismo a un nivel esperado, el cual mantenga su funcionamiento ante cualquier eventualidad o situación de interrupción en los servicios; ya sea esta por fallas propias en la infraestructura o por fenómenos naturales.

El capítulo V, Sobre la Gestión de Riesgo[4] establece un enfoque estructurado para la identificación y observación del riesgo a través de estrategias de desarrollo utilizando recursos gerenciales, abordando las directrices necesarias para el análisis, evaluación, tratamiento y entregables de la gestión del riesgo, así como también los lineamientos a seguir para elaborar un plan de acción efectivo que le permita al organismo cumplir con los objetivos y metas propuestos.

El capítulo final, sobre control de operaciones presenta de manera detallada las directrices para la correcta implementación de la seguridad web, especificando los controles de seguridad que deben seguir los manejadores de contenido, aplicaciones web y el uso, así como también las directrices sobre el uso de servicios wireless, dispositivos móviles y servicios en la nube.

[3] Hace referencia a la persona que consume o manipula un producto, servicio o información.

[4] La gestión de riesgos es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales.

CAPÍTULO I

NORMA PARA LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN EN EL ESTADO DOMINICANO

Esta norma indica las directrices que debe seguir cada organismo del Gobierno Dominicano para la gestión e implementación de la seguridad de la información en el Estado, con el objetivo de prevenir y manejar eficientemente los temas concernientes a todo lo relacionado con la gestión de la seguridad por parte de la administración pública y de esta manera, minimizar todos los riesgos que se puedan presentar.

SECCIÓN 1.01. Alcance

Las directrices de esta norma deben ser aplicadas por todos los organismos pertenecientes al Poder Ejecutivo, ya sean centralizados, descentralizados, o embajadas, consulados, misiones en el extranjero y municipios.

Entre los organismos centralizados se encuentran los Ministerios y sus dependencias, así como los organismos con nivel de ministerios, 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.

Entre los organismos descentralizados se encuentran las instituciones financieras y las no financieras, organismos reguladores, instituciones de la seguridad social y empresas públicas.

Los organismos pertenecientes al Poder Legislativo, y al Poder Judicial, así como aquellos organismos que entran dentro de la clasificación de "Organismos Especiales", según el Ministerio de Administración Pública (MAP), también pueden implementar los estándares indicados en esta norma como un modelo de buenas prácticas.

SECCIÓN 1.02. Referencias Normativas

Para la elaboración de esta norma se tomó como base la normativa elaborada por la OPTIC en el año 2014, sobre Seguridad de las Tecnologías de la Información y Comunicación (NORTIC A1). La estructura de la NORTIC A7:2016 engloba en sus capítulos los puntos concernientes a la seguridad de las TIC tratados en dicha normativa, respondiendo a los nuevos requerimientos técnicos de estos tiempos, por lo que esta normativa deroga los capítulos mencionados en la NORTIC A1:2014.

En la normativa, también se hace referencia al conjunto de estándares ISO 27018, de la Organización Internacional de Normalización (ISO, por sus siglas en inglés) sobre seguridad en la nube. De la misma manera se utilizó la norma ISO 27001, la cual especifica el estándar para la seguridad de la información. También se utilizó la ISO 27002, la cual especifica controles a seguir sobre la seguridad de la información.

SECCIÓN 1.03. Términos y definiciones

Para fines de esta norma el término "Organismo gubernamentales" será utilizado en ciertos casos como "Organismo".

Cuando se haga mención del "sistema para la administración de la seguridad de la información", este será sustituido por sus siglas "SASI". De igual manera, cuando se haga referencia al "Comité de Continuidad", este será sustituido por el acrónimo "CONTI".

Cuando en la normativa aparezca el término "Activos", este se refiere tanto a los activos físicos como los activos de información.

SECCIÓN 1.04. Marco regulatorio, legal y contractual de la organización

(a) Los organismos deben identificar y documentar de manera formal, mediante un documento escrito y de carácter oficial dentro de la organización, una relación de todos los aspectos legales y contractuales siguientes:

- Misión del organismo y su creación.
- Leyes que debe cumplir, en caso de que exista algún marco legal particular a esta organización.
- Compromisos contractuales que existen con otras organizaciones, tanto del Estado dominicano como con otras entidades de carácter privado o internacionales.

(i) Esta documentación debe estar aprobada por la máxima autoridad del organismo.

(b) En los casos en que la organización tenga acuerdos que deba cumplir por pertenecer a un sector especializado, estos deben estar claramente identificados y establecer el nivel de cumplimiento o compromiso que existe.

Algunos ejemplos de los que son sector especializado, pueden ser los siguientes: Salud, estadísticas nacionales y la milicia.

(i) En caso de que no exista un aspecto legal que obligue cierto nivel de cumplimiento, pero que, si hay expectativas de desempeño de otras organizaciones, estatales o no, y que dependen de los entregables de esta organización, la misma debe ser también establecida en dicha documentación.

SECCIÓN 1.05. Estructura organizativa

(a) Los organismos deben designar los roles y responsabilidades al personal interno correspondiente para los fines de la gestión de la seguridad de información.

(i) Los roles deben estar alineados a la estructura organizativa de las unidades de TIC, elaborado por el MAP.

(ii) Los roles deben estar claramente definidos y las personas a las cuales se le asigna esta responsabilidad deben tener la suficiente información documentada de la descripción de puesto, expectativas y responsabilidades de su rol.

(b) La organización debe evaluar la pertinencia del organigrama propuesto por el Ministerio de Administración Pública en conjunto con la OPTIC en cuanto a los esquemas propuestos para gestión del personal, la designación de roles y responsabilidades.

(c) El organismo debe evaluar como incluir en su estructura actual, según recomienda lineamiento del MAP, la función del rol de Oficial en Jefe de Seguridad de Información (CISO, por sus siglas en inglés), que es un ejecutivo de alto nivel quien está encargado de liderar todos los esfuerzos e iniciativas de seguridad de información.

SECCIÓN 1.06. Desarrollo de competencias

(a) Los organismos gubernamentales deben planificar y ejecutar un plan de desarrollo de capacidades de sus empleados de acuerdo a las responsabilidades asignadas en labores relacionadas con TIC y seguridad de información.

(b) Dependiendo del tamaño de la organización, perfil de riesgo y sensibilidad de la información que maneja el organismo, debe crearse un plan de capacitación en el desarrollo de competencias de Seguridad de la Información para un mínimo de dos personas.

(c) El logro de las competencias debe evaluarse mediante certificaciones profesionales del área de capacitación asociada al rol que desempeña el personal dentro del área de Seguridad de Información como requisito de la posición.

(d) Los participantes de estos entrenamientos deben asumir un compromiso formal de presentar el examen aprobado y obtener la certificación según satisfaga los requerimientos de experiencia que presenta la certificación.

(e) La alta dirección debe apoyar los planes de capacitación desarrollados o propuestos por el organismo mediante la

asignación de recursos oportunos para la formación, tanto en fondos como en tiempo disponible para los mismos.

(f) Debe crearse un Plan de Capacitación con énfasis en la Seguridad de Información, en particular basado en normativas internacionales de implementación de un Sistema de Gestión de Seguridad de Información, para el rol de Implementador para capacitar a los individuos en esta competencia ya que para esta existen capacitaciones formales que pueden ayudar en la implementación de la NORTIC.

(g) El organismo gubernamental debe asegurar que cada uno de los empleados tenga total conocimiento de las directrices establecidas en esta sección mediante la implementación de un programa de concienciación de seguridad de la información, así como las políticas de seguridad de la información propias del organismo. Ver **Sub-sección 4.02.4 Conciencia y capacitación del plan de continuidad.**

(h) El área de Recursos Humanos debe llevar un registro de todos los participantes en las sesiones de concienciación, así como un documento de aceptación por parte de los empleados y proveedores que tienen acceso a los activos de información del organismo.

(i) La gestión de riesgo de seguridad de información debe ser vista no solo como una función puntual sino como un proceso permanente dentro de la práctica de gestión del riesgo general del organismo.

(j) Los organismos deben elaborar actividades que tiendan tanto a hacer conciencia de la importancia de desarrollar una actitud proactiva en cuanto a la Gestión de Riesgo, sino también en cuanto al desarrollo de la especialización particular de Gestión de Riesgo de Seguridad de Información.

(k) Debe desarrollarse por medio de entrenamiento, el desarrollo de las tareas pertinentes para adquirir las habilidades, así como la obtención del personal de gestión riesgo en alguna de las certificaciones asociadas con Gestión de Riesgo.

(l) Deben tomarse en cuenta los diferentes tipos de análisis de riesgo los cuales se detallan en el **anexo A. Tipos de análisis de riesgos.**

CAPÍTULO II

ADMINISTRACIÓN Y TRATAMIENTO DE LA INFORMACIÓN

La información debe ser considerada como cualquier otro activo, es un elemento que tiene valor para el organismo, y por lo tanto debe ser protegida al igual que otros activos identificados por el organismo.

Este capítulo aborda las pautas para la implementación de un sistema de administración de seguridad, así como también establece políticas para la para la administración de la información y el tratamiento que se le dará a la misma.

SECCIÓN 2.01. Implementación del sistema

(a) Los organismos gubernamentales deben implementar un Sistema para la Administración de la Seguridad de la Información (SASI).

(i) El SASI debe contemplar las siguientes informaciones dentro de su elaboración:

- **Documento de definición y alcance del SASI:** Este debe establecer el alcance, objetivos y las responsabilidades del SASI.
- **Colección de documentos legales y contractuales:** Esta es la sumatoria de todos los compromiso u obligaciones que rigen la operación de los sistemas de información del organismo.
- **Manual de procedimientos:** Este debe establecer los documentos operativos que aseguran el debido funcionamiento del SASI.

- **Manual de instrucciones, lista de tareas y formularios:** Estos documentos deben establecer las actividades del nivel operativo para la correcta realización de las actividades del SASI.

La implementación de un SASI debe asegurar:

- *Que los activos de información estén dentro de un marco de seguridad.*
- *Que las informaciones estén disponibles.*
- *Que los datos estén íntegros.*
- *Que la infraestructura tecnológica que alberga el activo de información esté segura.*
- *Que estén establecidas las medidas y controles necesarios para mitigar riesgos que expongan los activos de información.*
- *Que se cumplen los compromisos legales y responsabilidades con las entidades relacionadas con el servicio que presta el organismo.*
- *Para ver las fases de implementación del SASI, ver* **Anexo B. Implementación del Sistema para la Administración de la Seguridad de la Información (SASI).**

- **Registros:** Estos documentos deben mantener evidencias de las acciones realizadas, según el SASI.

(ii) El SASI debe estar orientado a procesos, y el mismo debe tener la estructura de entradas, procesos y salidas. Los procesos para implementación de un SASI deben seguir las directrices a continuación:

a) El SASI debe contemplar las siguientes actividades para la elaboración e implementación del sistema:

i) Implicación de la máxima autoridad del organismo en el proceso de elaboración.

ii) Definición del alcance del SASI y políticas de seguridad.

iii) Identificación de amenazas[5], vulnerabilidades[6], probabilidad de ocurrencia e impactos.

iv) Definición y selección de controles para el tratamiento de riesgos.

[5] Es un evento que puede provocar un daño o perjuicio al organismo.

[6] Hace referencia a la incapacidad de defensa frente a una amenaza.

v) Aprobación por parte de la máxima autoridadtanto para la aceptación del riesgo como para el riesgo residual[7].

vi) Elaboración del documento de declaración de aplicabilidad[8].

vii) Implementación de controles, documentación de políticas, procedimientos e instrucciones de trabajo del SASI.

viii) Definición de los indicadores para la medición de la efectividad de los controles.

ix) Formación y concienciación, en lo relativo a seguridad de la información, a todo el personal del organismo gubernamental.

x) Monitoreo y registro de todas las incidencias.

xi) Monitoreo del SASI y mejora continua.

xii) Evaluación periódica de los riesgos, revisión de los niveles de riesgos residuales identificados para el SASI, así como su alcance.

xiii) Mejora continua del SASI.

(b) Los organismos gubernamentales deben hacer una revisión del SASI una (1) vez al año, o cuando se experimente algún cambio importante en la forma de operar del organismo o cambien el contexto interno y externo en el que opera el organismo.

SECCIÓN 2.02. Políticas para la administración de la información

Esta sección presenta las directrices sobre las políticas que debe cumplir el personal sobre el manejo de la información que está a su cargo.

[7] Hace referencia al riesgo que queda luego de haber tomado todas las medidas preventivas de reducción de riesgos.

[8] Hace referencia al documento que establece cuáles controles se aplicarán al organismo gubernamental en la implementación del SASI.

Sub-sección 2.02.1. Responsabilidad del empleado

(a) Los empleados de los organismos gubernamentales deben cumplir con las siguientes responsabilidades:

- **(i)** El empleado público debe velar porque otras personas no accedan a su estación de trabajo.
- **(ii)** El empleado público no debe dejar su estación de trabajo desatendida sin antes bloquearla.
- **(iii)** El empleado público debe velar por la integridad de sus equipos asignados y reportar al departamento de TIC cualquier irregularidad con los mismos.
- **(iv)** El empleado público no debe divulgar las credenciales que utiliza dentro del organismo gubernamental.
- **(v)** El empleado público no debe divulgar información confidencial a otro personal no autorizado para circular con dicha información.

(b) Recursos Humanos debe requerir de todo el personal la firma de un documento de entendimiento y compromiso y cumplimiento con todos los lineamientos de seguridad de información.

(c) Debe crearse un sistema de consecuencias de acuerdo a los lineamientos del MAP para aquellos casos en que se determine responsabilidad en el incumplimiento de las responsabilidades en cuanto al manejo de la seguridad de información, y de ser necesario escalarlo a la autoridad correspondiente cuando se determinen indicios de intencionalidad que sean referenciados en la ley.

Sub-sección 2.02.2. Divulgación de la información

(a) Toda solicitud de información requeridas al organismo por parte de la ciudadanía debe canalizarse a través de la oficina de libre acceso a la información pública.

