ESTADO PLURINACIONAL DE BOLIVIA

Aduana Nacional

RESOLUCIÓN No. RA-PE-02-020-21

La Paz, 29 SEP 2021

VISTOS Y CONSIDERANDO:

Que la Constitución Política del Estado, en su Artículo 103 prevé que el Estado garantiza el desarrollo de la ciencia y la investigación científica, técnica y tecnológica en beneficio del interés general.

Que el Artículo 72 de la Ley N° 164 de 08/08/2011, Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, establece que el Estado en todos sus niveles, fomentará el acceso, uso y apropiación social de las tecnologías de información y comunicación, el despliegue y uso de infraestructura, el desarrollo de contenidos y aplicaciones, la protección de las usuarias y usuarios, la seguridad informática y de redes, como mecanismos de democratización de oportunidades para todos los sectores de la sociedad y especialmente para aquellos con menores ingresos y con necesidades especiales.

Que el Reglamento a la Ley N° 164 de 08/08/2011, para el Desarrollo de Tecnologías de Información y Comunicación, aprobado por Decreto Supremo N° 1793 de 13/11/2013, en su Artículo 3, Parágrafo VI, define a la Seguridad de la Información como la preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad.

Que el precitado Reglamento, en su Artículo 4, Parágrafo II, en cuanto a la seguridad del tratamiento de datos personales, determina que se deben implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento.

Que el Decreto Supremo N° 2514 de 09/09/2015, crea la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación — AGETIC, como una institución pública descentralizada de derecho público, con personalidad jurídica, autonomía de gestión administrativa, financiera, legal y técnica y patrimonio propio, bajo tuición del Ministerio de la Presidencia.

Que el Artículo 8 del citado Decreto Supremo, establece la creación del Centro de Gestión de Incidentes Informáticos – CGII como parte de la estructura técnico operativa de la AGETIC, entidad que establece los lineamientos para la elaboración de Planes Institucionales de Seguridad de la Información en las entidades del Sector Público.

Que mediante la Resolución Administrativa AGETIC/RA/0051/2017 de 19/09/2017 la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación — AGETIC, aprobó el documento denominado *"Lineamientos para la Elaboración de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público"*, y sus

tres Anexos, documento que enmarca las directrices para la elaboración del Plan Institucional de Seguridad de la Información de la Aduana Nacional.

Que mediante Resolución Administrativa de Presidencia Ejecutiva N° RA-PE 01-011-21 de 31/05/2021, se aprobó la nueva versión del Reglamento del Comité de Seguridad de la Información.

Que por Resolución Administrativa de Presidencia Ejecutiva N° RA-PE 01-018-21 de 01/06/2021, se aprueba la nueva versión del Plan Institucional, de Seguridad de la Información de la Aduana Nacional.

Que por Resolución Administrativa de Presidencia Ejecutiva N° RA-PE 02-011-21 de 29/06/2021, se designa a los miembros del Comité de Seguridad de la Información (CSI) de la Aduana Nacional.

Que mediante Resolución Administrativa de Presidencia Ejecutiva N° RA-PE 02-014-21 de 03/08/2021, se aprueban los Manuales de Procedimientos de Seguridad de la Información de la Aduana Nacional, en su Primera Fase.

Que el Plan Institucional de la Seguridad de la Información (PISI) tiene como objetivo establecer e implementar controles de seguridad de la información de la Aduana Nacional que permitan dar continuidad a las operaciones aduaneras y alcanzar un adecuado nivel de seguridad de la información.

CONSIDERANDO:

Que mediante Informe AN-GNSGC-I-18/2021 de 07/09/2021, la Gerencia Nacional de Sistemas, señala que conforme el cronograma del Plan Institucional de la Seguridad de la Información (PISI) se establecieron dos fases para la aprobación de los Manuales de Procedimientos, habiendo sido aprobada la Primera Fase mediante Resolución Administrativa de Presidencia Ejecutiva N° RA-PE 02-014-21 de 03/08/2021, correspondiendo la aprobación de la Segunda Fase, la cual contempla los siguientes Manuales:

1. **Manual de Procedimientos de Seguridad en las Operaciones,** que establece las formalidades de Seguridad de la Información para la gestión de cambios significativos, baja y generación de respaldos de los servidores virtuales y/o contenedores.
2. **Manual de Procedimientos de Seguridad para Controles Criptográficos,** que establece las formalidades a seguir para implementar controles criptográficos que permitan cifrar la información confidencial almacenada y transmitida por la Aduana Nacional.
3. **Manual de Procedimientos para verificación del cumplimiento de los Controles de Seguridad,** que establece las actividades a ser desarrolladas para verificar el cumplimiento de los controles de seguridad establecidos en el Plan Institucional de Seguridad de la Información de la Aduana Nacional.
4. **Manual de Procedimientos de Seguridad Física,** que establece los lineamientos para asegurar áreas e instalaciones donde se cuenta con información considerada valiosa para

la institución, con el objetivo de prevenir accesos no autorizados que comprometan la seguridad de la información.

5. **Manual de Procedimientos de Seguridad en las Comunicaciones,** que establece las formalidades que permitan garantizar una adecuada administración de la infraestructura de equipos de comunicación de la Aduana Nacional.
6. **Manual de Procedimientos de Seguridad para Contingencias Tecnológicas,** que establece las formalidades generales que permitan comprobar la recuperación de las actividades normales de los sistemas informáticos, servicios e infraestructura tecnológica, ante eventuales sucesos internos o externos que produzcan su pérdida total o parcial.

Que el referido Informe concluye que: *"En reunión del Comité de Seguridad de la Información (CSI) realizada el 30 de julio de 2021, se determinó la aprobación de los Manuales de Procedimientos de Seguridad mediante Acta de Reunión N° 03/2021 suscrita por todos sus miembros (...). Por tanto, la aprobación de los seis (6) Manuales de Procedimientos que se desprende del PISI, es viable técnicamente y se enmarca en la normativa vigente".*

Que la Gerencia Nacional Jurídica mediante Informe AN-GNJGC-DALJC-I-813-2021 de 21/09/2021, concluye que: *"En virtud a los argumentos y consideraciones legales expuestas, habiendo efectuado una revisión de los antecedentes y el Informe AN-GNSGC-I-18/2021 de 07/09/2021, emitido por la Gerencia Nacional de Sistemas, se concluye que los Manuales de Procedimientos de Seguridad en las Operaciones, Seguridad para Controles Criptográficos, Verificación del cumplimiento de los Controles de Seguridad, Seguridad Física, Seguridad en las Comunicaciones y Seguridad para Contingencias Tecnológicas; no contravienen y se ajustan a la normativa vigente, siendo necesaria su aprobación, razón por la cual, en aplicación del artículo 39 inciso h) de la Ley General de Aduanas, corresponde su aprobación por parte de Presidencia Ejecutiva, para lo cual se adjunta al presente informe el respectivo proyecto de Resolución".*

CONSIDERANDO:

Que en el marco de lo dispuesto por el Artículo 39, Inciso h) de la Ley N° 1990 de 28/07/1999, Ley General de Aduanas, es atribución de Presidencia Ejecutiva de la Aduana Nacional el dictar resoluciones en el ámbito de su competencia, para la buena marcha de la institución.

Que conforme dispone el Manual para la Elaboración de Procedimientos, aprobado mediante Resolución de Directorio N° RD-02-016-21 de fecha 31/05/2021, corresponde a Presidencia Ejecutiva de la Aduana Nacional aprobar los procedimientos de las diferentes áreas y unidades organizacionales de la Aduana Nacional.

POR TANTO:

La Presidenta Ejecutiva a.i. de la Aduana Nacional, en uso de sus facultades y atribuciones conferidas por ley;

RESUELVE:

PRIMERO.- Aprobar los siguientes Manuales de Procedimientos, elaborados en el marco del Plan Institucional de la Seguridad de la Información (PISI), que en Anexo forman parte indisoluble de la presente Resolución:

1. Manual de Procedimientos de Seguridad en las Operaciones, con Código A-S-DAS-PD18, versión 1.
2. Manual de Procedimientos de Seguridad para Controles Criptográficos, con Código A-S-DAS-PD19, versión 1.
3. Manual de Procedimientos para verificación del cumplimiento de los Controles de Seguridad, con Código A-S-DAS-PD20, versión 1.
4. Manual de Procedimientos de Seguridad Física, con Código A-S-DAS-PD21, versión 1.
5. Manual de Procedimientos de Seguridad en las Comunicaciones, con Código A-S-DAS-PD22, versión 1.
6. Manual de Procedimientos de Seguridad para Contingencias Tecnológicas, con Código A-S-DAS-PD23, versión 1.

