


Universidad Cenfotec Maestría en Ciberseguridad

Documento Final de Proyecto de Investigación Aplicada 2

# Plan de Contingencia para el Departamento de Tecnologías Informáticas del Instituto Meteorológico Nacional

Lemus Obando Bryan

Herrera Herrera Patricia

Diciembre 2017

## Declaratoria de derechos de autor

La reproducción o consulta del presente proyecto quedará en completa confidencialidad, con un periodo mínimo de tres años, esto en acuerdo con el IMN, ya que algunos de los datos publicados para el desarrollo del mismo, son importantes y darlos a conocer al público podrá poner en riesgo al instituto. Una vez pasado el tiempo considerado por los interesados la documentación del proyecto puede ser público únicamente para la consulta o apoyo de otras investigaciones, siempre y cuando sean con fines académicos.

Por otra parte, una vez cumplido el periodo de confidencial, se prohíbe la reproducción parcial o total del documento como tal.

La siguiente carta detalla los términos de confidencialidad, así como el acuerdo entre las partes involucradas.

## Agradecimientos y dedicatorias

El presente proyecto lo dedicamos a los miembros de nuestras familias, por todo el apoyo que recibimos a lo largo de nuestra carrera y aún más, en la conclusión de esta etapa tan importante en nuestras vidas.

De igual forma les agradecemos a los miembros del IMN, por toda la colaboración que nos brindaron y por permitirnos realizar el proyecto en esta institución tan importante.

No dejamos de lado a Dios, que es el que nos brinda la inteligencia, fuerza y nos permite levantarnos cada uno de nuestros días para realizar las actividades diarias de nuestra vida.

A nuestro profesor tutor, le agradecemos todo su apoyo, dedicación y conocimiento que nos brindó a lo largo de la carrera y más que todo, con la conclusión del proyecto.

Por todos estos motivos, les dedicamos el proyecto a las personas que ya mencionamos, no tenemos las palabras para expresarles nuestra gratitud y todo el apoyo brindado a lo largo de esta etapa.

Hoja de aprobación

## Tabla de Contenidos


Introducción ..... 8
Planteamiento del Problema ..... 9
Formulación del Problema ..... 10
Objetivos ..... 10
General ..... 10
Específicos ..... 10
Alcance ..... 11
Marco Teórico ..... 12
Seguridad de la Información ..... 12
1. Análisis de Riesgos ..... 13
I Etapa: Identificación del Riesgo ..... 15
II Etapa: Valoración del Riesgo ..... 15
III Etapa: Administración del Riesgo ..... 18
2. Análisis de Impacto ..... 19
3. Plan de Contingencia del Negocio ..... 21
Marco Contextual ..... 22
Instituto Meteorológico Nacional ..... 22
Reseña Histórica ..... 23
Misión ..... 24
Visión ..... 24
Estructura Organizativa ..... 25
Investigación Aplicada ..... 26
1. Análisis de Riesgos ..... 29
I Etapa: Identificación del Riesgo ..... 29
II Etapa: Valoración del Riesgo ..... 32
III Etapa: Administración del Riesgo ..... 33
2. Análisis de Impacto ..... 34
3. Plan de Contingencia ..... 36
Plan de Atención de Incidentes ..... 44
Conclusiones ..... 46
Recomendaciones ..... 47
Glosario ..... 48
Bibliografía ..... 51

Anexos ..... 53
Apéndice ..... 62

## Lista de Tablas

Tabla 1. Categorización de Frecuencia ..... 16
Tabla 2. Categorización de Consecuencia ..... 16
Tabla 3. Criterios de aceptación del Riesgo ..... 18
Tabla 4. Servidores Críticos ..... 26
Tabla 5. Servidores Criticidad Media ..... 27
Tabla 6. Servidores baja criticidad ..... 28
Tabla 7. Infraestructura de red y alimentación eléctrica ..... 28
Tabla 8. Categorización de Riesgo ..... 30
Tabla 9. Continuación, Categorización de Riesgos ..... 31
Tabla 10. Actividades Críticas ..... 35
Tabla 11. Plan de Contingencia ..... 43
Tabla 12. Plan de Atención a Incidentes ..... 45

## Lista de Figuras

Figura 1: Estructura de SEVRI ..... 14
Figura 2. Vinculación Frecuencia – Consecuencia ..... 17
Figura 3. RPO – RTO ..... 20
Figura 4. Estructura Organizativa ..... 25

# Introducción

El Plan de Continuidad del Negocio es una herramienta que prepara a cualquier tipo de organización, independientemente de su objetivo de negocio, para enfrentar alguna eventualidad que se presente. Este plan posibilita la continuación de las operaciones en la empresa o institución que sea implementado. Luego de que una posible amenaza se materialice y afecte la continuidad del negocio, la puesta en marcha del mismo toma en cuenta elementos referentes a los sistemas de información, equipos, infraestructura, personal, servicios y otros, con el principal propósito de minimizar eventuales repercusiones ante situaciones adversas. Además de esto, contempla los lineamientos de la administración de la institución y el desarrollo de fases que componen el plan de continuidad y las metodologías definidas para su ejecución, como también la identificación de riesgos, su impacto en las operaciones y, por supuesto, el desarrollo de los planes de contingencia, que se realizan de acuerdo con las prioridades de la institución.

Como parte de este proyecto, el propósito de su enfoque es realizar un análisis detallado de cada una de las fases anteriormente mencionadas, identificando los posibles riesgos y amenazas que atenten contra el normal funcionamiento de las principales tareas del Instituto Meteorológico Nacional (IMN) en su Departamento de Informática. Por otra parte, pero sin desviar el propósito, se indaga acerca del impacto al que el negocio puede verse expuesto, principalmente en el Departamento de Informática, si alguna amenaza llega a materializarse ocasionando pérdidas, tanto monetarias como de datos. Como parte final, pero no menos importante, se brinda un plan de seguimiento luego de que ocurra el incidente inesperado, reanudando las operaciones sin mayores problemas y con el menor impacto posible.

El presente proyecto es aplicable única y exclusivamente al IMN en su Departamento de Informática, por consiguiente, los resultados de este análisis, y los resultados propuestos, le competen solo a dicha institución. Cada una de las fases es valorada por parte de su personal y los procedimientos, métodos o modelos aplicados para lograr los resultados son de entero acuerdo entre las partes interesadas.

## Planteamiento del Problema

El IMN tiene, hoy en día, la necesidad de valorar sus riesgos y gestionar cualquier tipo de incidente que llegue a ocurrir en el Departamento de Informática, donde no se cuenta con un sistema de seguridad de la información que permita realizar el respectivo análisis de riesgos que ayude a identificar todos los puntos débiles de la institución, en términos de seguridad de los datos. No se cuenta con un proceso definido que reduzca la amenaza de que se comprometan los tres pilares de la seguridad de la información: integridad, confidencialidad y disponibilidad.

Desafortunadamente, el IMN no cuenta con un proceso de gestión de riesgos que les permita identificar las amenazas a las cuales pueden estar expuestos, tanto los equipos de cómputo, meteorológicos como los sistemas de información. El proceso comprende aplicar medidas de seguridad para proteger y estar preparados para afrontar contingencias y desastres de diversos tipos que comprometan el funcionamiento del departamento de informática y la institución en sí.

Se consideran fases como el análisis de impacto de negocio, donde se identifican los procesos críticos para el buen funcionamiento del Instituto. Una vez que estos se hayan identificado, se analizarán los riesgos asociados a dichos procesos para determinar cuáles serían las causas potenciales que puedan llegar a interrumpir el funcionamiento adecuado del Departamento de Informática.

Este análisis de impacto permitirá a la institución identificar los procesos que poseen tiempo critico de recuperación en caso de falla, por lo que también se definirán parámetros como el RTO que permite identificar el periodo de tiempo permitido para la recuperación de cualquier función afectada. También el RPO, que identifica la antigüedad de los datos para su posterior recuperación, básicamente le permitirá al instituto determinar la tolerancia que podrían permitir para operar con datos adquiridos de respaldos.

Estableciendo procesos y parámetros como los mencionados, se le permitirá al IMN tener procedimientos óptimos para actuar en caso de que el funcionamiento de la institución se vea comprometido ante cualquier falla en los dispositivos informáticos, meteorológicos y sistemas de información.

## Formulación del Problema

¿Cómo identificar y gestionar los riesgos que afectan la seguridad de la información del Instituto Meteorológico Nacional, con el fin de definir e implementar un Plan de Continuidad para el Departamento de Informática?

## Objetivos

### Objetivo General

Proponer un plan de continuidad del negocio para el Departamento de Informática del Instituto Meteorológico Nacional; mediante acciones y procedimientos que se deben ejecutar en caso de fallas, que garantice la continuidad de las operaciones de los elementos considerados como críticos.

### Específicos

1. Identificar amenazas de orden natural, operacional o exógenos, asociadas a procesos o actividades relacionadas con el negocio, que puedan afectar eventualmente a la continuidad de cualquier proceso en el Departamento de Informática y afectar sus objetivos.
2. Establecer un manual de procedimientos formales que indique las acciones que se deben seguir para afrontar con éxito un incidente o emergencia, de tal manera que cause el menor impacto.
3. Generar un plan de respuesta que muestre diferentes estrategias definidas por procedimientos, recursos e instrumentos necesarios para la prevención, control y atención de los riesgos identificados que garantice razonablemente la continuidad de las operaciones.
4. Definir los responsables de la respuesta inmediata ante la ocurrencia de eventualidades, para que tome acciones de control, notificación y comunicación permanente, así como de capacitación del personal para ejecutar cualquier procedimiento.
5. Calcular la valoración del riesgo a partir de la frecuencia y la consecuencia de cualquier amenaza latente para el Departamento de Informática.

## Alcance

Este proyecto comprende la propuesta de implementación de un plan de continuidad del negocio para el Departamento de Informática del Instituto Meteorológico Nacional, el cual será sometido a diferentes análisis. Como parte de la primera etapa se aplica un análisis de riesgos, definiendo cada uno de sus activos y un universo de riesgos los cuales serán clasificados y valorados dependiendo de su frecuencia y consecuencia para el negocio. Como segunda etapa se aplica el análisis de impacto (BIA) y por último, el plan de continuidad del negocio en el mencionado Departamento.

# Marco Teórico

## Seguridad de la Información

La norma ISO 27001 define la seguridad de la información como la preservación de la confidencialidad, la integridad y la disponibilidad de la información. Además, puede involucrar otras propiedades tales como autenticidad, trazabilidad, no repudio y fiabilidad.