(b) Ningún empleado debe compartir información fuera de los canales establecidos por la ley 200-04 sobre libre acceso a la información pública, o por otros lineamientos que podrían categorizar ciertas informaciones como reservadas o áreas protegidas, o de un carácter de seguridad Nacional.

(c) Los empleados deben estar entrenados para que no divulguen información de manera accidental o mediante técnicas de ingeniería social.

Sub-sección 2.02.3. Política de retención de la información

Para la retención de información debe especificarse la cantidad de tiempo que debe preservarse, antes que la misma se sobre escriba o se destruya de manera definitiva:

(a) El organismo debe desarrollar políticas de retención de la información de acuerdo con los requerimientos legales a los cuales debe cumplir cada organismo.

(b) Los organismos deben implementar los controles tecnológicos y no tecnológicos necesarios para poder cumplir con la política de retención de la información.

SECCIÓN 2.03. Tratamiento seguro de la información

Esta sección indica las directrices necesarias para lograr el correcto tratamiento de la información basada en políticas para la administración del activo de información, su correcto almacenamiento dependiendo el tipo de información y los procedimientos que deben ejecutarse cuando exista inconvenientes con el activo de información.

Sub-sección 2.03.1. Clasificación de la información

(a) Toda información de los organismos gubernamentales debe estar debidamente categorizada dentro de los parámetros siguientes:

- **Información pública:** Esta información debe estar al alcance, tanto de los empleados del organismo gubernamental como del público externo.
- **Información valiosa:** Esta información se utiliza para las operaciones del organismo gubernamental y debe estar solo al alcance de los sus empleados.
- **Información sensitiva:** Esta información debe estar solo al alcance de personas autorizadas. Esta puede afectar un personal o departamento dentro del organismo gubernamental.
- **Información confidencial:** Esta información debe estar permitida para un personal autorizado. Este personal debe estar designado por la máxima autoridad del organismo gubernamental o áreas designadas para otorgar dichos permisos. Esta puede afectar los intereses del organismo gubernamental.

Esta categorización no entra en oposición con lo establecido con la Ley de Libre Acceso a la Información, sino que solo establece los lineamientos para el manejo interno y en ninguna manera limita el alcance de la ley que está por encima de esta normativa.

(b) Toda información generada debe reflejar el nivel de categorización que amerite a excepción de la información pública, que será especificada por la ausencia de etiquetado. Esto incluye documentos en papel, electrónicos, conversaciones telefónicas, correos, entre otros.

(c) Los organismos gubernamentales deben tener un sitio de almacenamiento especial para las informaciones sensitivas o confidenciales.

(i) El sitio de almacenamiento debe disponer de una ruta, la cual pueda ser accedida única y exclusivamente por el personal autorizado.

(ii) Todo intento de acceso a los recursos en esta ruta debe ser registrados y auditados, no solo en la frecuencia sino en la cantidad de accesos realizados por cualquier usuario.

(iii) Los intentos no autorizados deben generar alertas inmediatas y dar inicio a un proceso de investigación de los intentos.

(iv) Cuando un usuario autorizado acceda una cantidad de recursos, ya sea en el período de un día, una semana o un mes, esto debe iniciar un proceso de investigación.

a) Cada organismo debe determinar cuáles son las cantidades de acceso que pueden ser considerados normales y a partir de que cantidad deben generarse alertas de seguridad.

(d) Los medios de almacenamiento que albergan información clasificada deben estar cifrados y seguir las directrices relacionadas con las contraseñas seguras que se establecen en la **directriz 2.03.1.a.**

(e) Los organismos gubernamentales no deben permitir la divulgación ni replicación de informaciones clasificadas a terceros o personas no autorizadas, ya sea por vía electrónica o física.

(f) Los organismos gubernamentales deben tener los medios adecuados para poner a disposición su información pública y valiosa.

(i) Los medios mínimos requeridos son:

a) **Medios web**[9]: Para informaciones públicas dirigidas al ciudadano sobre el organismo gubernamental. Ver **NORTIC A2:2016, Norma para la Creación y Administración de Portales Web del Gobierno Dominicano.**

b) **Intranet**[10]: Para información exclusiva de los empleados del organismo gubernamental.

[9] Es un conjunto de páginas electrónicas que presentan información y recursos de interés al usuario.

[10] Es una red interna para compartir de forma segura cualquier información o aplicación y evitar que cualquier usuario de Internet pueda ingresar a la red.

c) **Correo electrónico**[11]: Para informaciones con carácter importante o urgente a los empleados del organismo. Ver la **NORTIC A1:2014, sub-sección 7.04.3 Correo institucional.**

Para tener más información sobre los portales web Gubernamentales, Ver NORTIC A1:2014 Norma General sobre uso e Implementación de las Tecnologías de la Información y Comunicación en el Estado Dominicano.

(g) Las áreas o departamentos que manipulen información clasificada, deben tener independencia de recursos como impresoras, escáner, trituradoras de papel y archiveros.

(h) Toda información clasificada debe tener una frecuencia de respaldo superior a las informaciones no clasificadas.

(i) Los organismos deben hacer revisiones periódicas para adecuar los niveles de clasificación de la información a la nueva realidad que aplique según el tiempo dentro del ciclo de vida la misma.

(j) Debido a la diversidad de la información envuelta en un proceso de respaldo, los medios de almacenamiento y la información contenida deben ser clasificadas con el nivel Confidencial según se especifica en la **sub-sección 2.03.1 Clasificación de la información.**

Sub-sección 2.03.2. Almacenamiento de la información

(a) Los organismos gubernamentales deben definir políticas para los siguientes tipos de almacenamiento de la información:

(i) Almacenamiento local: Debe llevarse a cabo en las estaciones de trabajo de cada empleado del organismo gubernamental y cumplir con las siguientes directrices:

a) Debe estar definido qué clase de información estará almacenada, según su clasificación. Ver **sub-sección 2.03.1 Clasificación de la información.**

[11] Es un servicio de mensajería en red que permite el intercambio de mensajes, a través de sistemas de comunicación electrónicos.

i) Las informaciones de relevancia o alto impacto que residan en el almacenamiento local con un permiso temporal, deben ser eliminadas de forma segura al terminar con su utilización.

ii) En caso de que la información sea de relevancia o alto impacto, la información debe estar cifrada.

(b) Debe estar definido en qué ubicación del árbol de directorios del sistema operativo[12] estará residiendo la información.

(i) A la hora de almacenar información en los servidores de archivo y almacenamiento debe cumplirse con las siguientes directrices:

a) Solo deben almacenarse datos relacionados con el organismo.

b) No debe almacenarse ningún tipo de contenido que esté protegido por las leyes de derecho de autor, propiedad intelectual.

c) Los derechos asignados al usuario son de carácter individual y no deben ser compartidos con otras personas.

d) Debe llevarse registros de los accesos a los archivos, exitosos o no, así como las modificaciones que el usuario intente o logre realizar.

e) Cada usuario es responsable de las acciones que se registres con su identidad en los servidores de archivo.

f) Los servidores de archivo deben poder discriminar y generar alertas cuando se almacenen materiales como fotos, videos o cualquier otro criterio que el organismo considere de importancia monitorear.

(ii) Servidores de almacenamiento en red: Este es el almacenamiento debe estar localizado en un servidor especial para los fines de almacenamiento, y cumplir con las siguientes directrices:

a) Deben estar configurados para poner a disponibilidad del empleado autorizado cualquier documento o información del organismo gubernamental.

[12] Conjunto de órdenes y programas que controlan los procesos básicos de una computadora y permiten el funcionamiento de otros programas.

b) Toda información alojada en los servidores[13], debe estar regida por las políticas definidas en la sección 2.02 Políticas para la administración de la información.

c) Deben permitir al empleado disponer de carpetas personales para el desarrollo de sus funciones.

d) Deben permitir compartir los contenidos creados por el propio empleado.

e) Deben tener los accesos definidos para cada empleado.

f) No deben ser utilizados para el almacenamiento de contenido personal.

i) No deben contener archivos de audio o video sin relación con el organismo.

ii) No deben contener archivos de información personal del empleado.

iii) No deben contener software[14] no licenciados. Ver la **NORTIC A1:2014, sub-sección 1.05.2. Licenciamiento.**

g) Los servidores de almacenamiento en red deben tener cuotas de almacenamiento por empleado.

Sub-sección 2.03.3. Respaldo de la información

Por la naturaleza y alcance de la información generada por los organismos, los procesos de respaldo y restauración de la información son, quizás, los activos más importantes luego de la vida humana. De no disponer de los medios administrativos, procedimientos y recursos técnicos adecuados podría ser imposible llevar a cabo un proceso de continuidad exitoso.

[13] Son equipos informáticos que forman parte de una red de datos y que proveen servicios a otros equipos en dicha red, llamados clientes.

[14] Se conoce como software al equipo lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

(a) Los organismos gubernamentales deben tener políticas, procedimientos y recursos tecnológicos para los sistemas de respaldo de la información.

(i) Los organismos gubernamentales deben definir cuáles informaciones serán incluidas en el respaldo.

a) Las informaciones vitales para el correcto funcionamiento de los organismos deben ser incluidas dentro del programa de respaldo.

(ii) Los organismos gubernamentales deben disponer de un espacio físico y seguro para el almacenamiento de los respaldos.

a) Solo el personal autorizado podrá acceder y manipular los respaldos.

Como información se entiende que son tanto los datos de las aplicaciones, los sistemas operativos, datos de configuración de equipos, aplicaciones, servicios.

(iii) Los organismos gubernamentales deben asegurar que los datos respaldados están íntegros y libres de errores para su posterior uso.

a) Debe probarse periódicamente y aleatoriamente los respaldos realizados para garantizar su integridad.

(iv) Los organismos gubernamentales deben definir la vigencia que tendrá cada respaldo realizado.

(v) Debe realizarse una frecuencia de respaldos semanal, mensual y anual de todos los datos identificados como críticos para el organismo.

(b) Los organismos deben presentar información verificable del cumplimiento y nivel de éxito de este proceso.

(c) Los organismos deben hacer el aprovisionamiento necesario de medios de almacenamiento para poder cumplir con las demás directivas antes expuestas.

Apartado 2.03.3.1 Almacenamiento fuera de sitio

(a) Debe mantener una copia fiel de la información respaldada en una localidad física diferente, fuera de las facilidades inmediatas donde se realiza el respaldo.

- **(i)** Esta localidad alternativa debe tener los controles de protección necesarios para que la información guardada no sea dañada tanto por factores ambientales, operacional o mal uso.
- **(ii)** Los medios de respaldo móviles, tales como cintas, y otras unidades externas, deben ser almacenadas bajo llave o con un acceso controlado.

(b) Estos lugares de almacenamiento de los medios deben incluir no solo el control de acceso sino también la protección contra fuego, humedad, electricidad estática e influencia electro magnético, iluminación, entre otros controles de seguridad.

(c) La información respaldada fuera de sitio debe también estar fuera de línea, es decir, que utilice dispositivos discretos que no requieran ni estén conectados a otros sistemas para proteger la información.

(d) Los medios de almacenamiento utilizados deben estar capacitados para proteger la información que contienen, aun después de períodos prolongados, de hasta varios años, sin recibir electricidad.

Apartado 2.03.3.2 Frecuencia de respaldo

(a) Los organismos gubernamentales deben definir la frecuencia en la que se realizarán los respaldos.

(b) Esta frecuencia debe estar contenida dentro de las políticas y disponer de los registros necesarios en los procedimientos operativos correspondientes.

(c) La frecuencia del respaldo debe ser la necesaria para poder cumplir con los lineamientos legales, contractuales u objetivos organizacionales.

(d) En todo caso, la frecuencia debe ser la necesaria como para que la ventana de pérdida de información desde el último proceso exitoso de respaldo hasta el momento en que ocurre el evento que afecta la disponibilidad o la integridad de la información pueda ser recuperada por otros métodos.

(e) La frecuencia del respaldo debe estar a la par con la frecuencia de los cambios.

Apartado 2.03.3.3 Confidencialidad de la información almacenada

(a) Para fines de mantener la confidencialidad de la información respaldada los organismos deben:

(i) Cifrar la información que se encuentra en los medios de respaldo móviles, para lo cual deben hacer las previsiones necesarias para la gestión de las llaves, contraseñas o cualquier otro esquema de autorización.

(ii) No indicar cual información contienen estos medios, para lo cual deben elaborar un esquema de etiquetado que sea útil desde el punto administrativo pero que no revele la información que está respaldada.

(iii) En caso de transporte físico, fuera de las facilidades del organismo, estos medios deben ser transportados por un personal autorizado.

(b) Los medios a transportar no deben ser incluidos en rutas de trabajo del personal que labora externamente evitando que el dispositivo este los menos posible en posesión de este personal y sean dejado en vehículos o en situaciones de riesgo en que puedan ser perdidos o sustraídos.

(c) El organismo debe disponer de mecanismos administrativos que permitan la rápida y correcta organización y acceso a los medios de almacenamiento externos.

(d) La pérdida de un dispositivo personal con información clasificada del organismo debe ser notificada y ser manejada

como un incidente[15] de seguridad de Información para ser categorizado y planificar la respuesta correspondiente al nivel del impacto del mismo.

Sub-sección 2.03.4. Recuperación de la información

(a) En caso de pérdida o destrucción de la información, sea está clasificada o no, los organismos deben:

(i) Proceder a utilizar los medios de respaldo establecidos anteriormente en la **sub-sección 2.03.3 Respaldo de la información.**

(b) La unidad de Seguridad y Monitoreo debe tener un personal que asuma la función de recuperación de pérdida de datos.

(c) Dependiendo de la naturaleza y tamaño de los organismos, estos deben separar los roles de quien realiza el respaldo y quien accede a la información respaldada.

(d) Dado que todo proceso de recuperación presupone una pérdida de información deben elaborarse procesos administrativos que sustenten bajo qué condiciones se tomará la decisión de realizar un proceso de recuperación de la información a partir de la información respaldada.