SEGUNDO.- Los Manuales de Procedimientos aprobados en el Literal Primero de la presente Resolución, entrarán en vigencia a partir del día siguiente hábil a su publicación.

La Gerencia Nacional de Sistemas queda encargada de la ejecución y cumplimiento de la presente Resolución.

Regístrese, notifíquese y cúmplase.

Karina Liliana Serrudo Miranda
PRESIDENTA EJECUTIVA a.i.
ADUANA NACIONAL

ADUANA NACIONAL
PRESIDENCIA EJECUTIVA

G.G. Carola Caero F. A.N.

G.G.A. Dolores G. Mendoza O. A.N.

G.N.S. Marcio L. Ramos M. A.N.

G.N.J. Abigail V. Zegarra F. A.N.

D.A.L. Rosmery Quintana A. A.N.

D.A.L. Claudia A. Soto R. A.N.

PE: KLSM
GG: CCF
GNJ: AVZF/RQA/CSR
GNS: MIRM
C.C. Arch.
H.R.: DASSC2021-34/3
CATEGORIA 02

Aduana Nacional

GERENCIA NACIONAL DE SISTEMAS
DEPARTAMENTO DE ADMINISTRACIÓN DE SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN

MANUAL DE PROCEDIMIENTOS DE CONTINGENCIAS TECNOLÓGICAS
CÓDIGO: A-S-DAS-PD23 VERSIÓN 1

Índice

MANUAL DE PROCEDIMIENTOS DE SEGURIDAD PARA CONTINGENCIAS TECNOLÓGICAS

I. OBJETIVO GENERAL

Establecer las formalidades generales para probar la recuperación de las actividades normales de los sistemas informáticos, servicios e infraestructura tecnológica, ante eventuales sucesos internos o externos que produzcan su pérdida total o parcial.

II. OBJETIVOS ESPECÍFICOS

- Determinar las personas responsables de las actividades a desarrollar antes, durante y después de una caída o la no disponibilidad de los servicios o sistemas informáticos considerados críticos por la institución.
- Identificar y analizar posibles riesgos y amenazas que puedan afectar la operatividad de los servicios y sistemas informáticos considerados críticos.
- Establecer los pasos que realizará el personal del área de seguridad de la Información del Departamento de Administración de Sistemas (DAS) para la verificación del Plan de Contingencia Tecnológica que permita contar con una alta disponibilidad de los servicios y sistemas informáticos de las Aduana Nacional.

III. MARCO LEGAL

- Constitución Política del Estado Plurinacional de Bolivia.
- Ley de Administración y Control Gubernamentales, Ley N° 1178 de 20 de julio de 1990.
- Decreto Supremo N° 23318-A de 03 de noviembre de 1992, Reglamento por la Función Pública.
- Ley General de Aduanas, Ley N° 1990 de 28 de julio de 1999.
- Ley N° 164 de 08/08/2011, Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación.
- Decreto Supremo N° 2514 de 9 de septiembre de 2015 que crea la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación

(AGETIC).

- Resolución de Directorio N° RD 01-016-21 de 31 de mayo de 2021 que aprueba la nueva versión del Manual para la elaboración de Procedimientos.
- Resolución de Directorio N° RD 01-011-21 de 31 de mayo de 2021 que aprueba la nueva versión del Reglamento del Comité de Seguridad de la Información.
- Resolución Administrativa de Presidencia Ejecutiva RA-PE-01-018-21 de 01 de junio de 2021, que aprueba la nueva versión del Plan Institucional de Seguridad de la Información de la Aduana Nacional.
- Resolución Administrativa de Presidencia Ejecutiva RA-PE-02-011-21 de 29 de junio de 2021, que designa a los miembros del Comité de Seguridad de la Información (CSI) de la Aduana Nacional.
- Resolución de Directorio N° RD 02-019-21 de 21 de julio de 2021, que aprueba el Reglamento Interno de Personal de la Aduana Nacional.
- Resolución Administrativa de Presidencia Ejecutiva RA-PE-02-014-21 de 03 de agosto de 2021, que aprueba los Manuales de Procedimientos de Seguridad de la Información de la Aduana Nacional.