### Pilares de seguridad de la información

Para alcanzar los objetivos descritos por la seguridad de la información, dentro del proceso de gestión de la seguridad informática es necesario contemplar una serie de servicios o funciones:

a) **Confidencialidad**: mediante esta función de seguridad se garantiza que cada mensaje transmitido o almacenado en un sistema informático solo podrá ser leído por su legítimo destinatario. Si dicho mensaje cae en manos de terceras personas, estas no podrán acceder al contenido del mensaje original: Por lo tanto, este servicio pretende garantizar la confidencialidad de los datos almacenados en un equipo, de los datos guardados en dispositivos de respaldo y/o de los datos transmitidos a través de redes de comunicaciones.
b) **Integridad**: la función de integridad se encarga de garantizar que un mensaje o archivo no haya sido modificado desde su creación o durante su transmisión a través de una red informática.
c) **Disponibilidad**: la disponibilidad del sistema informático también es una cuestión de especial importancia para garantizar el cumplimiento de sus objetivos. Lo anterior por cuanto se debe diseñar un sistema lo suficientemente robusto frente a ataques e interferencias como para garantizar su correcto funcionamiento, de manera que pueda estar permanentemente a disposición de los usuarios que deseen acceder de sus servicios.

La mención de estos tres pilares es de suma importancia ya que en torno a ellos se establecieron los objetivos de esta investigación para brindar una mayor y mejor solución de seguridad para el IMN.

Seguidamente se explica, con un poco más de detalle, cada una de las etapas o procedimientos que están establecidos para completar el Plan de Continuidad de Negocio, el

cual es el principal objetivo de este estudio. Cada una de ellas se encuentra acoplada al cumplimiento de distintos modelos con el fin de la obtención de resultados.

# 1. Análisis de Riesgos

Antes de definir que es el análisis de riesgos, se tiene que considerar lo que es un riesgo, el cual puede ser definido, según la ISO 27000, como la "*posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias*". (PriteshGupta.com, 2005)

Ahora bien, el proceso de análisis de riesgos debe ser el más importante de la gestión de la seguridad de la información de una organización, de aquí parte su gestión de riesgos, que es el proceso en donde se decide qué hacer con el riesgo, dependiendo de la posición actual de la empresa. Dentro de las posibles soluciones estos se pueden eliminar, aceptar, transferir o controlar. La forma en que se aplica la gestión de riesgos se basada en la compleja tarea de determinar, analizar, evaluar y clasificar los activos de información más importantes según la criticidad de los mismos. A nivel general, se debe tener claro el objetivo del análisis de riesgo estableciendo a su vez una escala para dar valor a cada riesgo, dependiendo de su frecuencia y consecuencia.

Para efectos del desarrollo de esta investigación, se hará con base en la metodología propuesta por la UNA, conocida como SERVI. Esta propone tres diferentes etapas para poder gestionar cada uno de los riesgos identificados. Adicionalmente, se debe presentar un informe general de todos los hallazgos, en el cual se identifiquen los riesgos y seleccionen las medidas de control para evitar la materialización de los mismos. El informe se presenta de forma detallada y con sus respectivas recomendaciones a la Junta Administrativa para la toma de decisiones.

### Metodología de Análisis de Riesgos SEVRI

Las metodologías son desarrolladas para la identificación de la falta de controles y el establecimiento de un plan de contramedidas. Existen dos tipos: Las cuantitativas y las cualitativas. Para efectos dl presente proyecto se adoptará el SEVRI (Sistema Específico de Valoración de Riesgos) creado por la UNA, el cual se concibe como un método que permite identificar, valorar y administrar los riesgos asociados con el cumplimiento de los objetivos institucionales. Para llegar al fin propuesto las siguientes etapas serán tomadas en cuenta para cumplir con la mitigación y el efecto que pueda ocasionar cualquier riesgo identificado:

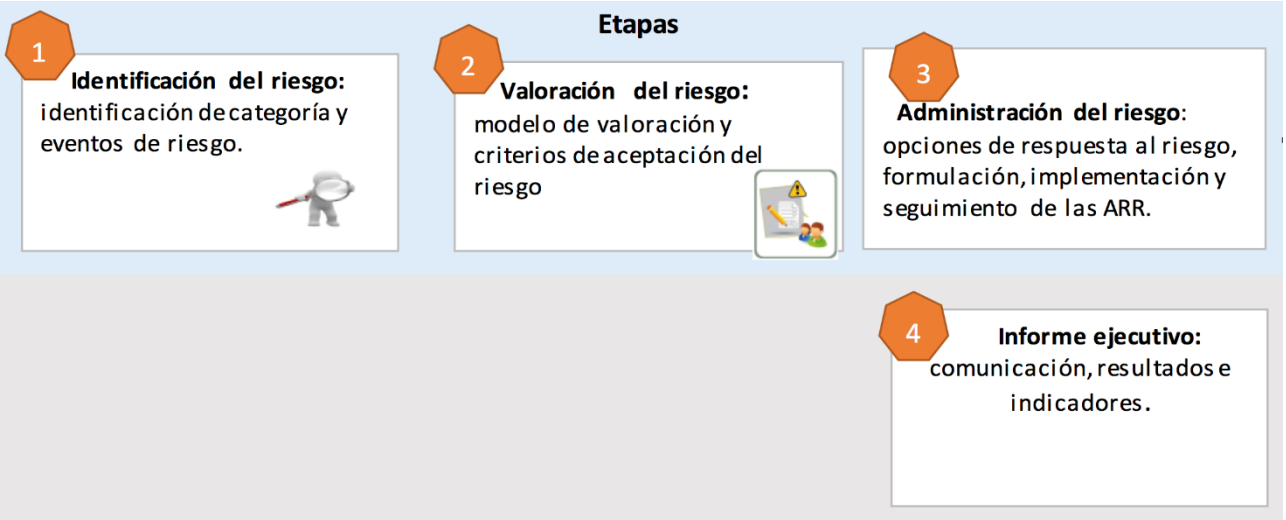



Figura 1: Estructura de SERVRI

Fuente: tomada de la Metodología Sevri_UNA 2017, referencia (UNA, 2017)

Con el seguimiento de estas etapas, al finalizar se podrán obtener los distintos riesgos encontrados. Además, se identificará su categorización y una detallada administración del riesgo, interponiendo las contramedidas para aceptar, evitar, reducir o compartir el mismo, según las decisiones de la alta administración. Más adelante, en este mismo documento, se encuentra la aplicación de este proceso en la institución.

## I Etapa: Identificación del Riesgo

En la siguiente fase se realiza la gestión de los riesgos, por lo cual se necesita de la creación de un portafolio de riesgos en el cual se definen sus respectivas categorías y eventos que pueden afectar el cumplimiento de los objetivos de la institución.

**Portafolio de Objetivos**

El portafolio de objetivos comprende aquellos procesos que se deben cumplir, plasmados en objetivos concretos para garantizar que el departamento de TI esté cumpliendo con las necesidades del negocio. A estos mismos se aplica una gestión de riesgos para priorizarlos de manera que todos sean atendidos de manera óptima.

**Portafolio de Riesgos**

Luego de varias reuniones y explicaciones por parte del personal y encargados del departamento de informática para comprender las necesidades del instituto y como parte de la identificación de los riesgos a los que se ve afectado el IMN hoy en día, y después de un exhaustivo análisis, se realiza la categorización de diferentes tipos de amenazas que podrían interferir en el cumplimiento de los objetivos institucionales.

## II Etapa: Valoración del Riesgo

Una vez identificados los riesgos se debe aplicar el siguiente modelo:

**Modelo de Valoración de Riesgos**

Con la aplicación de este modelo se puede obtener el resultado del riesgo inherente y residual relacionado a cada uno de los eventos identificados. El objetivo primordial de la valoración del riesgo es poder tomar las decisiones adecuadas en cada caso particular, permitiendo dar una respuesta ante la magnitud del riesgo y de qué forma se puede administrar.

Para efectos de este proyecto y de forma conjunta con los encargados del Departamento de TI del Instituto, se toma el acuerdo de utilizar una matriz de dos dimensiones (frecuencia por consecuencia). Para medir el riesgo inherente que produce un arreglo matricial de 5 x 5, a este se le asignan valores para poder medir la frecuencia con que un evento puede ocurrir. De igual forma la consecuencia consta de una puntuación definida por cumplimiento de las metas de la institución en caso de que una vulnerabilidad se materialice. Para esta primera calificación se

deben utilizar como referencia las siguientes definiciones, relacionadas con la forma de medir la frecuencia y la consecuencia con que se puede producir un evento.

### Categorización de Frecuencia

Respecto a la frecuencia, un evento puede ocurrir según se muestra en la siguiente tabla, con la categorización que debe utilizarse como referencia para asignar la calificación correspondiente:

| Frecuencia | Valor | Criterio |
|---|---|---|
| Excepcional | 1 | El evento podría ocurrir con una periodicidad superior a los 5 años. |
| Esporádica | 2 | El evento podría ocurrir al menos una vez cada 5 años. |
| Moderada | 3 | El evento podría ocurrir una vez cada año |
| Frecuente | 4 | El evento podría ocurrir en forma recurrente, una vez por semestre. |
| Constante | 5 | El evento podría ocurrir al menos una vez por mes. |

Tabla 1. Categorización de Frecuencia

Fuente: tomada de la Metodología Sevri_UNA 2017, referencia (UNA, 2017)

### Categorización de Consecuencias

Las alternativas seleccionadas, para medir el impacto negativo que podría provocar un evento sobre el logro de una meta de la institución, se presentan en la siguiente tabla:

| Frecuencia | Valor | Criterio |
|---|---|---|
| Insignificante | 1 | Se estima que la materialización del evento afectaría en menos de un 10% el logro de la meta de la institución. |
| Menor | 2 | Se estima que la materialización del evento afectaría entre un 10% y menos de un 20% el logro de meta de la institución. |
| Significativa | 3 | Se estima que la materialización del evento afectaría entre un 20% y menos de un 30% el logro de meta de la institución |
| Mayor | 4 | Se estima que la materialización del evento afectaría entre un 30% y menos de un 50% el logro de meta de la institución |
| Catastrófica | 5 | Se estima que la materialización del evento afectaría en 50% o más el logro de meta de la institución |

Tabla 2. Categorización de Consecuencia

Fuente: tomada de la Metodología Sevri_UNA 2017, referencia (UNA, 2017)

La vinculación entre las dos tablas se hace por medio de la multiplicación de los valores asignados a la frecuencia y la consecuencia del evento.

| | | | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| | | | Consecuencia | | | | |
| | | | Insignificante | Menor | Significativa | Mayor | Catastrófica |
| 1 | Frecuencia | Excepcional | 1 | 2 | 3 | 4 | 5 |
| 2 | | Esporádica | 2 | 4 | 6 | 8 | 10 |
| 3 | | Moderada | 3 | 6 | 9 | 12 | 15 |
| 4 | | Frecuente | 4 | 8 | 12 | 16 | 20 |
| 5 | | Constante | 5 | 10 | 15 | 20 | 25 |

Figura 2. Vinculación Frecuencia – Consecuencia

Fuente: tomada de la Metodología Sevri_UNA 2017, referencia (UNA, 2017)

La primera fila y la primera columna de la tabla muestran los valores asignados a las diferentes categorías (valores del 1 al 5), mientras que las celdas o casillas sin ningún tipo de sombreado, muestran el producto de multiplicar la frecuencia por la correspondiente consecuencia (valores del 1 al 25).