Apartado 2.03.4.1 Autorización para el proceso de recuperación

Dependiendo de la capacidad tecnológica los organismos y sus recursos de respaldo, el proceso de recuperación puede variar intraorganizacionalmente, no obstante, la tecnología o medios utilizados para la recuperación de la información debe cumplir las siguientes directrices.

(a) El proceso de recuperación de la información debe incluir una etapa de autorización para reducir las posibilidades de recuperar la información incorrecta.

(b) Los mecanismos de recuperación deben permitir hacer uso de características de granularidad para solo recuperar aquella

[15] Es cualquier funcionamiento incorrecto de cualquiera de los servicios tecnológicos.

información mínima necesaria sin tener que sobre escribir otras informaciones que no fueron afectadas, tal como puede suceder con la recuperación de archivo, un mensaje en vez de todo el buzón de correo.

Apartado 2.03.4.2 Prueba de la recuperación

(a) Los organismos deben de disponer de los procesos administrativos y recursos tecnológicos para la verificación de las facilidades de restauración, así como la integridad de la información respaldada.

(b) Los organismos deben disponer de los indicadores necesarios para poder confirmar cuando la prueba ha sido exitosa.

(c) En caso de que las pruebas no arrojen un resultado exitoso, debe abrirse un caso para la identificación y solución de la causa raíz del problema, realizando de nuevo el proceso de respaldo y restauración hasta que los resultados obtenidos sean satisfactorios.

(d) En caso de no poder disponer de los medios, recursos o cualquier otro factor crítico para las pruebas debe notificarse a la alta dirección con el más alto nivel de prioridad para la toma de acción correspondiente.

Sub-sección 2.03.5. Borrado seguro de la información

Los organismos gubernamentales deben tener los siguientes métodos disponibles para la eliminación de la información en caso de desechar medios de almacenamiento, avería permanente o borrado seguro de la información en un medio de almacenamiento no necesario.

Apartado 2.03.5.1 Destrucción física

(a) Para la destrucción física de un medio de almacenamiento, deben seguirse las siguientes directrices:

(i) **Para la desintegración, pulverización, fusión o incineración:** Estos métodos destruyen el medio de almacenamiento por completo, debe utilizarse una trituradora de metal o proceso de incineración.

- En caso de utilizar el método anterior, debe tomarse en cuenta las medidas de seguridad pertinentes para áreas no seguras[16], como lo especifica la **sección 3.02 Controles de acceso a la infraestructura.**

(ii) **Trituración:** Ese método debe ser utilizado para la destrucción de los medios de almacenamiento de información física como el papel.

a) En todo caso el proceso de destrucción de la información debe ser tratado como un proceso legal del cual debe tener el registro necesario y la supervisión por parte del personal interno del organismo.

Apartado 2.03.5.2 Destrucción lógica

(a) Los organismos deben disponer de políticas y procedimientos para la destrucción definitiva de la información en los medios de almacenamiento que así lo soporten.

(i) Para determinar cuál información debe ser considerada dentro de esta política, debe ver la **sub-sección 2.03.1 Clasificación de la información.**

(b) En los casos en que sea necesario reclamar garantías de los medios de almacenamiento, esto solo debe hacerse para aquellos medios que no contienen información sensible, en caso de contener información sensible el organismo no podrá devolver estos medios al fabricante o a su representante.

(i) El organismo debe designar una persona con esta responsabilidad y la ejecución de esta función debe ser primero aprobada, documentada y registrada para fines de auditoría.

[16] Hace referencia a los lugares no seguros dentro del organismo que solo el personal autorizado puede transitar, tomando precauciones para evitar lesiones.

(c) El organismo debe disponer de los medios tecnológicos necesarios, que podrían incluir la desmagnetización, y el borrado seguro.

(i) El uso de estas herramientas debe ser controlado y restringido a un reducido personal autorizado.

(d) Debido a las múltiples copias que existen de la misma información mediante los procesos de respaldo esta actividad podría requerir de un nivel de autorización y posiblemente no puede ser eliminado de todos los lugares donde ya existe.

(e) Cuando un equipo sea reasignado a otra persona, los datos deben ser respaldados, este equipo debe ser previamente sanitizados para garantizar que estos datos no puedan ser recuperados ya sea de manera accidental o intencional.

(f) Los equipos o medios de almacenamiento que pudieran ser parte de una investigación judicial o forense no deben ser sanitizados hasta que hayan cumplido su propósito dentro del proceso de investigación.

SECCIÓN 2.04. Recomendaciones

- Se recomienda las siguientes pautas para el manejo de dispositivos de almacenamientos externos:
  - Desactivar los dispositivos de almacenamiento externo para todos los usuarios y solo ser permitidos en casos muy especiales luego de un proceso de solicitud y aprobación.
  - Borrar la información cuando deje de ser necesaria en medios de almacenamiento externo. Ver **sub-sección 2.03.5 Borrado seguro de la información.**
  - No utilizar los dispositivos de almacenamiento externo para transportar información clasificada.

CAPÍTULO III

ADMINISTRACIÓN DE LOS CONTROLES DE ACCESO

En esta sección se establecen las directrices que deben implementar los organismos gubernamentales para la correcta administración de los controles de acceso, por medio de políticas que apoyan los marcos de acceso a la información, acceso a la red del organismo gubernamental, acceso a los sistemas que soportan las operaciones del organismo, y las políticas para la regulación de los accesos de los usuarios.

SECCIÓN 3.01. Control de acceso de usuario

(a) Los organismos gubernamentales deben tener procedimientos establecidos para la gestión de accesos de sus empleados, estos procedimientos deben contemplar:

- **(i)** Accesos de entrada y salida al organismo gubernamental.
  - **a)** El sistema de acceso al organismo gubernamental debe cumplir las directrices establecidas en la **sección 3.02 Controles de acceso a la infraestructura.**
- **(ii)** Controles de accesos a la información del organismo gubernamental.
  - **a)** Estos controles deben contemplar las directrices establecidas en la **sección 2.02 Políticas para la administración de la información.**
- **(iii)** Controles de accesos a estaciones de trabajo.
- **(iv)** Controles de accesos a áreas restringidas.
- **(v)** Controles de accesos a áreas de servidores.
- **(vi)** Controles de accesos a software del organismo gubernamental.

(vii) Movimiento de equipos de computación fuera del organismo; los cuales deben ser registrados y autorizados.

(b) Los organismos gubernamentales deben hacer una revisión de los accesos de los usuarios anualmente. Esta revisión debe estar documentada.

(c) Los organismos gubernamentales deben hacer una revisión, modificación o eliminación de los accesos de los usuarios al momento en que estos:

- Sean cancelados.
- Sean promovidos.
- Sean transferidos a diferentes localidades.
- En caso de fallecimiento.
- Cambien de funciones dentro del mismo organismo.

(d) La unidad de Seguridad y Monitoreo debe tener un personal asignado del área de Administración de accesos para la gestión de accesos de los empleados.

(e) Las aplicaciones deben disponer de un esquema de control de acceso que efectivamente controle la separación de roles de los usuarios, administradores y diferentes grupos de usuarios según los perfiles de uso.

SECCIÓN 3.02. Controles de acceso a la infraestructura

(a) Los organismos gubernamentales deben contar con un proceso de control de acceso.

(i) Los organismos gubernamentales deben tener un procedimiento de registro de entradas y salidas.

a) El sistema o el proceso registro de entradas y salidas debe contemplar los siguientes datos e informaciones:

- Fecha.
- Nombre del empleado.
- Hora de entrada.

- Firma a la hora de entrada.
- Hora de salida.
- Firma a la hora de salida, en caso de ser un proceso manual.
- Firma biométrica, en caso de ser un sistema.

(ii) Para la entrada de un visitante al organismo gubernamental, deben agotarse los pasos a continuación:

a) El visitante debe dejar una identificación en la recepción donde posteriormente se le entregará un carnet de identificación con el nivel de acceso permitido descrito en la **tabla No. 3. Niveles de acceso.**

b) El visitante debe ser acompañado por un personal del organismo gubernamental hasta su lugar de visita o reunión. Del mismo modo, el visitante debe ser acompañado a la salida de la locación, al momento de concluir su visita.

c) Al final de la visita del invitado, este debe entregar el carnet de identificación en la recepción donde se le entregaran sus credenciales.

(iii) El área de implementación de sistemas del departamento de TIC debe administrar la información generada por el sistema.

(iv) Los organismos gubernamentales deben hacer su asignación de niveles de accesos en base a la siguiente **tabla No. 3. Niveles de acceso:**

Tabla No. 3. Niveles de acceso

Nivel de acceso	Destinado a:	Descripción:
Nivel 1	• Invitados	• Acceso de entrada y salida al organismo • Acceso a áreas básicas del organismo • Acceso restringido al centro de datos[17] • Acceso restringido a áreas de seguridad específicas y clasificadas por el organismo
Nivel 2	• Personal del organismo	• Acceso de entrada y salida al organismo • Acceso a áreas pertinentes al rol del personal • Acceso restringido al centro de datos
Nivel 3	• Personal del organismo autorizado • Personal del departamento de TIC	• Acceso de entrada y salida al organismo • Acceso a todas las áreas básicas del organismo • Acceso abierto al centro de datos
Nivel 4	• Personal autorizado por el organismo	• Acceso de entrada y salida al organismo • Acceso a todas las áreas básicas del organismo • Acceso a áreas de seguridad específicas y clasificadas por el organismo

[17] Es un área donde se concentran y operan los equipos que conforman la infraestructura TIC que utilizan los organismos para administrar sus actividades y servicios.

(b) Los organismos deben tener señalizadas las áreas seguras[18] y no seguras para el empleado según el nivel peligro al que puedan estar expuestos.

(i) Las áreas no seguras deben estar igualmente señalizadas y solo el personal autorizado tendrá acceso a las mismas.

(ii) Dentro de las áreas no seguras debe incluirse:

- Áreas de carga.
- Áreas eléctricas.
- Áreas con productos derramados.
- Áreas con herramientas cortantes o filosas.
- Áreas con tránsito vehicular dentro del organismo.
- Áreas con desechos del organismo.
- Áreas con combustibles.
- Cualquier otra área determinada como no segura por el organismo.

(iii) Si un personal identifica algún área con un nivel de peligrosidad no identificado debe reportarlo inmediatamente al área designada por la máxima autoridad del organismo para los fines.

SECCIÓN 3.03. Control de acceso al sistema operativo

(a) Las conexiones remotas a las estaciones de trabajo o servidores deben:

(i) Tener un cifrado mínimo con una llave de 128 bits[19] de longitud mínima.

(ii) Tener un tiempo de bloqueo de la estación de trabajo o servidores tras quince (15) minutos de inactividad.

[18] Hace referencia a los lugares seguros dentro del organismo que los empleados y visitantes pueden transitar sin correr ningún peligro.

[19] Un bit es un dígito del sistema de numeración binario. La capacidad de almacenamiento de una memoria digital también se mide en bits.

(iii) Tener un tiempo de desconexión de acceso a la estación de trabajo o servidores tras quince (15) minutos de inactividad.

(iv) Este servicio solo debe estar disponible para el personal autorizado por el departamento de TIC.

(v) Todos los servidores deben disponer de conexión segura por medio del Intérprete de Órdenes Seguro (SSH[20], por sus siglas en inglés) o Seguridad de la Capa de Transporte (TLS[21], por sus siglas en inglés) en su versión 1.2 o superior.

(vi) Las conexiones remotas para transferencia de archivos deben ser por medio del Protocolo Seguro de Transferencia de Archivos (SFTP[22], por sus siglas en inglés).

(b) Las estaciones de trabajo que establezcan conexiones a servidores deben estar protegidas por antivirus[23].

(c) Las conexiones fuera de los organismos gubernamentales a servicios críticos en servidores deben ser por medio de una Red Privada Virtual[24] (VPN, por sus siglas en inglés), seguida por autentificación en el servidor.

(i) Los protocolos de seguridad en las conexiones en una VPN que los organismos deben utilizar son los siguientes:

- Protocolo Seguro de Internet[25] (IPsec, por sus siglas en inglés).
- TLS.
- Intérprete Órdenes Seguras[26] (SSH, por sus siglas en inglés).

[20] Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

[21] Es un protocolo criptográfico que proporciona comunicación segura por una red, comúnmente Internet. Este protocolo permite una serie de operaciones sobre archivos remotos.

[22] Es un protocolo de red utilizado para acceder y manejar archivos de manera remota utilizando métodos de encriptación.

[23] Es un programa desarrollado con el fin de proteger un computador o servidor contra virus informáticos.

[24] Es una red virtual privada que permite de forma segura la interacción de datos sobre redes compartidas utilizando como vínculo el Internet.

[25] Es un conjunto de protocolos de seguridad para proteger la comunicación IP y transmisión de paquetes en Internet.

[26] Es un protocolo y aplicación por el cual se accede remotamente a una computadora a través de una red de comunicaciones.

(d) Las conexiones dentro de los organismos gubernamentales a servicios críticos en servidores deben ser por medio de autentificación en el servidor que aloja los servicios.

(e) Los departamentos de TIC deben tener un sistema de monitoreo para detectar posibles violaciones a las políticas y medidas de seguridad.

(f) Solo el personal técnico del departamento de TIC, o a quién este autorice, tendrá permisos a conexiones de terminales de trabajo o servidores.

(g) Todos los usuarios deben estar registrados en la base de datos[27] del departamento de TIC para poder tener acceso a las estaciones de trabajo.

(i) Los departamentos de TIC deben asignar permisos para autentificación en las estaciones de trabajo y permisos para los servicios que estén disponibles en la red.

(h) Todas las estaciones de trabajo de los organismos gubernamentales deben estar protegidas por contraseña que cumplan las siguientes características:

(i) Las contraseñas deben tener un mínimo de ocho (8) caracteres.

(ii) Las contraseñas deben tener al menos una letra mayúscula.

(iii) Las contraseñas deben tener letras minúsculas.

(iv) Las contraseñas deben tener al menos un número.

(v) Las contraseñas deben ser renovadas cada cuarenta y cinco (45) días.

(vi) Las contraseñas personales no deben ser compartidas para no comprometer información sensible que resida en las estaciones de trabajo.