IV. ALCANCE

Se aplica a todos los servicios, sistemas informáticos e infraestructura tecnológica considerada crítica y administrada por la Gerencia Nacional de Sistemas (GNS) de la Aduana Nacional.

V. RESPONSABILIDAD DE LA APLICACIÓN

La ejecución y cumplimiento del presente procedimiento es responsabilidad de:

- Gerencia Nacional de Sistemas de la Aduana Nacional.
- Departamento de Servicio Tecnológico (DST).
- Departamento de Administración de Sistemas y Seguridad de la Información (DAS).
- Personal del área de Seguridad de la Información del Departamento de Administración de Sistemas y Seguridad de la Información (DAS).

VI. SANCIONES

El incumplimiento de lo establecido en el presente manual de procedimiento, será sancionado en estricta aplicación de la Ley N° 1178, Responsabilidad por la Función Pública, el Decreto Supremo N° 23318-A, Reglamento de la Responsabilidad por la Función Pública y el Reglamento Interno de Personal de la Aduana Nacional.

VII. DEFINICIONES

Activo de información: Es toda información, base de datos, sistema informático, documento o similares que tiene valor para la Aduana Nacional y debe ser protegido.

Base de Conocimientos: Es un repositorio de documentos de trabajo, guías, notas técnicas entre otros, que permite mantener la información organizada, accesible y fácil de gestionar para los diferentes equipos de trabajo de la Gerencia Nacional de Sistemas. El acceso al repositorio y su guía de usuario se encuentran publicados en Intranet → Catálogo de Sistemas → Base de Conocimientos.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Centro de Gestión de Incidentes Informáticos (CGII): Unidad dependiente de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) que establece lineamientos para la protección de activos de información y promueve la conciencia en seguridad, para prevenir y responder a incidentes de seguridad de la información.

Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

Equipos de Comunicación: Se refiere a los dispositivos que se encargan de la transmisión de datos a través de una red LAN o WAN. Su función es brindar seguridad, conmutar y enrutar el tráfico de datos, logrando la comunicación entre los equipos de usuario: Computadoras, tabletas, teléfonos inteligentes y otros similares, además de permitir el acceso a los servicios y herramientas informáticas instaladas en servidores de aplicaciones y de base de datos.

Incidente de Seguridad de la Información: Es un evento o una serie de eventos de seguridad de la información no deseados o inesperados, intento de

acceso, uso, divulgación, modificación o destrucción no autorizada de información; o una violación al Plan Institucional de Seguridad de la Información de la Aduana Nacional.

Integridad: Que la información no sea alterada por personas no autorizadas y que refleje la realidad de la información.

Personal del área de Seguridad de la Información: Es el Técnico o Profesional o Responsable de Seguridad de la información dependiente del Departamento de Administración de Sistemas y Seguridad de la Información que atiende casos de Seguridad de la Información de la Aduana Nacional.

Plan Institucional de Seguridad de la Información (PISI): Documento que establece las actividades relativas a la organización y gestión de la Seguridad de la Información en las entidades del sector público.

Plataforma de Soporte: Herramienta informática de tipo mesa de ayuda (Help Desk) que permite la generación de tickets de soporte para diferentes tipos de solicitudes. Esta herramienta y su respectiva guía de usuario se encuentran publicadas en la *Intranet* → *Catálogo de Sistemas* → *Plataforma de Soporte*.

Router: Corresponde a un dispositivo que proporciona conectividad enviando datos de una red a otra.

Responsable de Seguridad de la Información (RSI): Servidor Público responsable de gestionar, planificar, desarrollar e implementar el Plan Institucional de Seguridad de la Información.

Seguridad de la Información: Es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad.

Ticket: Es un boleto digital generado en la Plataforma de Soporte, a partir de la solicitud de asistencia de un usuario. Cada ticket tiene un tipo determinado, que define los datos que deberá registrar el usuario en su solicitud, el flujo de atención, además del personal involucrado en la misma.