En este modelo de 5 x 5, el escenario que presenta el nivel más alto de riesgo inherente, con una frecuencia constante y una consecuencia catastrófica, produce un valor de 25.

## III Etapa: Administración del Riesgo

**Criterios de Aceptación de Riesgo:**

El modelo aplicado a este proyecto tiene como propósito primordial el cumplimiento de los objetivos estratégicos del Departamento de TI ya anteriormente mencionados. Es por este motivo que al realizar la valoración de riesgos, lo que es equivalente a la aplicación de la tabla anterior, se obtiene una calificación para el riesgo residual. Este ayuda a determinar si el riesgo resultante se encuentra en un rango aceptable, definido por la institución, o no.

Luego de este cálculo, se ubican los resultados de acuerdo con los criterios o los niveles de aceptación del riesgo, según se especifica en la siguiente tabla:

| Nivel de riesgo | Rango | Administración del riesgo |
|---|---|---|
| Aceptable | Riesgo residual menor o igual que 15% | Se da por concluido el proceso de gestión de riesgos. |
| Bajo | Riesgo residual mayor que 15% y menor o igual que 25% | Se pasa al siguiente nivel, que consiste en definir las opciones de respuesta al riesgo. |
| Medio | Riesgo residual mayor que 25% y menor o igual que 40% | Se pasa al siguiente nivel, que consiste en definir las opciones de respuesta al riesgo, y comunicarlo a la vicerrectoría correspondiente. |
| Alto | Riesgo residual mayor que 40% y menor o igual que 60% | Se pasa al siguiente nivel, que consiste en definir las opciones de respuesta al riesgo y comunicarlo a la Rectoría. |
| Extremo | Riesgo residual mayor que 60% | Se pasa al siguiente nivel, que consiste en definir las opciones de respuesta al riesgo y comunicarlo al Consejo Universitario. |

Tabla 3. Criterios de aceptación del Riesgo

Fuente: tomada de la Metodología Sevri_UNA 2017, referencia (UNA, 2017)

# 2. Análisis de Impacto

El análisis de impacto al negocio, conocido por sus siglas en inglés como BIA *(Business Impact Analysis*) permite a cualquier entidad identificar con claridad los procesos críticos de la misma, con el objetivo de analizar el nivel de impacto con relación a la gestión del negocio.

Para poder obtener un análisis de impacto adecuado, cada entidad debe contar con un documento que respalde la verdadera identificación de las funciones críticas del negocio, así como un instrumento que permita garantizar la medición de la magnitud del impacto operacional y/o financiero del negocio, en el momento que se presenta cualquier interrupción en las operaciones diarias.

A continuación, se citan los tres puntos más importantes que son requeridos para llevar a cabo un buen análisis de impacto al negocio y en los cuales está basado este trabajo para realizar el respectivo procedimiento en el IMN:

a) Identificación de las funciones y procesos importantes para la supervivencia de las distintas unidades de negocio en el momento de la interrupción. Con este paso se debe tener en cuenta cuáles de los procesos son claves para que entren en operación rápidamente; asignándoles la mayor prioridad posible ante los de menor prioridad. Cabe mencionar que estos últimos deben ser tomados en cuenta en los planes de recuperación.
b) Determinar las posibles consecuencias operacionales y financieras que se presenten en el momento de cualquier interrupción.
c) Estimar los tiempos de recuperación en relación con las posibles alteraciones de los procesos de alta prioridad para la correcta continuidad del negocio.

Al finalizar con esta fase, se presenta un informe con los detalles de las funciones y procesos críticos del negocio, el cual contiene información básica de los recursos requeridos y los tiempos de recuperación para que se dé con éxito la continuidad del negocio.

Adicionalmente, como parte del mismo proceso, se hace uso de parámetros muy importantes como lo son el RPO (Punto de Recuperación en el Tiempo) y el RTO (Tiempo de Recuperación) que definen la capacidad de respuesta de la institución a la materialización de una interrupción en sus actividades críticas para minimizar la pérdida de datos.

Cabe mencionar que el RPO es la capacidad de recuperar información en un punto anterior al desastre o interrupción de actividades, es decir cuánto será la cantidad de datos que la institución podría perder, antes de paralizar su correcto funcionamiento.

Por ejemplo, si ocurre algún tipo de desastre en el instituto y se requiere recuperar la información, y los propietarios de ésta definen que es crítico no perder más allá de la última hora, la cual es factible de recuperar luego de manera manual, el RPO en este caso sería de 1 hora.

Además, el RTO es el tiempo que se puede permitir la institución para volver a dar su servicio con normalidad. Es decir, el tiempo que el personal de TI tiene para restablecer el sistema, después de la detección de la interrupción de actividades, más allá de este tiempo se causaría daños no tolerables para la organización y para sus usuarios.

La principal función de estos parámetros es la de identificar los tiempos de recuperación que las actividades críticas del instituto tendrán en caso de una interrupción o pérdida de servicio, mientras más se acerquen los tiempos a 0, mayor será su grado de criticidad.




Figura 3. RPO – RTO

Fuente: tomada de (Galileus, 2016)

# 3. Plan de Contingencia del Negocio

Se define como plan de contingencia a una estrategia planificada con una serie de procedimientos que faciliten u orienten una solución alternativa que permita continuar brindando los servicios críticos de la organización ante la eventualidad de cualquier tipo que pueda paralizar la continuidad de las funciones importantes de la institución, ya sea de forma parcial o total.

El plan de contingencia ayuda a que los procesos críticos de la institución continúen funcionando a pesar de una posible falla. Es decir, un plan que le permitirá al instituto seguir operando, aunque sea al mínimo de sus capacidades.

**Objetivos del Plan de Contingencia**

a) Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen las principales tareas realizadas por el instituto.
b) Definir acciones y procedimientos por ejecutar, en caso de fallas de los elementos o dispositivos que colaboran en conjunto con las actividades de importancia.

Además de dar a conocer las posibles consecuencias a las que se podría ver enfrentado el IMN, puede que el no tener un plan de contingencia ponga a la institución bajo las siguientes situaciones:

- Pérdida de datos.
- Pérdidas monetarias y de imagen.
- Sanciones legales.
- Cierre del negocio.

Es de suma importancia mencionar que la participación de los empleados de la institución es la parte más importante en cuanto a su diseño e implementación, según sea la planificación del mismo, ya que ellos serán los responsables de que funcione de la manera más eficiente.

## Marco Contextual

### Instituto Meteorológico Nacional

El IMN es una institución adscrita al Ministerio de Ambiente y Energía (MINAE), es un ente científico que tiene a cargo la coordinación de todas las actividades meteorológicas y climatológicas del país. Mantiene una vigilancia sistemática del estado del tiempo para brindar apoyo a la seguridad de la navegación aérea del país, para la prevención de los desastres hidrometeorológicos y coadyuvar a los efectos adversos de la variabilidad y el cambio climático.

Recopila, estudia y analiza la información meteorológica y climatológica que mide y registra la red de estaciones del Instituto en el país, así como información necesaria para la preparación de estudios e investigaciones en campos como la agro meteorología, climatología, variabilidad climática, contaminación atmosférica, interacción océano-atmósfera, gases con efecto invernadero, cambio climático y otros. Toda esta información se brinda con el fin de apoyar desde el punto de vista de las competencias institucionales, el desarrollo nacional.

Dichos estudios pueden ser interinstitucionales e interdisciplinarios, y como resultado suministra información y son referentes para la toma de decisiones en aspectos tan variados como: seguridad alimentaria, las fases del fenómeno ENOS, la relación clima y salud humana, la amenaza climática, la vulnerabilidad y riesgo a eventos hidrometeorológicos extremos. Además, incluye información que otras instituciones puedan tomar para lograr el mejor uso del recurso hídrico para la producción hidroeléctrica, la vulnerabilidad del agua para consumo humano y otros; a nivel local, regional o nacional.

Fuente: tomada de Instituto Meteorológico Nacional, referencia (IMN, s.f.)

## Reseña Histórica

De acuerdo con los registros históricos, los primeros datos meteorológicos se deben al botánico y naturalista danés A.S. Oersted, quien en 1846 inició una exploración geográfica en el país, verdadera hazaña en aquella época. Debido al desarrollo científico, a mediados del siglo XIX se genera en el país el interés de establecer un observatorio meteorológico, esta idea fue liderada por el Dr. Fernando Streber en 1873.

Para 1887, se establece el primer observatorio Meteorológico Nacional, sin embargo, no fue hasta el 7 de abril de1888 que se publica en la gaceta, la creación del Instituto Meteorológico Nacional y se nombra director a Pittier, quien también fue asignado como profesor en el Liceo de Costa Rica.

En 1963, motivado por los efectos de la erupción del Volcán Irazú y las inundaciones del Río Reventado (Cartago), se negoció la adquisición de un importante equipo meteorológico, incluyendo un radar.

En 1973, mediante la Ley 5222, se crea el Instituto Meteorológico Nacional (IMN), adscrito al Ministerio de Agricultura y Ganadería (MAG), y asume su dirección el Lic. Gerardo Lizano, uno de los primeros graduados en meteorología de la UCR. Desde 1975 las oficinas centrales se localizan en el Barrio Aranjuez.

Posteriormente, la Ley 7152 de 1990, traslada al IMN al Ministerio de Recursos Naturales, Energía y Minas (MIRENEM), el cual a partir de 1995 pasa a llamarse Ministerio de Ambiente y Energía (MINAE) como una dirección adscrita.