(vii) Las contraseñas definidas por el empleado no deben ser comunes.

[27] Son un conjunto de datos almacenados de manera ordenada y que guardan relación entre ellos para su uso posterior.

(viii) Las contraseñas no se pueden reutilizar en diferentes sistemas a menos que se esté utilizando un sistema de autenticación[28] centralizado o de Autentificación Sencilla.

(i) En caso de que el empleado tenga inconvenientes para acceder a su estación de trabajo, este debe solicitar soporte al departamento de TIC y bajo ningún término tratar de acceder por mecanismos de fuerza bruta.

SECCIÓN 3.04. Control de acceso en la red

(a) Los organismos gubernamentales deben tener políticas y controles técnicos para el uso de los servicios y recursos de la red.

(i) Dentro de los servicios y recursos a tomar en cuenta deben estar:

a) Para el uso de Internet deben seguirse las directrices a continuación:

i) Este servicio debe tener protección por cortafuegos[29] e intermediario (haciendo referencia a proxy[30]).

ii) Este servicio debe tener filtro de tráfico por niveles de usuario. Ver **Tabla No. 3. Niveles de acceso.**

- Con contenido ilícito.
- De juegos en línea.
- De apuestas en línea o actividades ilegales.
- Con contenido pornográfico.
- Cualquier otro que el organismo considere.

iii) El uso del acceso al Internet debe mantener registros del uso y del tiempo utilizado por los empleados.

iv) Debe generarse un informe resumen con los registros de uso del Internet para la supervisión de la máxima autoridad.

[28] Es el proceso de validación que sirve para detectar y probar la identidad de una entidad.

[29] Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

[30] En una red informática, es un servidor (un programa o sistema informático), que hace de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C).

v) Todos los accesos a la Internet deben ser denegados al visitante; en caso de que este lo necesite pueden ser otorgados temporalmente luego de una previa solicitud y aprobación.

b) Para el uso de Intranet deben seguirse las directrices a continuación:

i) Este servicio debe estar a la disposición del empleado por medio de autentificación.

ii) Este servicio debe ser para uso exclusivo de los empleados del organismo.

c) Para el uso de impresoras deben seguirse las directrices a continuación:

i) Este recurso debe ser utilizado exclusivamente para impresiones relativas al organismo gubernamental.

ii) Los empleados no deben hacer uso personal de este recurso.

iii) Los documentos impresos deben ser retirados de inmediato por el dueño del documento impreso.

iv) Las áreas que manejen información sensible deben tener una impresora cuyo acceso físico también sea restringido.

d) Para el uso de escáner deben seguirse las directrices a continuación:

i) Los documentos escaneados deben ser retirados de inmediato por el empleado dueño del documento escaneado.

(b) Los organismos gubernamentales deben tener políticas de autenticación y las implementaciones técnicas necesarias para gestionar conexiones externas a los servicios internos del organismo. Ver **NORTIC A1:2014, sub-sección 4.01.2. Administración de la red privada y la red de área local inalámbrica.**

(c) Cada equipo dentro de la red de los organismos gubernamentales debe estar registrado dentro del inventario de los departamentos de TIC. Ver **Sección 6.05 Gestión de activos.**

(d) El departamento de TIC debe controlar la configuración, y acceso físico o lógico, tanto interno como externo al organismo, a los puertos de diagnóstico de la infraestructura de TIC del organismo.

(e) El departamento de TIC debe tener controles establecidos de enrutamiento de las redes, para asegurar que las conexiones de las aplicaciones y servicios en la red del organismo gubernamental no incumplan las políticas de seguridad.

(f) El departamento de TIC debe mantener registros de todos los acceso otorgados y utilizados por el personal que se encuentra fuera de las redes del organismo.

(g) El organismo debe disponer de controles para dar acceso a los equipos de los empleados con antivirus y cortafuego como mínimo.

(h) Los equipos de visitantes solo deben tener un acceso restringido al internet sin interacción con la red del organismo, a menos que este lo requiera.

(i) En caso de necesitar acceso a la red local, los permisos deben ser asignados luego del equipo contar con las políticas de seguridad necesarias.

SECCIÓN 3.05. Control de acceso a los medios de respaldo

(a) Los organismos deben disponer de los procesos administrativos necesarios para que solo el personal autorizado tenga acceso a los medios de respaldo para fines de recuperación de información.

(b) Debe mantenerse una lista actualizada de quienes son las personas con acceso a los medios de respaldo.

CAPÍTULO IV

PLAN DE DISPONIBILIDAD Y CONTINUIDAD

Los planes de disponibilidad y continuidad juegan un papel muy importante en los organismos ya que contienen los pasos detallados de como volver la operación a un nivel esperado frente a eventos que interrumpan la capacidad de procesamiento por un componente tecnológico o causen la interrupción total de la operación como consecuenticas de la pérdida de un edificio o localidad principal de procesamiento de datos y operación de los empleados.

SECCIÓN 4.01. Plan de disponibilidad

Un plan de disponibilidad tiene como objetivo, velar por que la información, procesos y sistemas estén disponibles al momento en que se requieran, permitiendo el acceso, solo a las personas con la debida autorización y permisos.

Sub-sección 4.01.1. Gestión de la disponibilidad

(a) Dentro de los procedimientos operativos del organismo deben disponerse de procedimientos y recursos tecnológicos para dar seguimiento a la disponibilidad de los recursos de TIC.

(b) Cuando se presente alguna condición que afecte la disponibilidad de los sistemas debe elaborarse un registro de esta situación.

(c) Los problemas de disponibilidad deben ser evaluados para determinar si tienen que ser tratados como un incidente de seguridad de información.

(d) Los organismos deben disponer de los mecanismos necesarios para generar alertas y notificaciones cuando los sistemas críticos dejen de esta disponible y poder atenderlos antes de que afecten los niveles operativos del organismo.

(e) Deben hacerse análisis históricos periódico para identificar posibles ocurrencias que no han sido resueltas en su causa raíz.

Sub-sección 4.01.2. Gestión de la capacidad

(a) Dentro de los procedimientos operativos del organismo deben disponerse de procedimientos y recursos tecnológicos para dar seguimiento al uso de los recursos de TIC y poder identificar cualquier variación importante que demanden los usuarios o sistemas.

(b) Deben generarse los informes periódicos pertinente para identificar tendencias y proyecciones de posibles necesidades para poder actuar de manera oportuna en el aumento de la capacidad.

(c) Deben disponerse de los mecanismos necesarios para generar alertas y notificaciones cuando estas variaciones alcancen ciertos niveles de uso antes de que se lleguen a condiciones de criticidad.

Sub-sección 4.01.3. Gestión de incidentes

(a) Los organismos gubernamentales deben de implementar un Programa de Gestión de Incidentes (PGI), que les permita responder lo antes posible a un incidente con fines de restaurar el servicio o solucionar el problema, así como evitar que el impacto se extienda a otras áreas de recursos del organismo o fuera.

(b) Este programa debe crear un comité de trabajo multidisciplinario que contenga representantes de alto nivel de cada una de las áreas funcionales más importantes del organismo.

(c) Deben crearse los procedimientos y políticas necesarios para los principales escenarios a experimentar los cuales deben estar escritos, probados y aprobados por la dirección.

(d) Los incidentes de seguridad de información deben ser notificados al Departamento de Investigaciones de Crímenes y Delitos de Alta Tecnología (DICAT), cuando se encuentren indicios que puedan ser una evidencia criminal según lo establece la Ley No. 53-07 sobre crímenes y delitos de alta tecnología.

(e) El organismo debe disponer de procedimientos administrativos y operativos para disparar el proceso de gestión de incidentes tan pronto como se confirmen los eventos o notificaciones que, proviniendo de cualquier fuente, indique que está sucediendo un incidente.

(f) El organismo debe informar a las partes interesadas correspondientes cómo reportar un evento de seguridad o un incidente, esta capacidad de recibir notificaciones debe estar disponible las 24 horas del día 7 días de la semana 365 días al año.

(g) Deben implementarse los formularios necesarios para la recopilación de información pertinentes y los enrutados de llamadas necesarias para que los reportes sean dirigidos a personal activo o en turno fuera de horario.

(h) Debe motivarse al personal a identificar posibles situaciones de riesgo que pueden conducir a un incidente y reportarlos al punto de contacto[31].

(i) Debe elaborarse un procedimiento de escalamiento para que en los casos de que el personal interno no esté en capacidad de manejar el incidente de manera correcta, el caso pueda ser escalado a personas con las capacidades necesarias sin tener que recurrir a procesos de aprobación por tema de costos o cualquier otra autorización que sea necesaria.

Esto permitirá hacer uso de una horas estimadas y pre aprobadas de soporte en caso de ciertos escenarios.

[31] Dentro de la disciplina de Manejo de Incidentes, es el grupo, unidad o persona que tiene el rol de recibir el informe inicial de un evento de seguridad, para examinarlo, evaluarlo, resolverlo o tratarlo y en caso de que este fuera de su alcance de especialización escalarlo a los grupos de tratamiento de incidentes.

(j) Debe disponerse de un proceso de lecciones aprendidas que permitan evaluar las enseñanzas de las cosas que pudieron hacerse diferente, las que funcionaron y las posibles causas raíz de incidente.

(k) Luego de cada evento deben calendarizarse acciones de seguimiento para aquellos casos en que no se pudo resolver la causa raíz.

(l) Debe documentarse el procedimiento para que se active el plan de continuidad para aquellos incidentes que tengan un tiempo estimado de recuperación superior a lo identificado como aceptable para el organismo

SECCIÓN 4.02. Plan de continuidad

La implementación de los procesos de la gestión de la continuidad, es un aspecto de gran importancia dentro del departamento de TIC; esta implementación busca que tanto los servicios del organismo, como los procesos que sustentan las operaciones permanezcan en funcionamiento ante cualquier eventualidad, ya sea externa o interna.

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

(b) La continuidad del organismo debe tener como responsable a la máxima autoridady no al área de TIC.

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

(d) Los organismos gubernamentales deben tener un plan de continuidad para asegurar la recuperación ordenada y planificada de sus operaciones vitales y sus servicios al ciudadano o demás organismos.

(e) El CONTI debe considerar no solo los aspectos relacionados o dependientes de TIC sino también, y primariamente, los procesos, las personas, las localidades que son vitales para que el organismo pueda seguir proveyendo servicios a la comunidad y al estado.

(f) La seguridad de la información debe estar dentro del plan de la continuidad del organismo.

(i) Dentro del desarrollo del plan, debe contemplarse la activa participación de la máxima autoridad del organismo para garantizar los requerimientos necesarios para el correcto aseguramiento de las informaciones críticas y vitales del organismo.

(ii) Para la implementación de este plan debe tomarse en consideración lo siguiente:

a) Deben priorizarse los procesos críticos del organismo.

b) Deben identificarse los riesgos a los que se encuentra expuesto el organismo en términos de probabilidad.

i) Deben establecerse controles de prevención a los riesgos identificados.

c) Deben identificarse todos los activos involucrados en los procesos críticos del organismo, tanto de información como tecnológicos.

d) Deben establecerse políticas de procedimientos en caso de interrupciones causadas por incidentes en la seguridad de la información en el organismo, sean estos incidentes menores o críticos.

e) Deben identificarse recursos financieros y técnicos suficientes para tratar los requerimientos de seguridad de la información identificados en el proceso del plan.

f) Debe garantizarse el personal técnico que sirve de soporte para la protección de los medios de procesamiento de la información del organismo.

g) La seguridad de la información establecida en el plan, debe estar alineada con la estrategia de la continuidad del organismo.

h) Debe establecerse una recurrencia de pruebas y revisiones del plan según la naturaleza del organismo.

i) Para asegurar la gestión de la continuidad del organismo, esta debe incorporarse a la estructura organizacional y tener un responsable dentro del departamento de TIC.

(g) Para la continuidad del organismo y la evaluación del riesgo debe tomarse en cuenta lo siguiente:

(i) Deben identificarse los eventos que pueden causar interrupciones a la continuidad del organismo y asociar los mismos a la probabilidad y el impacto de las mismas en conjunto con las consecuencias para la seguridad de la información.

(ii) La evaluación de riesgo debe estar basada en eventos o secuencia de eventos para determinar las probabilidades e impactos de las interrupciones y periodos de recuperación.

(h) Para el desarrollo e implementación del plan de continuidad del organismo y seguridad de la información, debe tomarse en cuenta lo siguiente:

(i) Deben establecerse planes de restauración de las operaciones del organismo para asegurar la disponibilidad de la información en el menor tiempo posible, donde lo más crítico sea restablecido y puesto en funcionamiento en primer lugar.

(ii) Para la planificación de la continuidad del organismo debe tomarse en cuenta lo siguiente:

- Identificación y acuerdo de responsabilidades y procedimientos.
- Identificación de perdida de información aceptable y de servicios.
- Implementación de políticas para la recuperación y restauración de las operaciones y disponibilidad de la información del organismo.
- Evaluación de dependencia de servicios de TIC externos o internos.
- Documentación de procesos y acuerdos.

- Entrenamiento al personal designado sobre los procesos para la gestión de crisis.
- Prueba y actualización del plan.

(iii) La planificación debe estar enfocada al plan estratégico de la máxima autoridad apoyada en los recursos de TIC.

(iv) La planificación debe contemplar las debilidades del organismo para proteger las informaciones más críticas y confidenciales que afectan la continuidad y prestación de servicios.

a) En caso que el organismo disponga de varias localidades, el plan debe residir en cada una de las localidades del organismo.

(v) Los controles de seguridad en localidades temporales deben ser iguales a los niveles de las localidades principales.

(i) Debe tomarse en cuenta el siguiente marco de referencia para la creación del plan de continuidad del organismo:

(i) Para asegurar la consistencia de todos los planes, debe utilizarse un (1) solo marco de referencia para la elaboración del mismo.

(ii) Todo plan debe estar enfocado y orientado al plan estratégico de la máxima autoridad, así como a la disponibilidad y seguridad de la información que sustentan las operaciones del organismo.