UPS (Uninterrumpible Power Suply): En español Sistema de alimentación ininterrumpida (SAI), dispositivo que almacena energía eléctrica en baterías, proporciona energía de emergencia por un tiempo limitado a los dispositivos conectados ante una interrupción inesperada de energía en la red eléctrica.

VIII. DIRECTRICES DEL MANUAL DE PROCEDIMIENTOS

A. VALORACIÓN

De acuerdo a la valoración de los activos de información del Manual de Procedimientos de Gestión del inventario de activos de información, los Activos de Información identificados son valiosos, en el ámbito de una amenaza (disponibilidad, integridad y confidencialidad). Se estableció la siguiente escala para la valoración cualitativa de los Activos de Información:

Escala de Valoración	
1	Bajo
2	Medio
3	Alto

De acuerdo a lo anterior se han determinado las siguientes tablas de valoración:

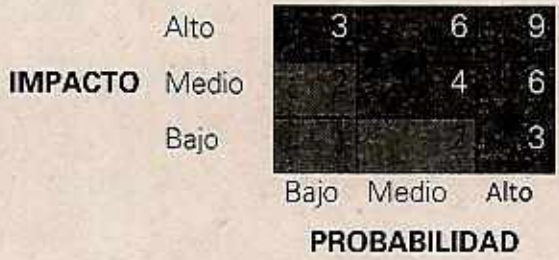
TABLA DE PROBABILIDAD DE QUE OCURRA LA AMENAZA	
VALOR	**DESCRIPCIÓN**
Bajo (1)	La amenaza se materializa a lo sumo una vez cada año o no se materializa.
Medio (2)	La amenaza se materializa a lo sumo una vez cada 3 meses.
Alto (3)	La amenaza se materializa a lo sumo una vez cada mes.

TABLA PARA ESTIMAR EL IMPACTO	
VALOR	**DESCRIPCIÓN**
Bajo (1)	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes.
Medio (2)	El daño derivado de la materialización de la amenaza tiene consecuencias que deben ser tomadas en cuenta.
Alto (3)	El daño derivado de la materialización de la amenaza tiene consecuencias graves.

CRITERIOS DE TRATAMIENTO DE RIESGO	
RANGO	**DESCRIPCIÓN**
Riesgo < 3	El riesgo es poco significativo.
Riesgo => 3	El riesgo es significativo y se debe proceder a su tratamiento.

La probabilidad y el impacto se combinan en una tabla para calcular y valorar el riesgo en una matriz de probabilidad versus impacto.

Tabla de Riesgo



B. ESTIMACIÓN DEL IMPACTO

El impacto operacional permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones de la Aduana Nacional, el impacto se puede medir utilizando un esquema de valoración, con los siguientes niveles:

Nivel A: La operación es crítica para la institución. Una operación es crítica cuando al no contar con está, la función principal de la institución no puede realizarse.

Nivel B: La operación es una parte integral de la institución, sin esta no podría operar normalmente, pero la función es crítica.

Nivel C: La operación no es una parte integral de la institución.

Se debe tener en cuenta la tolerancia a fallas por horas, cuya propiedad permite que un sistema pueda seguir operando normalmente a pesar de que una falla haya ocurrido en alguno de los componentes del sistema.

C. ESTABLECIMIENTO DE TIEMPOS DE RECUPERACIÓN

Con base a la clasificación y evaluación de los impactos operacionales de las organizaciones para lo cual se contempla:

Tiempo de Recuperación	Descripción
RPO	Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que pueda tolerar un proceso de la institución.
RTO	Tiempo disponible para recuperar sistemas y/o recursos que han

	sufrido una alteración.
WRT	Tiempo disponible para recuperar datos perdidos una vez que los sistemas están reparados. Tiempo de recuperación de trabajo.
MTD	Periodo máximo de tiempo de inactividad que puede tolerar la entidad sin entrar en colapso.