El IMN cuenta al 2015, con ciento veintisiete años de actividad continua, para el beneficio social y económico del país. Es una institución que se ha preocupado durante este tiempo por el desarrollo profesional y tecnológico, con el fin de ser un Instituto Meteorológico de punta en el ámbito nacional e internacional. Este cumpla con las exigencias que le impone el Siglo XXI, en campos como la prevención de desastres hidrometeorológicos, la adaptación y mitigación del Cambio Climático, y continuar educando a las nuevas generaciones sobre las aplicaciones de la ciencia meteorológica para el desarrollo de la sociedad costarricense.

Fuente: tomada de Instituto Meteorológico Nacional, referencia (IMN, s.f.)

## Misión

El Instituto Meteorológico Nacional como entidad científico-técnica especializada en tiempo, clima y agua, mantiene la vigilancia continua del tiempo y del clima en el país. Para ello proporciona pronósticos, avisos, e información meteorológica, administra el banco de datos climáticos institucional y publica estadísticas periódicas, promueve la cultura meteorológica por medio de un servicio de educación y divulgación. También, realiza estudios e investigaciones en todas sus aplicaciones, mantiene y fomenta las relaciones de cooperación con organismos nacionales e internacionales del ramo.

Para lograr sus objetivos, asesora a las autoridades nacionales en la materia, así como otros servicios orientados al apoyo de la eficiencia y seguridad del transporte aéreo y marítimo, la producción agrícola, el turismo y otros sectores productivos. Se ocupa de la prevención y mitigación de los desastres de origen hidrometeorológicos, la protección de la atmósfera y del ambiente, la mitigación y adaptación al cambio climático, y protección del recurso hídrico, todo en un marco de eficiencia y eficacia y de los principios del desarrollo humano sostenible.

Fuente: tomada de Instituto Meteorológico Nacional, referencia (IMN, s.f.)

## Visión

El Instituto Meteorológico Nacional será una institución con mayor perfil internacional y su liderazgo mejorará su capacidad como rectora en tiempo y clima, orientada a satisfacer las necesidades que el país demande acorde con su misión institucional, amparada en el conocimiento científico y en los avances tecnológicos del siglo XXI, y en un recurso humano altamente calificado y motivado, todo comprometido con los principios del desarrollo humano sostenible.

Fuente: tomada de Instituto Meteorológico Nacional, referencia (IMN, s.f.)

## Estructura Organizativa

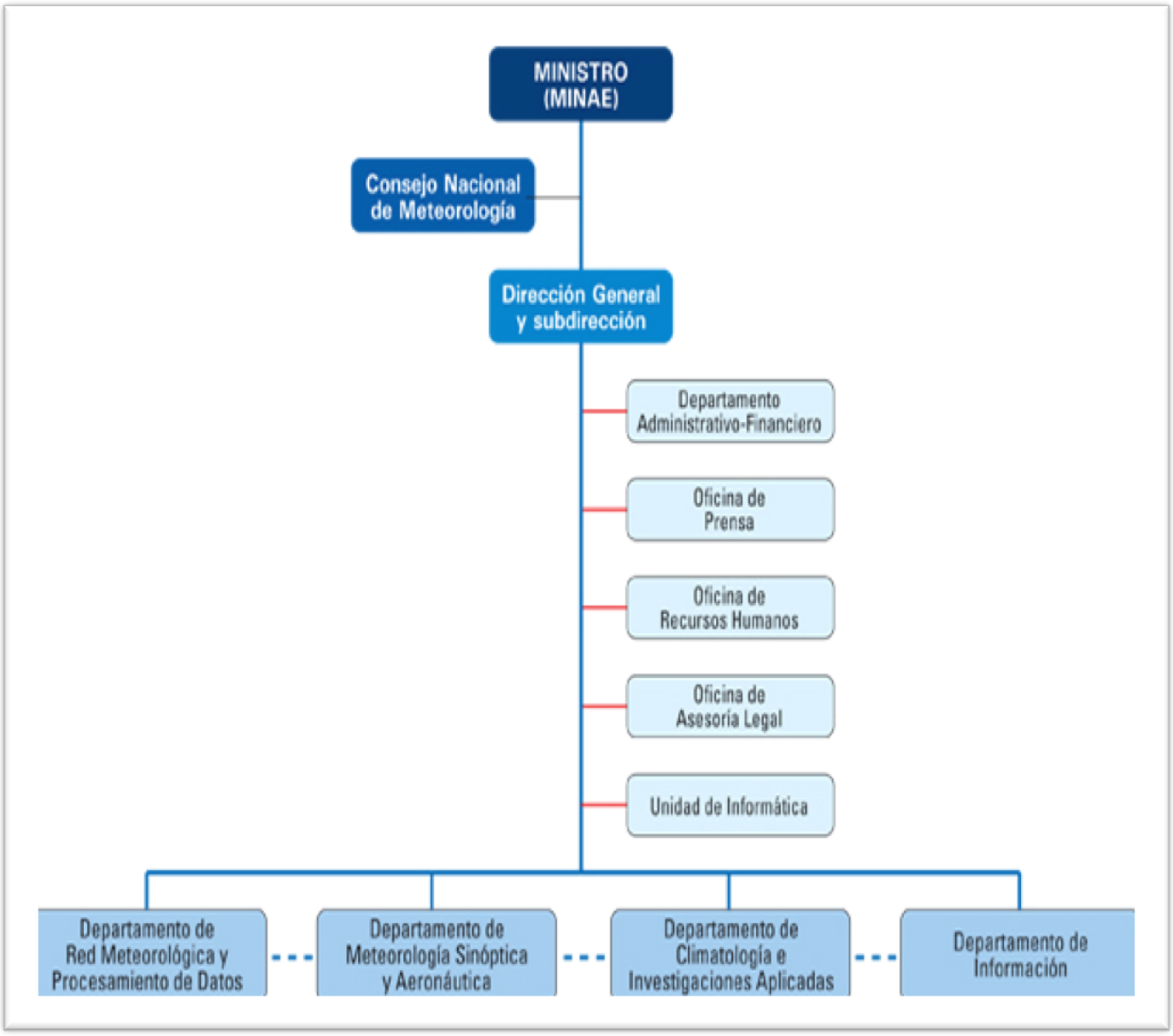



Figura 4. Estructura Organizativa

Fuente: tomada de Instituto Meteorológico Nacional, referencia (IMN, s.f.)

De acuerdo con la Ley de Creación del Instituto Meteorológico Nacional, este será dirigido por un Consejo Nacional de Meteorología y un Director General.

## Investigación Aplicada

Para efectos de la aplicación de un análisis de riesgo y como parte del inicio de esta investigación se identificaron los activos más críticos de la institución, estos van a estar involucrados tanto en el análisis de riesgos como los demás procesos. Se ocupa del impacto del negocio y del plan de continuidad, de esta manera se podrá identificar los activos del departamento de TI y más aún la previa evaluación de una categorización de criticidad en caso de una catástrofe. A continuación, se muestra una lista de activos según su grado de criticidad: [1]

SERVIDORES CON ALTA CRITICIDAD

| ID | Descripción | Responsable | Tipo | Ubicación | Crítico |
|---|---|---|---|---|---|
| ID_1.1 | Servidor AD, DNS, FTP, y otros | Desarrollo de Sistemas | Servidor (Físico) | T.I. | Sí |
| ID_1.2 | Servidor de AD, DNS, DHCP, Web, impresión, ESET y otros | Desarrollo de Sistemas | Servidor (Físico) | T.I. | Sí |
| ID_1.3 | Servidor de Correo | Desarrollo de Sistemas | Servidor (Físico) | T.I. | Sí |
| ID_1.4 | Servidor Portal Web Institucional | Desarrollo de Sistemas | Servidor (Físico) | T.I. | Sí |
| ID_1.5 | DNS EXTERNO | Desarrollo de Sistemas | Servidor (Físico) | T.I. | Sí |
| ID_1.6 | Base de datos Oracle 11G | Jefatura de T.I | Servidor (Físico) | T.I. | Sí |
| ID_1.7 | Weblogic producción | Jefatura de T.I | Servidor (Físico) | T.I. | Sí |
| ID_1.8 | Oracle VM para servidor de aplicaciones (ldoms) | Jefatura de T.I | Servidor (Físico) | T.I. | Sí |
| ID_1.9 | Base de datos Desarrollo | Jefatura de T.I | Servidor (Físico) | T.I. | Sí |

Tabla 4. Servidores Críticos

Fuente: Tomada del Inventario del IMN, referencia, (Inventario IMN, 2017)

[1] Por motivos de confidencialidad los nombres de los equipo y encargados no serán mostrados en ninguna sección del proyecto, sin embargo, cabe destacar que el IMN tiene una lista estipulada con la identificación de cada equipo y sus respectivos encargados

SERVIDORES CON MEDIA CRITICIDAD

| ID | Descripción | Responsable | Tipo | Ubicación | Critico |
|---|---|---|---|---|---|
| ID_2.1 | Modelo hidrológico | Desarrollo de Sistemas | Servidor (Físico) | T.I. | Sí |
| ID_2.2 | Servidor SQL base de datos fenómenos | Desarrollo de Sistemas | Servidor (Físico) | T.I. | Sí |
| ID_2.3 | Base de Datos Cambio Climático | Desarrollo de Sistemas | Servidor (Físico) | T.I. | Sí |
| ID_2.4 | *Recepción imágenes EUMESAT* | Jefatura de T.I | WorkStation (Físico) | Sinóptica | Sí |
| ID_2.5 | Servidor del model WRF | Desarrollo de Sistemas | WorkStation (Físico) | Sinóptica | Sí |
| ID_2.6 | Modelo numérico WRF | Desarrollo de Sistemas | WorkStation (Físico) | Sinóptica | Sí |
| ID_2.7 | Modelo | Desarrollo de Sistemas | WorkStation (Físico) | Sinóptica | Sí |
| ID_2.8 | Weblogic Desarrollo | Jefatura de T.I | Servidor (Físico) | T.I. | Sí |
| ID_2.9 | Receptor Satelital | Sistemas de Información | Servidor (Físico) | T.I. | Sí |
| ID_2.10 | Receptor Satelital | Sistemas de Información | Servidor (Físico) | T.I. | Sí |
| ID_2.11 | Diseminador Satelital | Sistemas de Información | Servidor (Físico) | T.I. | Sí |
| ID_2.12 | Diseminador Satelital | Sistemas de Información | Servidor (Físico) | T.I. | Sí |