(iii) Todo plan debe tener especificaciones para su activación, así como los responsables de las ejecuciones de sus instrucciones de procedimientos.

(iv) Todo plan debe tener un propietario en específico, sea un plan de emergencia, contingencia, crisis o continuidad del organismo.

a) Debe evaluarse cada doce (12) meses que los propietarios asignados, estén en condiciones de poder asumir la responsabilidad de ejecutar el plan a cabalidad.

(v) El marco de creación de la planificación de la continuidad del organismo debe incluir los siguientes:

- Condiciones para la activación de plan.
- Procedimientos de emergencia y descripción de acciones.
- Procedimientos de contingencia y descripción de acciones para traslado para locales temporales.
- Procedimientos de reanudación de las operaciones y servicios de TIC.
- Programa de mantenimiento, prueba o simulacro del plan.
- Programa de educación y capacitación al personal sobre los procesos del plan.
- Responsabilidades de las personas designadas dueños de planes y personal alternativo.
- Activos y recursos críticos de TIC con capacidad de realizar tareas de emergencia, respaldo y reanudación de la operación.

(j) Debe tomarse en cuenta lo siguiente para la prueba, mantenimiento y re-evaluación del plan de continuidad del organismo:

(i) El plan debe ser revisado, actualizado y/o aprobado cada doce (12) meses.

(ii) El plan debe asegurarse que los demás dueños de planes estén al tanto de las actividades relevantes.

(iii) El programa de prueba debe especificar cómo y cuándo debe probarse cada uno de los siguientes elementos del plan:

- Prueba simple o flexible de simulación: Evalúa acuerdos de recuperación por un tercero contratado.
- Simulaciones: Con el fin de capacitar a los responsables en sus roles.
- Prueba de recuperación técnica: Asegura la efectiva recuperación de los sistemas de información.
- Prueba de recuperación en local alterno: Asegura la efectiva recuperación en paralelo de los sistemas de información en conjunto con los servicios contratados en locales retirados al principal.
- Pruebas de los servicios contratados: Asegura que

los Acuerdos de Nivel de Servicio[32] (SLA, por sus siglas en inglés) sean óptimos.

- Simulaciones completas: Pone a prueba todos los escenarios para asegurar el correcto funcionamiento del plan.
- El programa de prueba debe ser implementado de manera que sea relevante al organismo y los resultados deben ser registrados para toma de decisiones sobre el plan.

(iv) Deben verificarse las siguientes informaciones del plan al momento de su revisión:

- Personal responsable de plan y personal alternativo.
- Direcciones y números de contacto.
- Alineación del plan con la estrategia organizacional.
- Locales y/o sucursales.
- Proveedores de servicios y clientes.
- Procesos, tanto nuevos como actualizados o eliminados.
- Evaluación de riesgo.

Sub-sección 4.02.1. Procedimientos de continuidad

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

(b) Los procedimientos deben establecer por adelantado la habilitación de un Centro de Comando[33] desde donde se dirigirán las labores de recuperación en caso de que la localidad principal resulta inoperante como consecuencia de algún incidente disruptivo.

[32] Es un documento que plasma los acuerdos entre un proveedor de servicio y el cliente, en donde se estipulan los requisitos y parámetros que el proveedor se compromete a cumplir para mantener unos niveles de calidad de servicio.

[33] Es el lugar desde el cual se dirigen las actividades de recuperación de las actividades críticas de las operaciones de un organismo luego de sufrir una catástrofe.

(c) Los procedimientos deben indicar los pasos de activación del plan, quien o quienes son las personas autorizadas para activar el plan, la forma en que se evaluará la toma de decisiones.

(d) Los procedimientos deben indicar las personas, los roles, los recursos necesarios, así como la forma de comunicación que existirá entre el equipo del CONTI las personas que llevan a cabo las tareas de recuperación.

(e) Los procedimientos deben indicar cuales personas deberían asumir los roles de liderazgo en caso de que el personal principal no pueda estar disponible para las tareas de recuperación.

Sub-sección 4.02.2. Análisis de riesgos e impacto

(a) Dentro del proceso de creación del análisis de riesgos, debe tomarse en cuenta lo siguiente:

- Identificar los ambientes operativos que se pueden ver afectados en caso de un incidente.
- Identificar los principales escenarios de falla y los recursos e infraestructuras críticas.
- Identificar oportunidades de mejora o exposiciones críticas a riesgos de falla.
- Identificar las políticas y mejores prácticas de seguridad existentes.
- Revisión de instalaciones físicas, centros de cómputo e infraestructuras tecnológicas en general.

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

(i) La integración de la máxima autoridad del organismo gubernamental en este proceso es fundamental para la correcta elaboración y aprobación del BIA.

(ii) En la elaboración de BIA deben tomarse en cuenta los siguientes procesos:

- Verificación del inventario de procesos.
- Identificación de impactos.
- Definición de tiempos y secuencia de recuperación.
- Identificación de interdependencias entre procesos.
- Identificación de los procesos críticos del negocio.
- Recursos e insumos necesarios para la recuperación de los servicios
- Personal clave.
- Análisis de riesgo. Ver **sub-sección 4.02.1 Análisis de riesgos e impacto.**

El BIA debe tener un Tiempo de Recuperación Objetivo (RTO, por sus siglas en inglés) y un Punto Objetivo de Recuperación (RPO, por sus siglas en inglés) aceptables que no comprometan las operaciones vitales del organismo gubernamental.

(iii) En caso de que los organismos gubernamentales no tengan el recurso humano para la elaboración del BIA, debe contratar un consultor certificado, con experiencia probada, específicamente en el área a ser contratado, para los fines. Ver NORTIC A1:2014, directriz 3.02.1.c.

Sub-sección 4.02.3. Pruebas y simulacros

(a) El CONTI solo debe ser considerado como completado cuando se ha realizado una prueba funcional del mismo, se han validado los resultados y realizados los ajustes necesarios a fin de que cumpla con los objetivos identificados durante su fase de diseño.

(b) La forma de medir que el plan ha sido completado es mediante el informe del comité del CONTI informando a la máxima autoridad, la cual, luego de revisarla hará las observaciones de lugar y dará por completado el proceso de implantación inicial mediante firma de que los objetivos han sido logrados.

(c) Los organismos gubernamentales deben generar periódicamente informes sobre la ejecución y estado de su plan de continuidad.

(i) Los organismos gubernamentales deben tomar en cuenta lo siguiente para sus evaluaciones periódicas del plan de continuidad:

- Análisis sobre nuevos riesgos y los impactos de los mismos.
- Revisión del impacto económico asociado al plan de continuidad.
- Evaluación sobre los simulacros del plan de continuidad.
- Capacitación del personal del departamento de TIC para llevar a cabo el plan de continuidad.

(ii) Los organismos gubernamentales deben hacer una revisión de su plan de continuidad una (1) vez al año, o cuando se experimente algún cambio importante en la forma de operar del organismo o cambien el contexto interno o externo en el que opera el organismo.

(d) El Plan de Continuidad de Negocios debe de ser probado bajo premisas o escenarios hipotéticos que permitan la medición del logro de ciertos objetivos, como tiempo de recuperación, nivel de recuperación, efectividad de los procedimientos, disponibilidad de los recursos entre otros posibles indicadores de éxito.

(e) Las pruebas y simulacros deben ser documentados.

(f) Las pruebas y ejercicios deben contemplar planes de evacuación y prevención de pérdidas humanas frente a la ocurrencia de ciertos escenarios.

(g) Las pruebas y simulacros deben medir los niveles de efectividad del desempeño del personal en labores de evacuación y rescate.

(h) Las pruebas y simulacros no deben introducir elementos de falla en los ambientes reales de producción.

Sub-sección 4.02.4. Conciencia y capacitación del plan de continuidad

(a) Debe concientizarse sobre la importancia del plan a todos los empleados del organismo.

(b) Debe socializarse el plan al CONTI y a todo el organismo.

(c) Debe designarse un responsable del plan para su actualización y mantenimiento

(d) El proceso y resultados de la concienciación debe estar documentado.

(e) Debe realizarse la capacitación del personal según se reemplacen personas con responsabilidades dentro del plan.

Sub-sección 4.02.5. Estrategias de recuperación alineadas con la gestión de riesgo y el análisis de impacto

(a) Dependiendo de las necesidades de recuperación el organismo debe identificar las estrategias de recuperación que satisfaga estos requerimientos.

(b) La estrategia debe seleccionarse poniendo énfasis en opciones que sean costo efectivas.

(c) Debe utilizarse tecnologías existentes con las cuales el personal esté familiarizado.

(d) La estrategia que se implementen a su vez debe también estar protegida de eventos similares o escenarios similares que produjeron la salida inicial de los procesos críticos del organismo.

(e) Para proteger estas estrategias deben realizarse los siguientes procesos:

- **(i)** Definir requerimientos mínimos para cada proceso.
- **(ii)** Identificar configuraciones alternativas de recursos.
- **(iii)** Determinar las redundancias de equipos y de comunicaciones.
- **(iv)** Analizar las diferentes posibilidades en procesamiento y en comunicaciones.

(f) Determinar las opciones estratégicas de procesamiento internas y externas.

Sub-sección 4.02.6. Plan de recuperación ante desastres

El Plan de Recuperación ante Desastres (DRP, por sus siglas en inglés) es utilizado para la recuperación de ciertos recursos o procesos tecnológicos una vez haya pasado una eventualidad o siniestro.

(a) Para la implementación del DRP debe tomarse como referencia lo establecido en la siguiente metodología:

- Análisis de riesgo sobre los servicios de TIC.
- Evaluación de riesgos de la infraestructura de TIC.
- Desarrollo de estrategias para la recuperación.
- Definición de roles y responsabilidades.
- Pruebas del DRP.

(b) Los planes de recuperación de desastres deben contemplar los requerimientos oportunos para protegerse de un fallo del proveedor de servicios.

(c) Los planes de recuperación de desastres deben hacer la provisión oportuna de contratos de mantenimiento, soportes y garantías con los fabricantes de los productos y/o servicios para garantizar la disponibilidad del recurso dentro de un tiempo acordado.

(d) Los planes de recuperación de desastres deben contemplar vías alternas para la recuperación de un servicio tecnológico en caso de que cierto dispositivo o servicio se encuentre fuera de garantía.

(e) Los planes de recuperación de desastres deben disponer de los recursos necesarios como repuestos locales para una rápida recuperación en caso de equipos y/o servicios fuera de garantía o en los que la respuesta del fabricante puede ser mayor de lo que se puede aceptar por parte de la operación del organismo.

(f) Los planes de recuperación de desastres deben identificar los posibles puntos únicos de falla[34] para crear esquemas alternos de recuperación.

[34] Se conocen como puntos únicos de falla a esos componentes únicos en una infraestructura, de manera que cuando experimentan una falla, el servicio también se ve interrumpido ya que no existe un mecanismo alterno de como continuar operando.

Sub-sección 4.02.7. Seguimiento y mejora

(a) Este plan debe ser revisado por lo menos una vez al año o cuando se realicen cambios importantes en la forma de operar del organismo.

(b) El plan de continuidad debe indicar fechas de revisiones periódicas para garantizar su idoneidad o relevancia y evitar su desactualización.

(c) Este plan debe actualizarse antes de las fechas previstas si se presentan cambios operativos o tecnológicos importantes en la forma de operar del organismo, tal como la implantación de un nuevo sistema de gestión operativa o automatización de procesos.

(d) Estas revisiones deben ser presentadas a la alta dirección con los informes de los objetivos alcanzados y oportunidades de mejora.

(e) La alta dirección debe aprobar estos informes, así como los planes de mejoras sugeridos en los mismos.

SECCIÓN 4.03. Recomendaciones

- Se recomienda que el organismo disponga de un seguro que forme parte del proceso de la continuidad del organismo en temas de riesgo operacionales e infraestructura TIC para reducir el impacto económico y la disponibilidad de recursos financieros para la restauración de los servicios críticos en caso de una pérdida significativa.
- Se recomienda que las prioridades de recuperación sean el resultado del consenso de las principales unidades organizativas.
- Se recomienda que los esfuerzos a realizar y las estrategias de recuperación tengan una orientación costo efectiva a la hora de selección de los controles.

- Se recomienda que los recursos humanos que tienen responsabilidad relevante en la ejecución del plan dispongan de más de un sustituto en caso de que el líder de la recuperación no esté disponible.
- Se recomienda que los tiempos objetivos de recuperación estén ajustados a la realidad del organismo.
- Se recomienda que el plan de continuidad contemple recursos más allá de tecnología de información y pudiera requerir de la consideración de recursos como mobiliarios, maquinaria, espacio físico para el personal y servicios de seguridad física.
- Se recomienda que las localidades alternas dispongan de una capacidad de autonomía de hasta dos (2) semanas a nivel de generación eléctrica, suministro de combustible y otros tipos de abastecimiento.
- Se recomienda que las localidades alternas estén geográficamente separadas para que el mismo evento no impacte tanto el sitio principal como el alterno.
- Se recomienda evitar localidades alternas muy distantes, ya que podría representar una dificultad para el traslado del personal o la disponibilidad del mismo.
- Se recomienda dar como aprobado el plan de continuidad luego de que el mismo supere todas las pruebas de lugar.

CAPÍTULO V

GESTIÓN DE RIESGO

En este capítulo se establecen las directrices para la gestión del riesgo, especificando su metodología, componentes, evaluación, tratamiento y entregables de la misma, así como también las directrices necesarias que un organismo debe cumplir al momento de realizar el proceso de análisis de riesgo.

SECCIÓN 5.01. Metodología de gestión de riesgo

(a) Los organismos gubernamentales deben tener una metodología formal, documentada y aprobada para la gestión de riesgos que trate de manera proactiva las amenazas y vulnerabilidades pudieran afectar la operación del organismo en caso de futuras situaciones.

- **(i)** Esta metodología debe estar enfocada y orientada a los procesos de la organización, y los activos asociados, no solamente a los activos sin guardar relación con los procesos.