D. ANÁLISIS DE AMENAZAS

Se ha determinado que existen amenazas que podrían afectar la operación normal del Centro de Procesamiento de Datos (CPD) de la Aduana Nacional y causar serios problemas y riesgos a los sistemas informáticos, infraestructura tecnológica y servicios de la institución. Se han definido como posibles amenazas a las siguientes:

	Amenaza	Detalle
1	**Acceso no autorizado**	Vulneración de sistemas de seguridad instalados, ingreso no autorizado físicamente a las instalaciones del CPD. Acceso a Servidores de infraestructura tecnológica (servidores de bases de datos, de correo electrónico, equipos de comunicaciones, equipos de red, servidores de telefonía, otros). Infección o ataque con Ransomware Sabotaje Intromisión por curiosidad, descuido.
2	**Desastres naturales o proximidad de peligro**	Inundaciones o terremotos La zona donde está ubicado el CPD principal tiene cercanía a oficinas que puede ser objeto de bloqueos e imposibilitar el acceso físico a las instalaciones de la Aduana Nacional.
3	**Fallas en los equipos de soporte**	Todos los equipos informáticos hacen uso de energía eléctrica regulada, por lo que su ausencia conduce directamente a una inoperatividad de los mismos, los generadores tienen un tiempo específico de horas de funcionamiento. Equipo Climatizadores (aire acondicionado), los cuales cuentan con un tiempo de funcionamiento de más de 5 años, por lo cual ya cumplieron su ciclo de vida. Se hace uso de empresas ISP para el servicio de Internet, por lo cual, podrían presentarse problemas en el enlace de comunicaciones por parte del proveedor. Falla en los equipos hardware/software que forman parte de la red de datos interna de comunicación (core switches, routers de

		borde, otros).
4	**Personal de Administración**	Administrador de redes comunicaciones. Administrador de energía y climatización. Administrador de Servicios Tecnológicos. Administrador de Base de Datos. Sobre los cuales existe riesgo de accidente, enfermedad, renuncia, abandono de puesto de trabajo, otros.
5	**Fallas de Hardware /Software**	Todos los equipos de procesamientos de datos e infraestructura tecnológica están sujetos como cualquier hardware a posibles fallas en: discos duros, tarjetas madre, puertos, transceiver, fuentes entre otros accesorios. Situación fortuita que imposibilite el acceso a sistemas de Gestión Aduanera, servicios de internet, correo electrónico, portales institucionales entre otros.

E. CLASIFICACIÓN DE INTERRUPCIONES Y NIVEL DE AFECTACIÓN

Los incidentes que pasan a ser tratados dentro del Plan de Contingencia Tecnológica serán evaluados en base al impacto que tiene sobre la prestación del servicio tecnológico de la Aduana Nacional, de acuerdo a la siguiente clasificación:

Tipo de Interrupción	Características	Ejemplos	Respuesta
[redacted]	Evento que inhabilita el centro de procesamiento de datos para prestar sus servicios. No permite que el personal de infraestructura tecnológica trabaje de forma física en las instalaciones de la institución.	Terremoto. Incendio general. Guerra Civil. Convulsión social. Fallo eléctrico permanente.	Comunicar en la prensa la baja de los sistemas informáticos.
PARCIAL	Evento que afecta a más de un recurso informático de manera drástica ocasionando la suspensión parcial del funcionamiento del hardware o software considerados como críticos.	Fallas técnicas en equipos servidores que alojan sistemas de Gestión Aduanera o sus bases de datos. Fallas técnicas en equipos de red del	Actividades de contingencia descritas en el Manual de Procedimientos de Contingencia de Servidores.

		Centro de procesamiento de datos.	
[redacted]	Evento que afecta puntualmente un recurso necesario para la prestación de los servicios de Informática	Inconsistencia técnica de una Base de Datos que aloja un sistema o servicio Ausencia de personal clave.	Actividades de contingencia descritas en el Manual de Procedimientos de Contingencias de Base de Datos.

IX. DESCRIPCIÓN DEL MANUAL DE PROCEDIMIENTOS

A. VERIFICACIÓN DEL PLAN DE CONTINGENCIAS

1. Directrices del Procedimiento

1.1. Periodicidad

La periodicidad del presente procedimiento es trimestral.

1.2. Generación automática de tickets

El área de seguridad del DAS genera automáticamente la última semana cada 3 meses un ticket del tipo "Verificación Plan Contingencias" en la Plataforma de Soporte.