Tabla 5. Servidores Criticidad Media

Fuente: Tomada del Inventario del IMN, referencia, (Inventario IMN, 2017)

SERVIDORES CON BAJA CRITICIDAD

| ID | Descripción | Responsable | Tipo | Ubicación | Critico |
|---|---|---|---|---|---|
| ID_3.1 | Desplegador Imágenes Satelitales | Sistemas de Información | Servidor (Físico) | Sinóptica | Sí |
| ID_3.2 | Desplegador Imágenes | Sistemas de Información | WorkStation (Físico) | Sinóptica | Sí |

Tabla 6. Servidores baja criticidad

Fuente: Tomada del Inventario del IMN, referencia, (Inventario IMN, 2017)

Infraestructura de Red y otros.

| ID | Nombre | Descripción | Responsable | Tipo | Ubicación | Critico |
|---|---|---|---|---|---|---|
| ID_4 | Access Point | Puntos de Acceso | Infraestructura | Físico | T.I. | Sí |
| ID_5 | Hubs | Enrutadores | Infraestructura | Físico | T.I. | Sí |
| ID_6 | Routers | Enrutadores para la red. | Infraestructura | Físico | T.I. | Sí |
| ID_7 | Modems | Comunicación con el proveedor de servicios de Internet | Infraestructura | Físico | T.I. | Sí |
| ID_8 | Firewalls | Corta Fuegos | Infraestructura | Físico | T.I. | Sí |
| ID_9 | Planta Eléctrica | Sistema de corriente alternativa para el cuarto de T.I. | Infraestructura | Físico | T.I. | Sí |
| ID_10 | A\C | Alimentación de corriente eléctrica | Infraestructura | Físico | T.I. | Sí |

Tabla 7. Infraestructura de red y alimentación eléctrica

Fuente: Tomada del Inventario del IMN, referencia, (Inventario IMN, 2017)

# 1. Análisis de Riesgos

Para efectos de la investigación, se hace uso de la metodología SEVRI para realizar la respectiva gestión de los riesgos institucionales. La herramienta permite identificar, valorar y administrar los riesgos que impidan el cumplimiento de los objetivos de la institución, con el objetivo de mitigar el efecto que puedan generar.

## I Etapa: Identificación del Riesgo

### Portafolio de Objetivos

Para tal efecto, se citan los objetivos estratégicos del departamento de TI del IMN:

a) Aplicar las mejores prácticas en el manejo de datos para garantizar la seguridad de la información, infraestructuras de procesamiento y aplicaciones.
b) Cumplir de forma adecuada las leyes y normativas institucionales para satisfacer con las necesidades del departamento de TI.
c) Identificar los procesos - fases - métodos que cumplirán con el fortalecimiento de sistema de control de calidad y control interno de TI.

Fuente: tomada de la información brindada por los miembros del IMN

### Portafolio de Riesgos

Cada una de las categorías se explica con detalle, además de la mención de los riesgos existentes por cada una de ellas. Esta sección debe ser revisada de forma constante para evitar la discontinuidad, o no cumplimiento con nuevos riesgos al paso del tiempo.

Fuente: tomada después de la investigación que realizamos, para determinar cuáles son los riesgos que pueden vulnerar las actividades del departamento de TI.

## Categorización de Riesgos

| ID | Categoría | Riesgo |
|---|---|---|
| **ID_Cat1** | 1. Establecimiento y mantenimiento del portafolio | a) Riesgo de que no exista una evaluación previa del *software, hardware* o proceso interno al departamento de TI, no cumpliendo así con los requisitos necesarios de compatibilidad de la institución.<br>b) Riesgo de incorrecta asignación de los recursos e incumplimiento de los objetivos prioritarios del negocio. |
| **ID_Cat2** | 2. Pericia y habilidades de TI | a) Riesgo por ausencia de recursos competentes para realizar distintas actividades relacionadas con algún rol de trabajo, presentando falta de entrenamiento y conocimiento adecuado ante nuevas tecnologías y procesos básicos.<br>b) Riesgo de no separación de roles y falta de personal con la capacidad de asumir otro puesto en caso de despido, ausencia o incapacidad del personal. |
| **ID_Cat3** | 3. Operaciones del personal (error humano e intento malicioso) | a) Riesgo de falta de compromiso por parte del personal, cometiendo errores o poniendo en peligro cualquier tipo de información, la misma infraestructura, *hardware*, *software*, entre otros, con intención. (Daño a equipos, pérdida de información, errores en la configuración o inserción de información, etc.)<br>b) Riesgo por daños en dispositivos críticos, como cuarto de servidores o dispositivos de seguridad, etc. |
| **ID_Cat4** | 4. Información (brecha de datos: daño, fuga y acceso) | a) Riesgo en el acceso de información sensitiva e importante de la institución poniendo en peligro la misma al robo o revelación a personas no autorizadas.<br>b) Riesgo por falta de respaldos, no pudiendo utilizarse en caso de presentar archivos corruptos o pérdida de datos.<br>c) Riesgo por mala manipulación de dispositivos de almacenamiento como USB, servidores, CD y discos portátiles. |
| **ID_Cat5** | 5. Infraestructura (*hardware,* sistemas operativos y tecnología de control) (selección/implementación, operaciones y des patrimonio) | a) Riesgo por fallas intermitentes en la electricidad o telecomunicaciones, que interrumpan las actividades de la institución.<br>b) Riesgo en la carencia de infraestructura para satisfacer nuevos servicios (redes, seguridad, base de datos, almacenamiento, etc.) necesarios para el cumplimiento de objetivos de TI. |

Tabla 8. Categorización de Riesgo

Fuente: tomada después de la investigación que realizamos, para determinar cuáles son los riesgos que pueden vulnerar las actividades del IMN

Continuación con la categorización,

| ID | Categoría | Riesgos |
|---|---|---|
| **ID_Cat6** | 6. *Software* y aplicaciones comunes de forma interna | a) Riesgo de que el *software* aplicativo esté obsoleto (p.ej., tecnologías anticuadas, pobremente documentadas, costosas de mantener, difíciles de entender, no integradas en la arquitectura vigente).<br>b) Riesgo de que no existan procesos adecuados para retornar a versiones anteriores en caso de problemas de compatibilidad con nuevas versiones.<br>c) Riesgo a la mala administración de las bases de datos a nivel interno. |
| **ID_Cat7** | 7. Robo o destrucción de la infraestructura | a) Existe el riesgo de que se haya producido el robo de un dispositivo con datos sensibles o que dispositivos individuales se destruyan accidentalmente.<br>b) Riesgo de que personas sin los suficientes privilegios tengan acceso a las áreas restringidas donde solo el personal de TI debería de accesar. |
| **ID_Cat8** | 8. Código malicioso, Ataques lógicos | a) Riesgo relacionado al robo de datos de la institución a través de accesos no autorizados obtenidos mediante ataques como "*phishing",* troyanos, *ransomware,* virus, etc.<br>b) Riesgo de que usuarios no autorizados traten de forzar el ingreso a los sistemas de la institución.<br>c) Riesgo a la falta de actualizaciones de los equipos y sistemas necesarios (*AV, Firmware, FW*) |
| **ID_Cat9** | 9. Actos de la naturaleza | a) Existe el riesgo de que la institución se vea afectada por cualquier acto de la naturaleza, por ejemplo, inundaciones, terremoto, tormentas tropicales entre otros que puedan afectar a la institución de manera que no puedan fungir con sus actividades con normalidad. |
| **ID_Cat10** | 10. Innovación | a) No se investigan nuevas tendencias e importantes de TI. |

Tabla 9. Continuación, Categorización de Riesgos

Fuente: tomada después de la investigación que realizamos, para determinar cuáles son los riesgos que pueden vulnerar las actividades del IMN

## II Etapa: Valoración del Riesgo

Para efectos de esta investigación y como parte de la documentación, se toman tres ejemplos de riesgos del catálogo antes identificado, con el objetivo de realizar una valoración y poder presentar evidencia para que esta sea tomada como guía, en caso de cualquier consulta, ya sea por parte del IMN o de cualquier persona interesada, y que tenga la necesidad de leer el presente proyecto.

Ejemplo 1: Riesgo de que no existan procesos adecuados para retornar a versiones anteriores en caso de problemas de compatibilidad con nuevas versiones.

La valoración de este ejemplo fue la siguiente: el instituto cree que la frecuencia con que ocurre esta actividad es de "2", siendo esta una frecuencia "esporádica “, además, considera que su consecuencia es de "4", correspondiente a una consecuencia "mayor". Valor del riesgo es de: 8.

Ejemplo 2: Riesgo por falta de respaldos, no pudiendo utilizarse en caso de presentar archivos corruptos o pérdida de datos.

La valoración de este ejemplo fue la siguiente; el Instituto cree que la frecuencia con que ocurra esta actividad es de "3", siendo esta una frecuencia "moderada “, además, considera que su consecuencia es de "5", correspondiente a una consecuencia "catastrófica". Valor del riesgo es de: 15.

Ejemplo 3: Riesgo por fallas intermitentes en la electricidad o telecomunicaciones.

La valoración de este ejemplo fue la siguiente; el Instituto cree que la frecuencia con que ocurra esta actividad es de "2", siendo esta una frecuencia "esporádica “, además, considera que su consecuencia es de "3", correspondiente a una consecuencia "significativa". Valor del riesgo es de: 6.

## III Etapa: Administración del Riesgo

De acuerdo con el IMN, y analizando sus necesidades, se ha considerado que cuando se esté valorando el riesgo, el valor generado corresponderá al riesgo residual. Con este resultado la Junta Administrativa debe considerar el nivel de aceptación del riesgo de una forma inmediata y con más detalle para valorar qué acción será tomada. De igual forma, si el riesgo residual presenta un valor mayor a 12, será de suma importancia atacar el riesgo y aplicar de inmediato las contramedidas recomendadas o aplicar nuevas que apliquen a la administración del riesgo que se necesite dar ya sea mitigar, transferir o controlar.

Este proceso debe ser aplicado para cada uno de los riesgos de forma individual, ya que cada uno de ellos generará un valor distinto y las acciones que se deben tomar en cuenta son distintas en cada caso en particular.