(b) El organismo debe crear un inventario de los activos. Ver **sección 6.05 sobre gestión de activos.**

(c) La metodología de gestión de riesgos debe formar parte de la toma de decisiones de la máxima autoridad del organismo gubernamental.

(d) La metodología de gestión de riesgos debe estar alineada al plan estratégico del organismo gubernamental.

(e) La gestión de riesgos debe atender y dar prioridad a los objetivos estratégicos establecidos en el plan del organismo.

(f) El plan de gestión de riesgos debe tomar en cuenta los recursos humanos dentro de su planificación, los elementos externos a la operación del organismo.

(g) El plan de gestión de riesgos debe facilitar la mejora continua del organismo gubernamental.

(h) El plan de gestión de riesgos debe ser lo suficientemente flexible al cambio, en caso de que sea requerido por la máxima autoridad del organismo gubernamental.

(i) La organización debe desarrollar una metodología de gestión de riesgo que sea coherente y que pueda proveer resultados consistentes.

(j) En esta metodología deben estar claramente establecidos el o los criterios de aceptación del riesgo, lo cual significa que se establecen los niveles de riesgo para los cuales la organización, especialmente alta dirección, entiende que no debe aplicarse ningún control y no existe una razón económica, funcional o de reputación que justifique ningún tipo de acción en reducir el nivel de riesgo particular de algún activo de información o proceso.

(k) Esta metodología debe estar alineada con la práctica organizacional de Gestión de Riesgo, si existe.

No se exige que se utilice ningún marco de referencia de Gestión de Riesgo específico, existen diferentes alternativas y posiblemente los aspectos culturales de como la organización viene ya gestionando el riesgo puede servir de base para formalizar esta disciplina en lo futuro.

La norma ISO/IEC 27005, aunque no requerida, puede servir de guía para el desarrollo de una metodología orientada a seguridad de información.

(i) La gestión del riesgo es la base que sirve de sustento para todas las medidas y planes de acción del organismo, por lo tanto, no debe existir ninguna medida que no responda a la gestión de riesgo, por lo que todo plan de acción debe indicar el riesgo al cual está respondiendo.

(l) Esta metodología debe incluir los procesos de revisión de los niveles de riesgo en función a las nuevas realidades, como varían los agentes de amenaza a los componentes del impacto.

(m) Debe aplicarse esta metodología siempre que se realicen cambios sustanciales en la forma de operar del organismo o se introduzcan o modifiquen elementos de TIC.

SECCIÓN 5.02. Componentes de la apreciación del riesgo

En la siguiente sección se establece el procedimiento que deben seguir todos los organismos para la gestión del análisis, evaluación y tratamiento del riesgo.

Sub-sección 5.02.1. Análisis del riesgo

(a) El proceso de Análisis del Riesgo debe tomar en cuenta las siguientes fases con sus respectivas acciones para la elaboración del plan.

- **Probabilidad:** Es el nivel de potencialidad de que la amenaza explote la vulnerabilidad
- **Impacto:** Indica el nivel de daño que se puede sufrir de la amenaza explotar la vulnerabilidad.
    - El impacto a su vez puede tener varios componentes, tales como confidencialidad, integridad, disponibilidad, costo económico.

(b) Para la determinación del riesgo debe usarse la formula riesgo (R) = impacto (I) x probabilidad (P), siendo R = I x P donde los posibles valores, tanto del impacto como de la probabilidad en un orden del número 1 hasta el 4, siendo:

- **Uno (1)** equivale a un riesgo insignificante.
- **Dos (2)** equivale a un riesgo bajo.
- **Tres (3)** equivale a un riesgo medio.
- **Cuatro (4)** equivale a un riesgo alto.

Para más información sobre la determinación del riesgo ver Anexo C. Referencia para determinar el nivel del riesgo identificado.

(c) El análisis del riesgo debe ser cuantitativo.

(i) El análisis cuantitativo puede presentar dificultades a la hora de obtener fuentes confiables y objetivas para la determinación numérica de los valores, por lo cual no puede ser tan objetivo como se puede asumir.

Sub-sección 5.02.2. Evaluación del riesgo

(a) La evaluación del riesgo debe repetirse periódicamente para tratar cualquier cambio que podría influir en los resultados de evaluación.

(b) Para los controles de seguridad de la información debe de tomarse en cuenta lo siguiente:

(i) Seleccionar controles para asegurar que los riesgos reduzcan a un nivel aceptable.

(ii) Deben existir los siguientes controles de seguridad:

a) Para protección de data y privacidad de la información.

b) Protección de los registros organizacionales.

(c) Las evaluaciones del riesgo deben identificar, cuantificar y priorizar los riesgos y los objetivos relevantes del organismo.

(i) Debe calcular la magnitud de los riesgos.

(ii) Debe realizarse periódicamente.

(iii) Deben ser metódicas para producir resultados comparables.

(iv) Tener un alcance claramente definido. Este alcance debe ser:

a) Al organismo completo.

b) Partes del organismo.

c) Un sistema de Información Individual.

(v) Cuando se utilice un alcance parcial, debe especificarse las partes o el sistema a evaluar.

Sub-sección 5.02.3. Tratamiento del riesgo

(a) Debe existir una documentación con los criterios determinados por el organismo para la aceptación o no de los riesgos.

(b) Las decisiones de aceptación o no del riesgo deben quedar registradas.

(i) El registro debe contener:

- La decisión del tratamiento del riesgo.
- El riesgo evaluado.
- Las razones de porqué se tomó la decisión.
- Los criterios tomados en cuenta.

(ii) Los resultados obtenidos de la evaluación del riesgo deben tratarse con algunas de las siguientes medidas:

- Aplicar controles para reducir el riesgo.
- Aceptar los riesgos siempre y cuando cumplan claramente con la política de criterios de aceptación de la organización.
- Evitar los riesgos sin permitir acciones que podrían causar que el riesgo ocurra.

> *Los riesgos pueden ser transferidos a organizaciones especializadas, por Ejemplo, aseguradoras u otros proveedores.*

- Los controles determinados por el organismo deben tomar en cuenta los siguientes puntos:
  - Objetivos organizacionales.
  - Requerimiento y restricciones operacionales.
  - Costo de implementación y operación.

Sub-sección 5.02.4. Plan de acción para el tratamiento de los riesgos

(a) Todo organismo debe elaborar un plan de acción.

(b) El documento debe contener los siguientes puntos:

- La relación de las acciones a realizar.
- Los recursos necesarios para llevar a cabo el plan de acción.
- El período estimado de compleción de las actividades propuestas.
- Las personas responsables de proveer los recursos.
- La forma en que se medirá la efectividad de la medida a tomar.

(c) El documento debe ser aprobado por la alta dirección y esta debe asumir el compromiso de proveer los recursos necesarios para su ejecución presupuestaria.

SECCIÓN 5.03. Entregables de la gestión de riesgo

(a) Este proceso debe entregar los siguientes documentos con su evidencia de ejecución.

- Metodología de Gestión de Riesgo.
- Tablas de apreciación de Riesgo.
- Plan de Acción para el tratamiento de los riesgos no aceptables
- Actas que validen que se completaron de los objetivos establecidos en el Plan de Acción y el porcentaje de los objetivos alcanzados.
- Posibles acciones a tomar con el propósito de completar los objetivos que no fueron satisfechos durante este período.

CAPÍTULO VI

CONTROL DE OPERACIONES

Este capítulo establece las directrices a seguir para la gestión de la seguridad web, uso de servicios web, dispositivos móviles y servicios en la nube.

SECCIÓN 6.01. Seguridad web

(a) El uso de manejadores de contenido y otras aplicaciones web debe seguir las siguientes prácticas:

(i) La selección del manejador de contenidos debe considerar la frecuencia con que dicha herramienta es actualizada por parte del fabricante, así como el historial de vulnerabilidades encontradas.

(ii) El encargado de soporte del Sistema de Manejador de Contenido[35] (CMS, por sus siglas en inglés), debe aplicar las actualizaciones y nuevas versiones luego de que estas sean evaluadas y aprobadas por el área de desarrollo e implementación de sistemas.

(iii) El uso de complementos[36] de terceros debe pasar por una evaluación del área de desarrollo e implementación de sistemas del departamento de TIC.

a) Esta evaluación debe realizarse en base a los beneficios que aporta y tener como criterios de referencia los siguientes puntos:

[35] Es una aplicación web que permite al usuario administrar contenidos de un portal, por medio de un panel de control, el cual no requiere conocimientos técnicos.

[36] También conocidos como plugins, son aplicaciones hechas para agregarle funcionalidades a otras aplicaciones, plataformas o manejadores de contenido.

- La edad del complemento.
- El historial de revisiones de versiones.
- El historial de vulnerabilidades.

(iv) Las aplicaciones web desarrolladas internamente deben identificar y documentar los requerimientos de seguridad durante la etapa de planificación y diseño para su implementación.

(v) Todas las aplicaciones web, tanto las adquiridas como las desarrolladas internamente, deben ser evaluadas por una herramienta de búsqueda de vulnerabilidades.

a) La herramienta utilizada en estas evaluaciones debe ser actualizada con frecuencia.

(vi) Toda aplicación web publicada debe pasar por una etapa de autenticación a nivel del cortafuego o proxy inverso antes de que los usuarios accedan a la misma.

(vii) Los cortafuegos a ser utilizados para la protección web deben ofrecer, y tener activadas, las funciones de protección de aplicaciones, prevención de intrusos y filtrados por país para bloquear aquellos accesos de lugares en zonas remotas del mundo que no guardan relación con la naturaleza del organismo.

(viii) Las aplicaciones web transaccionales deben ser evaluadas por un personal externo especializado con las credenciales apropiadas para este tipo de análisis.

(ix) Toda la sesión de autenticación de la aplicación web debe ser protegida con un certificado digital[37] comercial del tipo validación extendida.

a) No debe utilizase certificados autogenerado o auto firmados en cualquier aplicación web que valide credenciales.

(x) Las aplicaciones web con informaciones del organismo, deben tener una separación entre la aplicación y las bases de datos.

[37] Es un documento digital que permite garantizar la identidad de una persona en la red, a través de una firma electrónica. Se utiliza como una forma segura de garantizar la autentificación, integridad y confidencialidad de la información.

(xi) Los portales, o pantallas administrativas, de las aplicaciones web, especialmente los manejadores de contenido, solo deben ser visibles desde la red interna, no desde la Internet.

(xii) Deben recolectarse y analizarse los registros de los accesos, sean válidos o inválidos a las aplicaciones web del organismo, emitiendo informes mensuales del estado de posibles ataques que puedan estar experimentando.

(xiii) Los componentes de las aplicaciones web deben estar separados en servidores diferentes. Estando las bases de datos en una zona de seguridad diferentes y de mayor nivel de seguridad que la aplicación expuesta al público.

(b) El departamento de seguridad de información debe emitir un informe mensual con el estado de los siguientes puntos:

(i) El uso de los parchos de seguridad[38] de la aplicación web o del servidor y sus componentes mayores, tal como sucede con LAMP.

(ii) Las publicaciones de seguridad de los diferentes complementos utilizados en la solución.

(iii) Las actualizaciones de nuevas versiones de cualquiera de los componentes mencionados anteriormente.

(iv) El estado de la aplicación con relación a las listas de vulnerabilidades del Proyecto Abierto de Vulnerabilidades de Aplicaciones Web (OSWASP, por sus siglas en inglés).

Sub-sección 6.01.1. Implementación y uso de correo electrónico

(a) El correo electrónico no debe ser usado para enviar correos masivos.

(b) El correo electrónico es para el uso exclusivo de temas pertinentes al organismo gubernamental.

(c) Para la correcta implementación del correo electrónico de los organismos gubernamentales, deben seguirse las pautas establecidas en la **NORTIC A1:2014, sub-sección 7.04.3 Correo institucional.**

[38] Aplicación encargada de hacer modificaciones de seguridad a un software solucionando vulnerabilidades del mismo.

(d) Debe llevarse un registro de todos los correos entrantes o salientes.

(i) Deben mantenerse copias de seguridad de los correos independientes de si el usuario los borra.

(e) El organismo debe velar porque los usuarios no burlen los controles establecidos como medidas de seguridad por medio de renombrar archivos o cambiar las extensiones.

(f) El cifrado solo debe utilizarse bajo condiciones específicas.

(g) Los servicios de correo electrónico deben disponer de protección de correo molestoso, spam, propagación de código malicioso[39], mensajes en cadena, entre otros.

(h) El organismo se reserva el derecho de crear copias automáticas de cualquier cuenta de correo según previa autorización de la dirección.

(i) Los correos organizacionales son propiedad del organismo, y por lo tanto los usuarios no deben tratar de destruir su contenido.

(j) Todas las cuentas organizacionales deben disponer de leyendas al final del mensaje que indiquen las condiciones de uso y la responsabilidad personal del que envía en caso de no ser el contenido apropiado para el organismo.

Sub-sección 6.01.2. Protección contra código malicioso y vulnerabilidades

(a) El organismo debe disponer de las medidas administrativas y tecnológicas para la aplicación de parchos de seguridad y mejoras de los sistemas operativos, aplicaciones y servicios que se utilicen en su infraestructura.

(b) Esta gestión de las actualizaciones debe disponer de una administración centralizada que sea capaz de generar los reportes y alertas de aquellos equipos que no se encuentren actualizados.

[39] Son un conjunto de líneas programadas para ejecutar una acción con fines maliciosos.

(c) La gestión de las actualizaciones debe generar reportes regulares con el estado de actualización de los equipos, servicios, aplicaciones y sistemas operativos en la infraestructura.

(d) La gerencia de TIC del organismo debe hacer el aprovisionamiento de fondos necesarios para la actualización y programas de mantenimiento que demanden los componentes de la infraestructura.

(e) Los sistemas operativos, tanto de servidores, equipos de usuario, dispositivos en hardware[40] y otros componentes que almacenen, procesen o transmitan información deben disponer de una solución de protección contra código malicioso que ofrezca una capacidad de protección multicapas, no únicamente antivirus.

(f) Esta solución debe disponer de sistema de gestión centralizado para los equipos que así lo soporten, tales como servidores y equipos de escritorio, sin importar el sistema operativo.