1.3. Planes de Contingencia

El DST debe contar mínimamente con los siguientes planes de Contingencia Tecnológica:

a) Plan de Contingencia del sistema de energía eléctrica del CPD.

b) Plan de Contingencia para recuperación de Sistemas Informáticos y Bases de Datos de Producción.

c) Plan de Contingencia del sistema de respaldo y recuperación de servidores virtuales y/o contenedores.

d) Plan de Contingencia para fallas en equipos críticos del Centro de Procesamiento de Datos.

1.4. Guía de Verificación del Planes de Contingencia Tecnológica

La Guía de verificación de los Planes de Contingencia Tecnológica de la infraestructura institucional, se encuentra se encuentra en la Base de Conocimientos *GNS → DAS → Seguridad de la Información.*

2. Descripción de Actividades

Nº	Actividad	Responsable	Tareas
1	Creación del ticket	Responsable de Seguridad de la Información	**1.1.** Ingresa a la Plataforma de Soporte y busca un nuevo ticket de tipo *Gerencia Nacional de Sistemas → Seguridad de la Información →* Pruebas Plan Contingencia. **1.2.** Llena los campos solicitados en la Plataforma de Soporte. **1.3.** Crea el ticket y elabora una propuesta de verificación del Plan de Contingencia Tecnológica, considerando como referencia lo siguiente: • Pruebas de suministro de energía eléctrica con UPS. (Corte del servicio de energía y verificación de la entrada de las UPS en funcionamiento). • Prueba del canal principal de Internet y verificación que el canal secundario sigue en conexión (si existe redundancia de ISP). • Puesta en producción como mínimo de un equipo de respaldo y sistemas de información de la Aduana Nacional. • Recuperación de la información, como mínimo una copia de respaldo de información, para verificar su correcto proceso de restauración (de acuerdo a lo descrito en el Manual de Procedimientos de Seguridad en las Operaciones).
2	Elaboración de cronograma de pruebas	Responsable de Seguridad de la Información	**2.1.** Elabora una propuesta de cronograma del plan de pruebas, en horarios preferentemente fuera de oficina. **2.2.** Deriva el ticket al Jefe del Departamento de Servicio Tecnológico.
3	Revisión y autorización	Jefe del Departamento de Servicio Tecnológico.	**3.1.** Revisa los tickets asignados a su persona y busca uno de tipo *Pruebas Plan Contingencia.* **3.2.** Revisa la propuesta de pruebas del plan de contingencia propuesto por el área de seguridad y su cronograma. **Si tiene observaciones:** **3.3.** Devuelve el ticket a través de la Plataforma de Soporte con las observaciones para su corrección.

Nº	Actividad	Responsable	Tareas
			3.4. Continúa en la *tarea 1.3.* **Si NO tiene observaciones:** **3.5.** Autoriza la realización de las pruebas del Plan de Contingencia, en la fecha y hora propuesta en el cronograma. **3.6.** Devuelve el ticket al área de seguridad de la información.
3	Ejecución de pruebas	Personal del área de Seguridad de la Información	**4.1.** Genera tickets en la Plataforma de Soporte para cada prueba del tipo Pruebas de Contingencias **4.2.** Procede a realizar las pruebas del Plan de Contingencias de acuerdo a lo establecido en el ticket generado coordinando con el personal del DST. **Si las pruebas resultaron de forma satisfactoria:** **4.3.** Registra un resumen de las acciones realizadas para la ejecución de las pruebas al plan de contingencia, en la Plataforma de Soporte. **4.4.** Continúa en la *tarea 4.1.* **Si las pruebas no fueron satisfactorias:** **4.5.** Continúa en la tarea 3.2.
4	Generación de Informe	RSI	**5.1.** Realiza un informe con todos los detalles de las pruebas realizadas. **5.2.** Remite el informe a Jefatura del DAS, DST y Gerencia de la GNS. **5.3.** Cierra el ticket en la Plataforma de Soporte.

X. HISTORIAL DE CAMBIOS

Revisión Revisada	Descripción de los Cambios	Fecha de Aprobación
	Edición Inicial	

XI. ANEXOS

No Aplica