## 2. Análisis de Impacto

El IMN es una institución de gran relevancia para el desarrollo del país, y lleva a cabo muchísimas tareas que le impactan, sin embargo, sus actividades dependen de muy pocos puntos de criticidad, pero de verdadera importancia. Esta institución cuenta con una amplia lista de funciones que son llevadas a cabo por diferentes departamentos. Sin embargo, se detectó que el departamento de Meteorología Sinóptica y Aeronáutica es el que podría tener el mayor impacto en caso de que algunos de los riesgos definidos en la siguiente tabla se materialicen.

Aunque muchas de las actividades secundarias no son críticas, hay una gran cantidad que son consideradas de bastante importancia para el instituto como ejemplo:

a) Creación de manuales para distintos procesos
b) Tener definidas políticas de la institución
c) Tener planes de acción en caso de emergencia, entre otras

Estas tareas deben ser revisabas periódicamente y estar actualizadas con tiempos menores a 3 o 6 meses para que, en caso de cualquier eventualidad, sean puestas en práctica sin ningún problema.

Para obtener un buen análisis de impacto se deben obtener la actividades críticas o acciones más importantes que tienen un alto impacto en la concurrencia normal de las funciones del instituto, después de un largo análisis y luego de una buena elección de tareas se encontraron los siguientes puntos como los más críticos y dicho esto se debe recalcar que si en algún momento se vieran afectadas tienen un alto impacto para el instituto por lo que se debe dar inmediata importancia para la continuidad de las mismas.

| Departamento de Meteorología Sinóptica y Aeronáutica | | | | |
|---|---|---|---|---|
| **Actividades** | **Criticidad** | **RPO** | **RTO** | **Dispositivos** |
| Disponibilidad de los servicios de Internet | ALTA | Inmediato | 30 min | Enlaces a internet |
| Disponibilidad de los servicios de electricidad | ALTA | Inmediato | 30min | Planta Eléctrica |
| Respaldo digital de la información sinóptica y aeronáutica que corresponda a cada departamento. | ALTA | 30 min | 1h | SAN (Servidor de archivos), NAS (Respaldos), y otros servidores |
| Funcionamiento y equipamiento del sistema de modelación numérica del tiempo. | ALTA | 1h | 5 - 6h | Servidores Web |
| Emitir productos claros, oportunos y eficaces en los ámbitos marino, aéreo y en nuestra área continental. | ALTA | 5-10min | 30min | Servidores Web |
| Funcionamiento, actualización, gestión e implementación del sistema de recepción del satélite GOES. | ALTA | Menos de 1h | 3h | 2 Servidores<br>2 Desplegadores |
| Atender a los medios de comunicación (prensa, radio, televisión, internet) en el departamento. | MEDIA | 24h | 12h | Todos los anteriores |

Tabla 10. Actividades Críticas

Fuente: tomada de Actividades Criticas IMN, referencia (Cuadro de Actividades Criticas y Grado de Criticidad, 2017)

La tabla anterior detalla cada una de las actividades destacadas como críticas, su nivel de criticidad, los distintos tiempos de recuperación y restauración, así como los dispositivos que son usados para realizar el respectivo funcionamiento.

## 3. Plan de Contingencia

Para la confección del plan de contingencia, deben haberse desarrollado los procesos de análisis de riesgos y de impacto con anterioridad, este último proceso se encarga de recapitular varios de los resultados que han sido obtenidos al finalizar cada uno de ellos. Además, este plan permite reanudar las operaciones en un tiempo prudencial, con el objetivo de impactar lo menos posible al negocio, ya que estos periodos fueron definidos en el BIA proceso (descrito en el tema anterior).

Con el análisis de riesgos se realiza la categorización adecuada, en donde por medio de grupos específicos se lista cada uno de los riesgos para su fácil manipulación.

Por otra parte, el análisis de impacto dio a conocer las actividades más importantes, el grado de criticidad y los tiempos adecuados para la recuperación de datos y restablecimiento de la continuidad de las operaciones.

Con estos resultados, se pudo consolidar toda la información, para tener a mano, de una forma más oportuna y simple, qué se debe priorizar en caso de una materialización de amenazas. Para efectos de la creación del plan de contingencia es importante tener siempre actualizado, como a la vista y al conocimiento de todos los encargados y responsables de las actividades críticas, la existencia de estos dos documentos.

En el siguiente recuadro se encuentra un resumen de la información mencionada anteriormente. Además, se exponen las contramedidas con las que cuenta el instituto hoy en día, también está expuesta en dicha tabla la información sobre si hay algún grado de riesgo existente, conocido como riesgo residual, asimismo una lista de controles recomendados por este estudio. Cabe destacar que estos controles pueden ser puestos en marcha o no, ya que la decisión de su implementación queda completa a discrecionalidad de la Junta Administrativa del IMN. Por lo que si el riesgo residual se decide que sea aceptado, transferido, mitigado o eliminado es completamente responsabilidad de los altos jerarcas.

| ID Categoría | Descripción | Impacto | Riesgo Corriente | Controles Existentes | Riesgo Residual | Controles Recomendados |
|---|---|---|---|---|---|---|
| ID_Cat1 | Déficit en el estudio previo de *Hardware y Software* de parte del dpto. TI e incumplimiento de objetivos de la institución. | Medio | Riesgo de que no exista una evaluación previa del *software, hardware* o proceso interno al departamento de TI, no cumpliendo así con los requisitos necesarios de compatibilidad de la institución.<br><br>Riesgo de incorrecta asignación de los recursos e incumplimiento de los objetivos prioritarios del negocio. | Revisión previa de una forma exhaustiva y tomando en cuenta cualquier detalle para la implementación de nuevas tecnologías a nivel interno tanto s*oftware* como *hardware,* para que cumplan con los requerimientos básicos.<br><br>Evaluación de todos los recursos antes de darles cualquier asignación, siguiendo el plan ya existe para que se cumplan los objetivos de forma satisfactoria. | Falta de presupuesto, o que este sea insignificante para cuando se lleve a cabo alguna necesidad, con la desventaja de que este se solicita un año o año y medio de antelación. | Tratar de mantener un presupuesto adicional o de emergencia, sin embargo, hay que tomar en cuenta que el IMN es una institución pública y depende de otras entidades, por lo que si el costo de alguna nueva implementación sobrepasa el presupuesto no se podrá adquirir. |
| ID_Cat2 | Selección correcta del personal y adecuada asignación de roles según el puesto que desempeña. | Medio | Riesgo por ausencia de recursos competentes para realizar distintas actividades relacionadas algún rol de trabajo, presentando falta de | Evaluar las necesidades de personal de forma regular o en cambios importantes en la empresa u operativos o entorno a TI para garantizar que la empresa cuenta con | Selección de personal y en el momento de ocupar el puesto, el empleado no tenga la capacidad. | Evaluar continuamente los roles y responsabilidades de cada empleado para verificar que se esté |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | entrenamiento y conocimiento adecuado ante nuevas tecnologías y procesos básicos.<br><br>Riesgo de no separación de roles y falta de personal con la capacidad de asumir otro puesto en caso de despido, ausencia o incapacidad del personal. | los recursos humanos suficientes para apoyar las metas y objetivos de la empresa. En el personal se incluye tanto los recursos internos como los externos. | | cumpliendo de forma adecuada. |
| ID_Cat3 | Capacitación inadecuada y\o negligencia del uso correcto de los medios informáticos de la institución. | Medio | Riesgo de falta de compromiso por parte del personal, cometiendo errores o poniendo en peligro cualquier tipo de información, la misma infraestructura, *hardware, software*, entre otros, con intención. (Daño a equipos, pérdida de información, errores en la configuración o inserción de información, etc.)<br><br>Riesgo por daños en | Constante capacitación para el personal haciéndoles comprender su responsabilidad en el negocio.<br><br>Administrar las instalaciones de forma periódica, incluyéndose los equipos de comunicaciones y de energía, de acuerdo con las leyes y reglamentos, requisitos técnicos y comerciales, las especificaciones del | No existe riesgo residual | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | dispositivos críticos, como cuarto de servidores o dispositivos de seguridad, etc. | fabricante, y las directrices de seguridad e higiene.<br><br>Control de ingreso y único acceso, por control de cámaras | | |
| ID_Cat4 | Manipulación inadecuada de la información ocasionando pérdida o fuga de datos sensibles. | Alto | Riesgo en el acceso de información sensitiva e importante de la institución poniendo en peligro la misma al robo o revelación a personas no autorizadas.<br><br>Riesgo por falta de respaldos, no pudiendo utilizarse en caso de presentar archivos corruptos o pérdida de datos.<br><br>Riesgo por mala manipulación de dispositivos de almacenamiento como USB, servidores, CD y discos portátiles. | Definir y mantener las responsabilidades de la propiedad de la información (datos) y de los sistemas de información.<br><br>Asegúrese que los usuarios toman las decisiones clasificando la información y los sistemas y revisan la protección de acuerdo con dicha clasificación.<br><br>Establecer un proceso para el resguardo de la información que se encuentre en dispositivos externos o cuando se dé errores en la extracción de los mismos. | Negligencia por parte de los empleados | Campañas de concienciación y capacitación en la manipulación de datos críticos para mantener la seguridad de la información |

| | | | | | | |
|---|---|---|---|---|---|---|
| ID_Cat5 | Fallas de infraestructura y aprovechamiento inadecuado de los recursos informáticos. | Alto | Riesgo por fallas intermitentes en la electricidad o telecomunicaciones, que interrumpan las actividades de la institución.<br><br>Riesgo en la carencia de infraestructura para satisfacer nuevos servicios (redes, seguridad, base de datos, almacenamiento, etc.) necesarios para el cumplimiento de objetivos de TI. | Elaborar un plan para realizar mantenimientos y conocer el estado de los sistemas, así como de la información que maneja el departamento de TI.<br><br>Dar manteniendo y constantes revisiones a los sistemas eléctricos y proveedores de telecomunicaciones.<br><br>Analizar las tecnologías emergentes identificadas y / u otras sugerencias de innovación de TI.<br><br>Trabajar con las partes interesadas para validar las hipótesis sobre el potencial de las nuevas tecnologías y la innovación. | Riesgo de una posible falla del servicio de internet y de electricidad. | Adquisición de un nuevo proveedor de internet.<br><br>Instalación de una segunda planta eléctrica. |
| ID_Cat6 | Implementación de *software* que no sea compatible con la | Bajo | Riesgo de que el *software* aplicativo esté obsoleto (p.ej., tecnologías | Se realizan pruebas de aceptación de los usuarios y entrenamiento | Nuevas herramientas de desarrollo elegidas no cumplan con el | Hacer un estudio de factibilidad con los productos que se |