(g) Los accesorios de hardware, como cortafuegos, proxy, sistemas de almacenamiento deben disponer de esta capacidad de detección y respuesta a los ataques de código malicioso.

(h) Los navegadores deben restringir el procesamiento de código de ejecución móvil y solo ser activados cuando se determine una necesidad, tal como es el caso de Java y otros sistemas de scripting.

(i) La solución de protección contra código malicioso debe disponer de su esquema de licenciamiento y mantenimiento actualizados.

(j) Debe llevarse un registro de los eventos e incidentes relacionados con contaminación de código malicioso.

(k) Los sistemas operativos deben tener habilitados la función de cortafuego, Sistema de Prevención de Intrusos[41] (IPS, por sus siglas en inglés), defensa contra código malicioso y otras herramientas según estén disponible, ya sea en el sistema operativo o en soluciones especializadas.

[40] Se refiere a todas las partes físicas o tangibles de un sistema de información.

[41] Es una tecnología que ejerce el control de acceso a una red para protegerla de ataques y abusos basados tanto en hardware como software.

(l) Las soluciones de protección contra código malicioso deben disponer de un esquema de protección basado en reputación del origen del archivo.

(m) Deben seguirse las guías del fabricante y otras guías especializadas en la configuración segura de los servicios.

(n) Deben elaborarse configuraciones base para cada una de las familias de sistemas operativos y equipos.

(o) Todos los sistemas operativos deben ser reinstalados de fuentes confiables y originales luego de ser recibidos del proveedor.

(p) Cualquier cambio de configuración en un servidor o dispositivo de hardware debe contemplarse en el plan de evaluación del riesgo. Ver **sub-sección 5.02.2 Evaluación del riesgo.**

SECCIÓN 6.02. Uso de redes inalámbricas

Los servicios de acceso a la Internet haciendo uso de las tecnologías de WIFI son una realidad en todas las aplicaciones de la vida, no obstante, existen riesgos inherentes al uso de estas tecnologías. Por tal razón se han agregados las directrices a continuación:

(a) Los riesgos de prestación de servicios Wireless deben ser gestionados tanto de manera administrativa por medio de políticas de uso aceptable o políticas específicas para el uso de WIFI como por implementaciones técnicas.

(b) Los servicios de WIFI ofrecidos por el organismo, tanto para los usuarios internos como externos, deben utilizar las últimas tecnologías disponibles tanto a nivel de la infraestructura de WIFI como de la disponibilidad en los sistemas operativos y aplicaciones actuales.

> *Esto tiene como propósito el reducir la presencia de vulnerabilidades asociadas a tecnologías ya descontinuadas como autenticación utilizando WEP, que en ningún caso puede ser utilizada en la infraestructura de organismo ni por los usuarios del organismo.*

(c) El organismo debe llevar a cabo actividades de concienciación a los usuarios y empleados, acerca del uso correcto de las tecnologías de WIFI y como protegerse de las diferentes amenazas asociadas a las mismas.

(i) Este programa de concienciación debe disponer de evidencia formal y documentada de la participación de los usuarios con objetivos establecidos a ser alcanzados mediante estas charlas y talleres.

(d) Toda implementación de WIFI debe ser evaluada y autorizada por el responsable del área TIC del organismo.

(e) Los requisitos mínimos a satisfacer con estas soluciones son las siguientes:

(i) No debe utilizarse autenticación WEP bajo ninguna circunstancia.

(ii) La autenticación debe ser individual, no utilizar claves compartidas.

(iii) Ninguna conexión al WIFI debe estar conectada directamente a la red interna.

(iv) Todas las conexiones de WIFI deben ser tratadas como externas. Estas deben ser consideradas como parte de la Internet.

(v) El acceso a los servicios internos que no estén previamente publicados a la Internet, deben hacer uso de los servicios de una Red Privada Virtual (VPN, por sus siglas en inglés).

(vi) Todos los servicios WIFI deben utilizar certificados digitales comerciales, del tipo Validación Extendida.

(vii) Los visitantes o personas externas que requieran hacer uso de los servicios de WIFI del organismo, deben solicitar los accesos por un período específico y dentro de cierto horario según se justifique.

a) Estos deben recibir una clave única para los accesos establecidos y el uso de esta facilidad será una responsabilidad del empleado que guía al visitante.

(viii) Los servicios de WIFI solo deben estar autorizados para la navegación, y esta debe tener filtros al igual que la red interna.

(ix) Los accesos a los servicios de WIFI solo deben estar permitidos durante el horario laborable.

a) Esto debe manejarse mediante clave única otorgadas para el acceso.

(x) Los servicios de WIFI deben disponer de un IPS para detectar y frenar ataques tanto a los usuarios como a otras redes.

(xi) Los nombres de las redes WIFI no deben contener el nombre del organismo, esto para no difundir información innecesaria frente a un atacante.

(xii) El uso de los servicios de WIFI debe ser monitoreado, medido, y reportado al responsable del área de TIC.

(xiii) Todo uso por no justificado, o abuso, debe contemplar consecuencias para las personas a las cuales se les ha otorgado este acceso, tanto al personal interno como el externo.

SECCIÓN 6.03. Uso dispositivos móviles

Debido a la gran penetración que la computación móvil tiene, y la tendencia al aumento de este tipo de dispositivo se hace necesario que el organismo disponga de lineamientos y herramientas para el uso de los mismos en todo lo relativo a almacenamiento, transmisión o procesamiento de la información del organismo.

(a) Todo organismo debe cumplir con los siguientes requerimientos mínimos para el uso de dispositivos móviles que guardan relación con información sensitiva:

(i) El organismo debe disponer de una evaluación de riesgo para aquellos usuarios que manejan información sensitiva en sus dispositivos, sean estos facilitados por el organismo o no. Ver **sub-sección 5.02.2 Evaluación del riesgo.**

a) El plan de acción resultante del análisis anterior debe contemplar proteger los tres elementos principales de la seguridad, que son, confidencialidad, integridad y disponibilidad en todo lo relativo al uso de dispositivos móviles.

(ii) Los dispositivos móviles deben disponer de protección contra código malicioso y amenazas.

(iii) Los dispositivos móviles deben disponer de un servicio de cifrado de los datos en caso de que el dispositivo pueda extraviarse o ser robado.

(iv) Los dispositivos móviles deben disponer de un Sistema de Gestión de Dispositivos Móviles[42] (MDM, por sus siglas en inglés), que facilite controlar aspectos críticos como el borrado en caso de robo, respaldo de los datos y detección de aplicaciones no deseadas.

(v) Los usuarios de dispositivos móviles deben notificar inmediatamente al departamento de seguridad de información cuando uno de estos equipos se extravíe.

(vi) Debe existir un proceso de borrado de los datos, así como el de restaurar los datos independientemente del dispositivo en caso de pérdida y en cada caso debe registrarse el incidente.

(vii) Los dispositivos móviles deben disponer de un programa de actualización de versiones y refrescamiento del hardware como una forma de reducir las vulnerabilidades asociadas con equipos y versiones del software que entran en obsolescencia.

(viii) Debe existir una política en la que se establezca la responsabilidad del usuario sobre no compartir ni permitir el acceso a los dispositivos móviles del organismo.

(ix) Los dispositivos nunca deben llevarse a ser reparados, modificados, o que se instalen nuevas versiones fuera de los centros autorizados del distribuidor.

(x) Cuando los dispositivos móviles hayan agotado su vida útil estos no pueden ser regalados ni transferidos a otras personas sin que antes pasen por un proceso de borrado seguro por parte del departamento TIC.

(xi) Los dispositivos móviles no deben tener instalados programas o aplicaciones de libre acceso sin que antes estos programas sean evaluados por el departamento de TIC.

[42] Es una solución que se utiliza para la admiración de dispositivos móviles, propios del organismo o del empleado, mediante la cual se pueden especificar medidas de protección para la información almacenada, procesada o transmitida por estos dispositivos, así como que cosas se pueden o no hacer con los mismos.

SECCIÓN 6.04. Servicios en la nube

Los servicios en la nube ofrecen ventajas importantes en cuanto a la disponibilidad de los servicios, abastecimiento de energía, replicación en caso de falla, disponibilidad de comunicaciones, entre otras ventajas. Sin embargo, la seguridad en estos entornos, especialmente lo relativo a la confidencialidad y la integridad, no necesariamente exceden los controles actuales en los servicios provistos por los organismos. Por tal razón los organismos deben implementar las directrices siguientes para minimizar los riesgos de seguridad en estos servicios:

Cabe señala la diferencia entre los servicios de colocación y de hospedaje, ya que en el primero se renta un espacio para colocar equipos propios del organismo, mientras que en el segundo el procesamiento y almacenamiento hacen uso de recursos del proveedor, donde toda la información siempre está en equipos y facilidades de terceros.

(a) Deben realizarse análisis de riesgo correspondiente para identificar, analizar, y evaluar las amenazas e implicaciones de poner informaciones del organismo en manos de terceros. Ver **sub-sección 5.02.2 Evaluación del riesgo.**

(b) Ninguna información, sistemas o servicios de carácter de seguridad nacional debe ser alojada en infraestructuras bajo el control administrativo de otros Estados o de proveedores que respondan a los sistemas legales de otros Estados, estén estos en el extranjero o con presencia en República Dominicana.

(c) Los organismos deben identificar las leyes o regulaciones que puedan aplicar al momento de considerar, procesar o almacenar información de los ciudadanos en dichas facilidades.

(d) Los organismos no deben depender de manera exclusiva de los servicios en la nube o de los proveedores especializados para el aprovisionamiento de servicios para el Estado.

(e) Los organismos deben hacer un análisis costo efectivo del uso de estas tecnologías para evaluar sus implicaciones económicas y viabilidad tanto a mediano como a largo plazo.

(f) Los organismos deben disponer de respaldos locales de la información y configuraciones de los servicios en la nube.

(g) Los accesos privilegiados de administración de servicios en la nube deben considerar el uso de autenticación multifactorial para que se utilice más de un criterio para la autenticación de manera que se reduzca la posibilidad de accesos no autorizados o accesos fraudulentos.

(h) Los organismos deben disponer de políticas y procedimientos para el manejo de incidentes para los casos en que ocurran brechas de seguridad.

(i) Los organismos deben implementar procedimientos regulares de gestión y eventos para la identificación de posibles tendencias a incidentes.

(j) Los organismos deben implementar servicios de cifrado en toda aquella información que esté clasificada como sensitiva.

(i) La gestión de las llaves de seguridad debe ser local.

(k) Los servicios provistos en la nube deben cumplir con los siguientes requerimientos:

- Prevención de intrusos.
- Separación entre zonas de seguridad.
- Gestión de eventos.

SECCIÓN 6.05. Gestión de activos

(a) Para llevar un control de los activos de TIC, cada organismo debe gestionar dichos activos siguiendo las directrices especificadas a continuación:

(i) Todo organismo debe realizar un inventario ordenado, completo y actualizado de todos los activos que estén bajo la responsabilidad del departamento de TIC.

a) Este inventario debe realizarse siguiendo los lineamientos establecidos en la **NORTIC A1:2014, sección 2.04 sobre inventario general de TIC.**

b) El inventario debe registrar el personal responsable de cada activo documentado.

(b) Debe existir un registro en donde se especifiquen los activos importantes. Este debe documentar las razones de la importancia de dichos activos.

(i) Tipo de activo.

(ii) El registro debe contener informaciones para la recuperación ante un desastre.

(c) El organismo debe establecer políticas de usos de los activos.

(i) El organismo debe velar porque todo el personal contratado o de terceros cumplan con las políticas de uso de los activos.

SECCIÓN 6.06. Recomendaciones para el uso de servicios wireless

- Se recomienda evitar las siguientes prácticas:
  - Esconder el Identificador de Conjuntos de Servicios[43] (SSID, por sus siglas en inglés) como medida de seguridad.
  - Filtrar equipos por la Dirección de Control de Acceso al Medio[44] (MAC Address, por sus siglas en inglés), ya que este es un tipo de identificación de fácil suplantación con un mínimo de conocimiento y experiencia.
- Auditar los servicios de WIFI por un personal externo especializado con las credenciales y/o certificaciones adecuadas para este tipo de evaluación.

[43] Es un nombre que consta con un máximo de 32 caracteres y es utilizado para identificar una red inalámbrica, este código se incluye en todos los paquetes que viajaran en la red para identificarlos como parte de ella.

[44] Es una identificación única asignada por el fabricante a los equipos que formaran parte de una red, conformada por números y letras.

GLOSARIO DE TÉRMINOS

ACUERDO DE NIVEL SERVICIO (SLA)

Es un documento que plasma los acuerdos entre un proveedor de servicio y el cliente, en donde se estipulan los requisitos y parámetros que el proveedor se compromete a cumplir para mantener unos niveles de calidad de servicio.

AMENAZA

Es un evento que puede provocar un daño o perjuicio al organismo.

ANTIVIRUS

Es un programa desarrollado con el fin de proteger un computador o servidor contra virus informáticos.

ÁREAS NO SEGURAS

Hacen referencia a los lugares no seguros dentro del organismo que solo el personal autorizado puede transitar, tomando precauciones para evitar lesiones.

ÁREAS SEGURAS

Hacen referencia a los lugares seguros dentro del organismo que los empleados y visitantes pueden transitar sin correr ningún peligro.

AUTENTICACIÓN

Es el proceso de validación que sirve para detectar y probar la identidad de una entidad.

BASES DE DATOS

Son un conjunto de datos almacenados de manera ordenada y que guardan relación entre ellos para su uso posterior.

BIT

Un bit es un dígito del sistema de numeración binario. La capacidad de almacenamiento de una memoria digital también se mide en bits.

CENTRO DE COMANDO

Es el lugar desde el cual se dirigen las actividades de recuperación de las actividades críticas de las operaciones de un organismo luego de sufrir una catástrofe.

CENTRO DE DATOS

Es un área donde se concentran y operan los equipos que conforman la infraestructura TIC que utilizan los organismos para administrar sus actividades y servicios.

CERTIFICADO DIGITAL

Es un documento digital que permite garantizar la identidad de una persona en la red, a través de una firma electrónica. Se utiliza como una forma segura de garantizar la autentificación, integridad y confidencialidad de la información.

CÓDIGO MALICIOSO

Son un conjunto de líneas programadas para ejecutar una acción con fines maliciosos.

COMPLEMENTOS

También conocidos como plugins, son aplicaciones hechas para agregarle funcionalidades a otras aplicaciones, plataformas o manejadores de contenido.

CORREO ELECTRÓNICO

Es un servicio de mensajería en red que permite el intercambio de mensajes, a través de sistemas de comunicación electrónicos.

CORTAFUEGOS

Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

DERECHO DE AUTOR

Es el conjunto de leyes y principios que provee protección a los autores, artistas y demás creadores para sus creaciones.

DIRECCIÓN DE CONTROL ACCESO AL MEDIO (MAC ADDRESS)

Es una identificación única asignada por el fabricante a los equipos que formaran parte de una red, conformada por números y letras.

DOCUMENTO DE DECLARACIÓN DE APLICABILIDAD

Hace referencia al documento que establece cuáles controles se aplicarán al organismo gubernamental en la implementación del SASI.

GESTIÓN DE RIESGO

La gestión de riesgos es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales.

HARDWARE

Se refiere a todas las partes físicas o tangibles de un sistema de información.

IDENTIFICADOR DE CONJUNTO DE SERVICIOS (SSID)

Es un nombre que consta de un máximo de 32 caracteres y es utilizado para identificar una red inalámbrica, este código se incluye en todos los paquetes que viajaran en la red para identificarlos como parte de ella.

INCIDENTE

Es cualquier funcionamiento incorrecto de cualquiera de los servicios tecnológicos.

INTÉRPRETE DE ÓRDENES SEGURA (SSH)

Es un protocolo y aplicación por el cual se accede remotamente a una computadora a través de una red de comunicaciones.

INTRANET

Es una red interna para compartir de forma segura cualquier información o aplicación y evitar que cualquier usuario de internet pueda ingresar a la red.

INVENTARIO

Es un registro organizado de los activos pertenecientes o bajo la responsabilidad de un organismo determinado.

PARCHOS DE SEGURIDAD

Aplicación encargada de hacer modificaciones de seguridad a un software solucionando vulnerabilidades del mismo

PORTAL WEB

Es un conjunto de páginas electrónicas que presentan información y recursos de interés al usuario.

PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS SEGURO (SFTP)

Este protocolo permite una serie de operaciones sobre archivos remotos.

PROTOCOLO SEGURO DE INTERNET (IPSEC)

Es un conjunto de protocolos de seguridad para proteger la comunicación IP y transmisión de paquetes en Internet.

PROXY

En una red informática, es un servidor (un programa o sistema informático), que hace de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C).

PUNTO ÚNICO DE FALLA

Se conocen como puntos únicos de falla a esos componentes únicos en una infraestructura, de manera que cuando experimentan una falla, el servicio también se ve interrumpido ya que no existe un mecanismo alterno de como continuar operando.

RED PRIVADA VIRTUAL (VPN)

Es una red virtual privada que permite de forma segura la interacción de datos sobre redes compartidas utilizando como vínculo el Internet.

RIESGO RESIDUAL

Hace referencia al riesgo que queda luego de haber tomado todas las medidas preventivas de reducción de riesgos.

SEGURIDAD DE LA CAPA DE TRANSPORTE (TLS)

Es un protocolo criptográfico que proporciona comunicación segura por una red, comúnmente Internet.

SERVIDORES

Son equipos informáticos que forman parte de una red de datos y que proveen servicios a otros equipos en dicha red, llamados clientes.

SISTEMA DE GESTIÓN DE DISPOSITIVOS MÓVILES (MDM)

Es una solución que se utiliza para la admiración de dispositivos móviles, propios del organismo o del empleado, mediante la cual se pueden especificar medidas de protección para la información almacenada, procesada o transmitida por estos dispositivos, así como que cosas se pueden o no hacer con los mismos.

SISTEMA DE PREVENCIÓN DE INTRUSOS (IPS)

Es una tecnología que ejerce el control de acceso a una red para protegerla de ataques y abusos basados tanto en hardware como software.

SISTEMA OPERATIVO

Conjunto de órdenes y programas que controlan los procesos básicos de una computadora y permiten el funcionamiento de otros programas.

SOFTWARE

Se conoce como software al equipo lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

USUARIO

Hace referencia a la persona que consume o manipula un producto, servicio o información.

VULNERABILIDAD

Hace referencia a la incapacidad de defensa frente a una amenaza.

ABREVIATURAS Y ACRÓNIMOS

No.	Abreviaturas y Acrónimos	Inglés	Español
1	BIA	Business Impact Analysis	Análisis de Impacto del Negocio
2	CD	Compact Disc	Discos Compactos
3	CONTI	N/A	Comité de Continuidad
4	DICAT	N/A	Departamento de Investigaciones de Crímenes y Delitos de Alta Tecnología
5	DRP	Disaster Recovery Plan	Plan de Recuperación de Desastres
6	DVD	Digital Versatile Disc	Discos Versátiles Digitales
7	IPS	Intrusion Prevention System	Sistema de Prevención de Intrusos
8	IPSec	Internet Protocol security	Seguridad del protocolo de Internet
9	ISO	International Organization for Standardization	Organización Internacional de Normalización
10	MAC Address	Media Access Control Address	Dirección de Control Acceso al Medio
11	MAP	N/A	Ministerio de Administración Pública
12	MDM	Master Data Management	Sistema de Gestión Centralizado

13	OPTIC	N/A	Oficina Presidencial de Tecnologías de la Información y Comunicación
14	OSWASP	Open Web Application Security Project	Proyecto Abierto de Seguridad de Aplicaciones Web
15	SASI	N/A	Sistema para la Administración de la Seguridad de la Información
16	SFTP	Secure File Transfer Protocol	Protocolo de transferencia de Archivos Seguro
17	SLA	Service Level Agreement	Acuerdo de Nivel Servicio
18	SSH	Secure Shell	Intérprete Órdenes Seguras
19	SSID	Service Set Identifier	Identificador de Conjunto de Servicios
20	TIC	N/A	Tecnología de la Información y Comunicación
21	TLS	Transport Layer Security	Seguridad de la Capa de Transporte
22	USB	Universal Serial Bus	Memorias Bus Universal en Serie
23	VPN	Virtual Private Network	Red Privada Virtual
24	WEP	Wired Equivalent Privacy	Privacidad Equivalente a Cableado

BIBLIOGRAFÍA

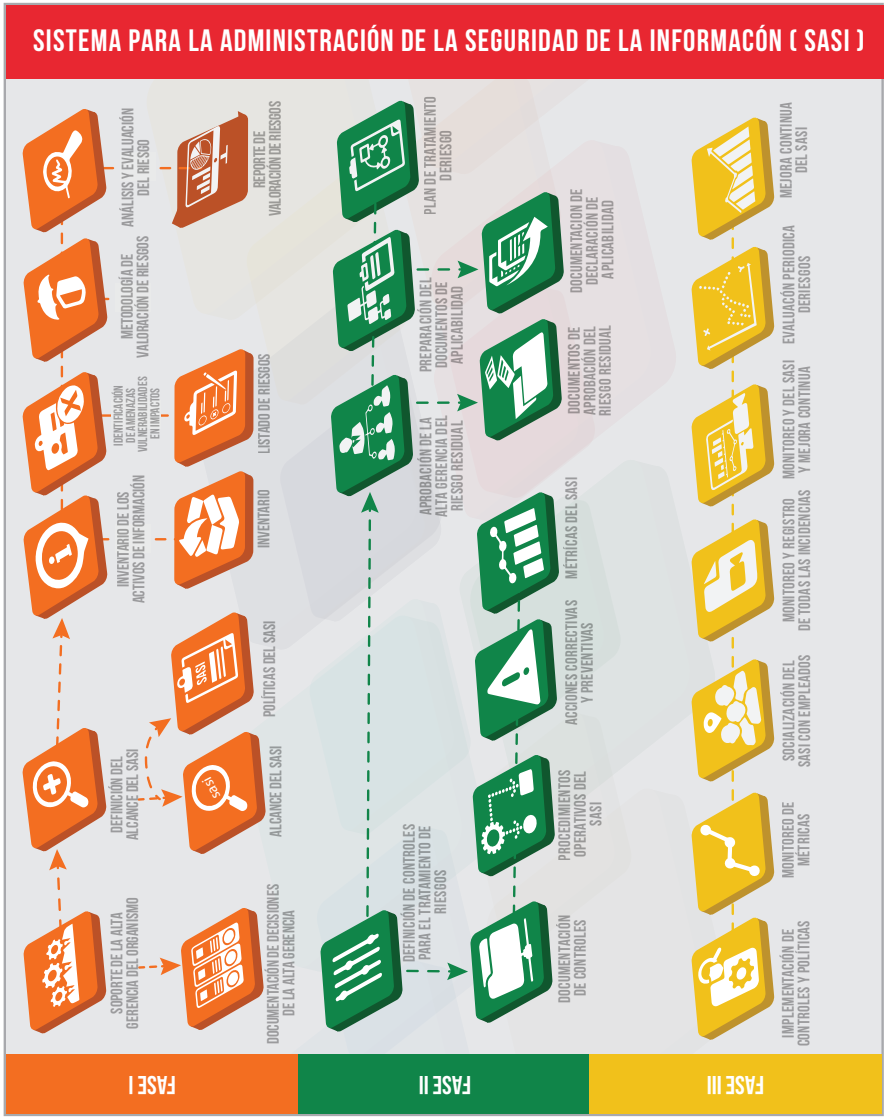
- Internationational Organization for standardization / International Electrotechnical Commission. (2005). ISO/IEC 27001. Information technology – Security techniques – Information Security managements systems – Requirements.
- Internationational Organization for standardization / International Electrotechnical Commission. (2007). ISO/IEC 27002. Information technology – Security techniques – Information Security managements systems – Code of practice for information security management.
- Internationational Organization for standardization / International Electrotechnical Commission. (2008). ISO/IEC 27005. Information technology – Security techniques – Information Security managements systems – Information security risk management.
- Internationational Organization for standardization / International Electrotechnical Commission. (2011). ISO/IEC 27035. Information technology – Security techniques – Information Security managements systems – Information security incident management.
- Internationational Organization for standardization / International Electrotechnical Commission. (2012). ISO/IEC 27032. Information technology – Security techniques – Information Security managements systems – Guideline for cybersecurity.
- Cloud Security Alliance. (2011). Security Guidance for Critical Areas of Focus in Cloud Computing v3.0. Estados Unidos.
- Dirección de Tecnologías de Información y Comunicaciones. (2007). Manual para Elaborar un plan de Continuidad de la Gestión en Tecnologías de información y Comunicaciones. Costa Rica.
- Ministerio de Hacienda y administraciones Públicas; Centro Criptológico Nacional. (2013). Guía/Norma de Seguridad delas TIC Seguridad en entornos cloud. España
- Ministerio de Industria, Turismo y Comercio Instituto Nacional de Tecnologías de la Comunicación. (2011). Guía sobre almacenamiento y borrado seguro de la Información. España

ANEXOS

Anexo A. Tipos de análisis de riesgos

Tipo de análisis	Descripción	Ventajas	Inconvenientes
Cualitativo	Basado en clasificaciones descriptivas y subjetivas del riesgo	• Sencillez • Rapidez • Equilibrio en Coste-Beneficio • Uso extendido	Subjetividad
Cuantitativo	Basado en términos monetarios	• Exactitud • Objetividad	Complejidad para estimar costes reales

Anexo B. Implementación del Sistema para la Administración de la Seguridad de la Información (SASI)



Anexo C. Referencia para determinar el nivel del riesgo identificado

4	4	8	12	16
3	3	6	9	12
2	2	4	6	8
1	1	2	3	4
	1	2	3	4

Probabilidad (P)

- Según el resultado de la multiplicación para obtener el riesgo, el mismo caerá dentro de diferentes niveles de atención como se menciona a continuación:
  - **Resultado de 1 a 6:** Riesgo bajo.
  - **Resultado de 8 a 9:** Riesgo medio.
  - **Resultado de 12 a 16:** Riesgo alto.
- Caso de ejemplo: siendo un huracán un riesgo detectado en República Dominicana, en una empresa X, le asignaremos un impacto de valor tres (3) y una probabilidad, también de valor tres (3), entonces, si multiplicamos el impacto por la probabilidad (R=IxR), tendríamos como resultado el valor nueve (9), quedando en el rango de los riesgos medios.

EQUIPO DE TRABAJO

Dirección General

Armando García, Director General

Departamento de Estandarización, Normativas y Auditoría Técnica (ENAT)

Elvyn Peguero, Gerente del ENAT

Shalem Pérez, Auditor de Estándares NORTIC

Winner Núñez, Auditor de Estándares NORTIC

Ariel Acosta, Consultor de Estándares y Normativas

Ginsy Aguilera, Consultor de Estándares y Normativas

Hamlet Durán, Analista de Estándares y Normativas

Enyer Pérez, Analista de Estándares y Normativas

Comité Interno para Evaluación de las Normas (CIEN) – Equipo OPTIC

Charli Polanco, Director de TIC

José Luis Liranzo, Director de DIGOB

Miguel Guerra, Gerente Multimedia

Comité de Estándares de Tecnologías de la Información y Comunicación (COETIC)

Ing. Reyson Lizardo

Ministerio de Administración Pública (MAP)

Ing. Jesus Morla

Ministerio de Obras Públicas y Comunicaciones (MOPC)

Carmen Mejía

Contraloría General de la República

Francis Valdez Soto
Cámara de Cuentas (CC)

Asesor
Daniel Robles, experto en TIC

Para Visualizar y descargar este documento leer este código

Av.27 de Febrero #419, Santo Domingo, R.D.
Tel.:1+ 809.286.1009 info@optic.gob.do
www.optic.gob.do www.dominicana.gob.do

OpticRD