| | | | | | | |
|---|---|---|---|---|---|---|
| | tecnología o infraestructura actual. | | anticuadas, pobremente documentadas, costosas de mantener, difíciles de entender, no integradas en la arquitectura vigente).<br><br>Riesgo de que no existan procesos adecuados para retornar a versiones anteriores en caso de problemas de compatibilidad con nuevas versiones.<br><br>Riesgo a la mala administración de las bases de datos a nivel interno. | personalizado antes de decisiones de la puesta en marcha, asegurando una transición fluida del nuevo *software* y que continúe la generación de valor para el negocio. | objetivo y se deba cambiar a versiones anteriores siendo estas ya obsoletas | encuentran en el mercado para que cumplan con las necesidades del instituto<br><br>Hacer plan pilotos antes de la implementación del producto |
| ID_Cat7 | Acceso de personal no autorizado en zonas restringidas. | Alto | Existe el riesgo de que se haya producido el robo de un dispositivo con datos sensibles o que dispositivos individuales se destruyan accidentalmente. | Los componentes clave de la infraestructura se monitorean 24x7 para hacer un seguimiento del desempeño, disponibilidad, etc.<br><br>Se disparan alarmas en | Negligencia por parte de los empleados<br><br>Guarda de seguridad tiene acceso al cuarto de servidores | Control de accesos tecnológicos, uso de *badge* en el cuarto de servidores<br><br>Capacitación constante a los empleados que se |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | Riesgo de que personas sin los suficientes privilegios tengan acceso a las áreas restringidas donde solo el personal de TI debería accesar. | caso de irregularidades y se actúa en forma inmediata.<br><br>El centro de datos se protege adecuadamente, permitiendo sólo el acceso del personal autorizado de TI. | | encargan de la seguridad del edifico |
| ID_Cat8 | Robo o destrucción de datos por parte de terceros utilizando medios tecnológicos. | Medio | Riesgo relacionado al robo de datos de la institución a través de accesos no autorizados obtenidos mediante ataques como "*phishing", troyanos, ransomware*, virus, etc.<br>Riesgo de que usuarios no autorizados traten de forzar el ingreso a los sistemas de la institución.<br><br>Riesgo a la falta de actualizaciones de los equipos y sistemas necesarios (*AV, Firmware, FW)* | La infraestructura de TI se protege de forma apropiada a través de *firewalls* y monitoreo continuo de la red, para asegurar la ejecución de las actividades diarias | Brechas de seguridad al no aplicar parches o actualizaciones.<br><br>Mala manipulación de credenciales compartiéndolas con personas no autorizadas | Mantener los equipos actualizados, realizándolo al menos cada 3 meses<br><br>Capacitación continua del uso de credenciales |
| ID_Cat9 | Instalaciones afectas por | Alto | Existe el riesgo de que la | Contar con un sitio alterno | Falta de presupuesto | Presentar proyecto a |

| | | | | | | |
|---|---|---|---|---|---|---|
| | eventos naturales. | | institución se vea afectada por cualquier acto de la naturaleza, por ejemplo, inundaciones, terremoto, tormentas tropicales entre otros que puedan afectar a la institución de manera que no puedan fungir con sus actividades con normalidad. | para reanudar las tareas | para la migración de un sitio alterno o la nube | jefatura para la adquisición de un servicio alterno o en la nube para evitar impacto en las actividades |
| ID_Cat10 | Implementación de nuevas tecnologías. | Medio | No se investigan nuevas tendencias e importantes de TI. | Se impulsa y avala la innovación y la atención a las tendencias, asegurando que se evalúen en forma oportuna las nuevas tecnologías para identificar su impacto en el negocio y que se adopten, si fuera necesario | No participación o quedarse desactualizado a nivel tecnológico | Participar en los eventos que permitan conocer las nuevas tendencias |

Tabla 11. Plan de Contingencia

Fuente: tomada de la investigación realizada, además es formada por información recolectada de los procesos anterior

## Plan de Atención de Incidentes

El siguiente cuadro detalla qué hacer en caso de que alguna de las actividades críticas se interrumpa y qué se debe hacer para que el servicio continúe, con esta información el IMN puede tener a mano la forma en que se debe actuar para atender una caída de servicios y su pronta restauración.

| Actividades | En caso de fallo | Continuidad de la actividad |
|---|---|---|
| **Disponibilidad de los servicios de Internet** | Utilizar el segundo enlace de fibra óptica, si esta falla se llama al proveedor y por ser una institución de gran criticidad el problema lo resuelven casi de inmediato | Acudir a los números de atención inmediata del proveedor de servicios. En este caso el riesgo es aceptado y se de esperar a que se restaure la conexión. |
| **Disponibilidad de los servicios de electricidad** | Se utiliza la segunda planta de electricidad, esta es un poco vieja (17 años), sin embargo, está en constante mantenimiento | El instituto cuenta con un protocolo bien establecido para la reanudación de la electricidad. El riesgo remanente es aceptado. |
| **Respaldo digital de la información sinóptica y aeronáutica que corresponda a cada departamento.** | Utilización de servidores asignados a respaldos, y en caso necesario acudir a los respaldos almacenados en un sitio alterno | Poner en funcionamiento con servidores alternos y reestablecer los respaldos |
| **Funcionamiento y equipamiento del sistema de modelación numérica del tiempo.** | Utilización de servidores asignados a respaldos, y en caso necesario acudir a los respaldos almacenados en un sitio alterno | La reanudación del servicio dependerá de si la falla en el equipo es de *software o hardware* |
| **Emitir productos claros, oportunos y eficaces en los ámbitos marino, aéreo y en nuestra área continental.** | Utilización de servidores asignados a respaldos, y en caso necesario acudir a los respaldos almacenados en un sitio alterno | La reanudación del servicio dependerá de si la falla en el equipo es de *software o hardware* |

| | | |
|---|---|---|
| **Funcionamiento, actualización, gestión e implementación del sistema de recepción del satélite GOES.** | La operación no se verá muy impactada ya que se tiene acceso a un servicio satelital por parte de un ente meteorológico ubicado en US | La reanudación del servicio dependerá de si la falla en el equipo es de *software o hardware* |
| **Atender a los medios de comunicación (prensa, radio, televisión, internet) en el departamento.** | Se solicita a los medios mantenerse informado por medio de la *página web* y redes sociales por un tiempo ni mayor a 24 horas | Cuando el IMN no se encuentra en alerta roja ya será posible atener a los medios de comunicación con normalidad |

Tabla 12. Plan de Atención a Incidentes

Fuente: tomada de la investigación y análisis realizado en conjunto con el departamento de TI

## Conclusiones

a) Este proyecto en su totalidad representa la etapa 4 de la metodología del Sistema Específico de Valoración de Riesgo Institucional (SEVRI), esta se caracteriza por la realización de un reporte o informe efectivo dirigido a la administración de la institución, se recomienda al menos generar un informe similar una vez al año para su continua actualización.

b) Se concluye que con la implementación del plan de continuidad del negocio se puede llegar a conocer qué tanto está preparada una empresa para enfrentar cualquier amenaza, además de estar al tanto en cuál nivel se encuentra, cuándo se debe avanzar o qué hace falta para estar preparado en caso de una amenaza. Por otra parte, permite poder llevar a cabo la planificación, verificación, análisis y la búsqueda de soluciones en caso de e riesgo materializar alguna vulnerabilidad.

c) El IMN es de suma importancia para el país, ya que es el ente recolector de los datos importantes del comportamiento meteorológico básicos para el desarrollo del país, la atención de emergencias y la preparación para enfrentar eventos extremos del clima, por lo que la continuidad de sus funciones es de alta criticidad.

d) Cabe mencionar, que el IMN, además de ser de gran importancia para Costa Rica cumple un papel muy importante a nivel centroamericano por el tipo de datos que son recolectados.

e) Además, si este plan no se hubiese realizado, el Instituto Meteorológico Nacional podría ser vulnerable a muchos de los riesgos identificados, ya que, por falta de controles y conocimiento, estos se pueden materializar en cualquier momento y poner a la institución en una situación riesgosa.

f) Debido a los reportes de los últimos meses de alerta roja en el país, por los distintos fenómenos climáticos, se puede concluir que, si el Instituto Meteorológico Nacional no hubiese estado preparado para enfrentar una discontinuidad en los servicios que brindan, la situación de emergencia pudo haber sido de mayor relevancia, sin embargo, con la implementación del plan de continuidad, el instituto puede continuar con la disponibilidad del servicio y mejorar la preparación del país ante eventuales eventos climáticos extremos.

## Recomendaciones

La principal recomendación es dar seguimiento a los distintos productos obtenidos durante este análisis:

- Análisis de Riesgos
- Análisis de Impacto
- Plan de Contingencia

a) Realizar revisiones de cada una de las etapas, con un periodo no mayor a un año, ya que, cada uno de los casos, podría cambiar en periodos muy cortos.

b) Mantener de igual forma la documentación actualizada, ya sea inventario de activos, riesgos detectados, actividades críticas, contra medidas aplicadas, riesgos residuales, controles por implementar y demás documentos conexos.

c) Hacer revisiones constantes para el cumplimiento de las políticas, y planes establecidos como, por ejemplo: de evacuación, y de restablecimiento de procesos o servicios; además, asegurarse de que se estén efectuando los protocolos que son importantes para la continuidad de las funciones.

## Glosario y Acrónimos

A continuación, se ofrecen el Glosario y los Acrónimos utilizados a lo largo de todo el proyecto:

**AV:** antivirus.

**BIA:** Siglas en inglés (Business Impact Analysis), Análisis de Impacto del negocio.

**Categoría de riesgo**: tema estratégico proclive al riesgo que sirve para orientar la identificación de los eventos.

**Contingencia:** posibilidad de que una cosa suceda o no suceda.

**Continuidad:** circunstancia de suceder o hacerse algo sin interrupción.

**Consecuencia:** impacto negativo que puede llegar a tener la materialización de un evento en el cumplimiento de cada meta del instituto.

**Criterios de aceptación del riesgo:** definición de rangos en valoración de los riesgos, con el propósito de determinar en cuáles casos se debe pasar al nivel de opciones de respuesta al riesgo.

**Frecuencia:** estimación de la posibilidad de que un evento de riesgo se presente.

**FW**: conocido como *Firmware*, también utilizado para la abreviación de *Firewall.*

**Gestión del riesgo:** método que le permite a la institución identificar, valorar y administrar los riesgos asociados con los objetivos institucionales.

**Identificación de riesgos:** fase compuesta por el establecimiento de los portafolios de objetivos y de riesgos.

**IMN:** Instituto Meteorológico Nacional.

**Impacto:** conjunto de los efectos que un suceso o un hecho producen en su entorno físico o social.

**ISO 27001:** Norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.

**Las fases del fenómeno ENOS:** cómo se comporta las distintas etapas de los fenómenos de la Niño y el Niña.

**MAG**: Ministerio de Agricultura y Ganadería

**Metodología:** Según el Diccionario, Método es el "modo de decir o hacer con orden una cosa". Asimismo, define el diccionario la palabra Metodología como "conjunto de métodos que se siguen en una investigación científica". Esto significa que cualquier proceso cinético debe estar sujeto a una disciplina de proceso defina con anterioridad que llamaremos Metodología.

**MINAE**: Ministerio de Ambiente y Energía

**Modelo de valoración:** procedimiento estándar que se utiliza para determinar los riesgos residual e inherente.

**Opciones de respuesta al riesgo:** alternativas que la administración puede asumir cuando el riesgo residual ha superado el nivel de calificación de aceptable.

***Phishing**:* utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

**Portafolio de objetivos**: compendio de ejes, objetivos, líneas de acción y metas estratégicas del instituto.

**Portafolio de riesgos:** listado de las categorías de riesgo y sus eventos asociados, que se tratarán en las fases de valoración.

***Ransomware*:** Tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción.

**Riesgo:** Según Fernando Izquierdo Duarte: "El Riesgo es un incidente o situación, que ocurre en un sitio concreto durante un intervalo de tiempo determinado, con consecuencias positivas o negativas que podrían afectar el cumplimiento de los objetivos".

**Riesgo inherente:** nivel de riesgo de un evento mediante la valoración de las variables frecuencia y consecuencia, a falta de cualquier tipo de medida administrativa tendiente a mitigar ese riesgo.

**Riesgo residual:** riesgos inherentes de un evento multiplicado por el factor de valoración de la madurez de las medidas administrativas establecidas en la institución, tendientes a mitigar cada riesgo identificado.

**RPO:** *Recovery Point Objective* (RPO), define la pérdida de datos máxima tolerable que se acepta ante una situación de desastre.

**RTO:** *Recovery Time Objective* o punto de Recuperación en el Tiempo es el tiempo que se tarda en volver dar servicio**.** Es decir, cuánto tiempo tiene el personal dedicado a IT para volver a poner en funcionamiento el sistema después de una parada o pérdida de información.

**SEVRI:** Sistema Específico de Valoración de Riesgos.

**TI:** Tecnologias informáticas o de información**.**

**Valoración de riesgos**: cálculo para obtener el riesgo inherente y el riesgo residual de cada uno de los eventos de riesgo identificados, y aplicar los criterios de aceptación respectivos para determinar en cuáles casos se requiere generar una respuesta.

**UCR:** Universidad de Costa Rica

**UNA**: Universidad Nacional

## Bibliografía


Anex, A. (2013). Obtenido de http://emb.cl/gerencia/articulo.mvc?xid=2717

Cabrera, M. (s.f.). Obtenido de GUIA PARA EL MANEJO DE CRISIS Y LA COMUNICACION DE CRISIS.pdf: http://www2.congreso.gob.pe/sicr/cendocbib/con3_uibd.nsf/6F1F80A0ADACC7D805257967007263B4/$FILE/GUIA_PARA_EL_MANEJO_DE_CRISIS_Y_LA_COMUNICACI%C3%93N_DE_CRISIS.pdf

(2017). *Cuadro de Actividades Criticas y Grado de Criticidad.* San Jose.

Galileus. (12 de April de 2016). *Business Continuity*. Obtenido de http://businesscontinuity-pe.blogspot.com/2016/04/video-tiempo-objetivo-de-recuperacion.html

*https://www.imn.ac.cr/es/inicio*. (s.f.). Obtenido de Instituto Meteorologico Nacional.

IMN. (s.f.). *https://www.imn.ac.cr/es/inicio*. Obtenido de Instituto Meteorologico Nacional.

*Infosol*. (s.f.). Obtenido de Mi Espacio: http://www.infosol.com.mx/espacio/Articulos/Desde_la_Trinchera/la_importancia_de_la_comunicacion_en_situaciones_de_crisis.html#.V6Peh3ouyw9

(2017). *Inventario IMN.* San Jose.

*Isaca*. (2017). Obtenido de http://www.isaca.org/cobit/pages/default.aspx?utm_source=2012-cobit5-brochure&utm_medium=direct-mail&utm_content=friendly-cobit5overview&utm_campaign=cobit5

PriteshGupta.com, F. W. (2005). *ISO 27000.es*. Obtenido de El portal de ISO 27001 en Español: http://www.iso27000.es/glosario.html

R, A. R. (Abril de 2010). *Manual_Comunicacion_Crisis.pdf*. Obtenido de https://www.icetex.gov.co/portal/Portals/0/images/manuales/Manual_comunicaci%C3%B3n_Crisis.pdf

*Replicalia*. (s.f.). Obtenido de Business Continuity as a Service: http://www.replicalia.com/que-es-el-rpo-y-el-rto/

Sánchez, R. R. (2012). *PREVENCIÓN Y MANEJO DE CRISIS*. Obtenido de http://www.coparmex.org.mx/upload/seminario2012/directores/12RicardoRoblesManejoDEcrisis.pdf

*Top Comunicacion*. (2011). Obtenido de Los ejemplos de comunicación de crisis más recordados en la Historia de las RR.PP.: http://www.topcomunicacion.com/noticia/6439/ejemplos-de-comunicacion-de-crisis-mas-recordados-en-la-historia-de-las-rrpp

UF338950. (18 de 1 de 2006). Obtenido de http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/4AnalisisycuantificaciondelRiesgo%28AR%29_es.pdf

UNA. (2017). *Metodologia Sevri_UNA 2017.* Heredia: UNA.

# Anexos

1. Riesgos




Anexo1: Definición de Riesgos

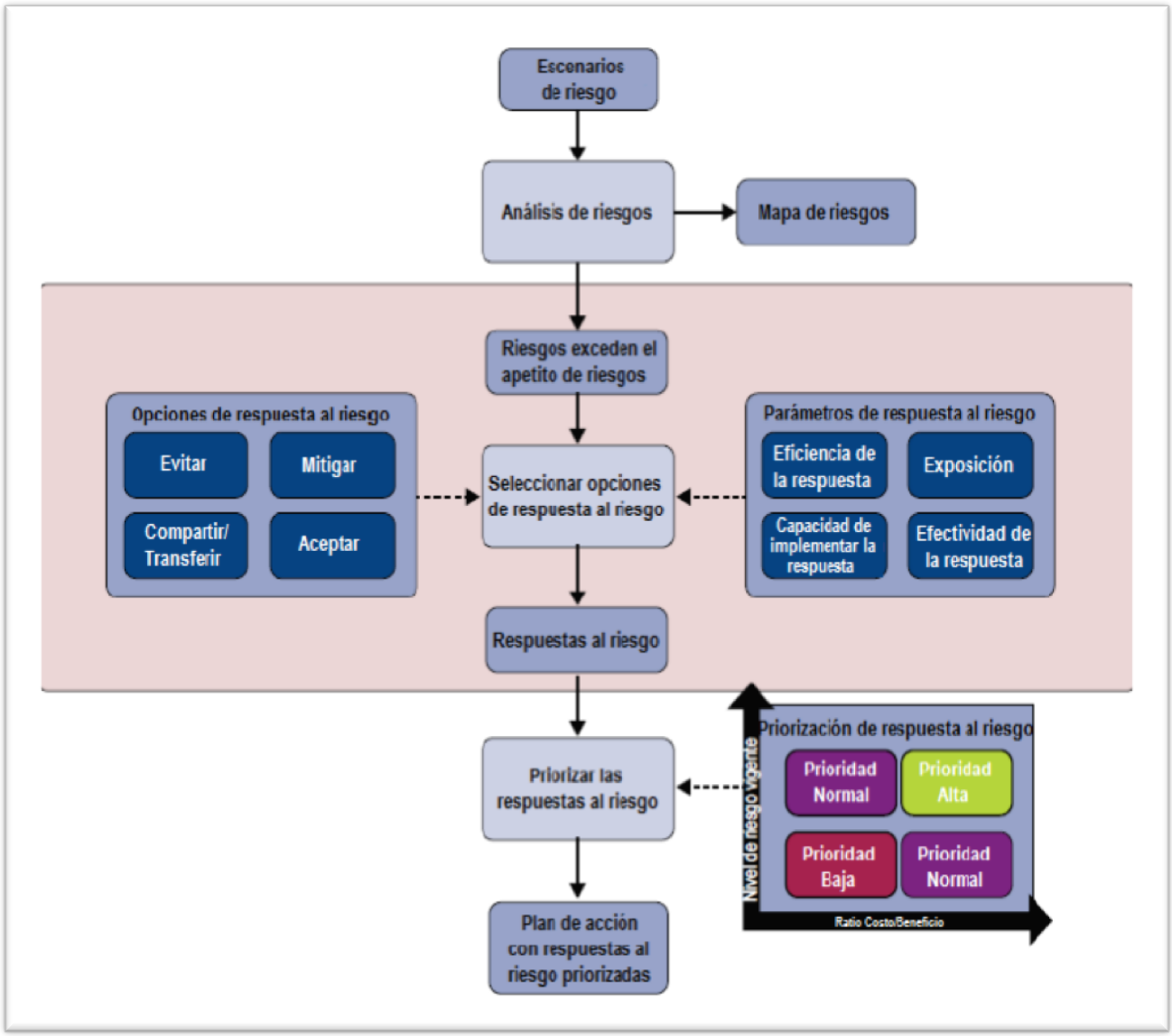
Fuente: tomada de (Isaca, 2017)

| Término | Definición |
|---|---|
| Apetito de riesgo | El nivel de riesgo, a un nivel amplio, que una entidad está dispuesta a aceptar en pos del logro de su misión. |
| Tolerancia al riesgo | El nivel aceptable de variación que la gerencia está dispuesta a permitir para cualquier riesgo en particular, con la finalidad de lograr sus objetivos. |
| Capacidad de riesgo | El nivel objetivo de pérdida que una empresa puede tolerar sin arriesgar su viabilidad. Difiere del apetito del riesgo, el cual es una decisión de la gerencia o del directorio, sobre cuánto riesgo es deseable aceptar. |

Anexo 2: Otros términos de Riesgos

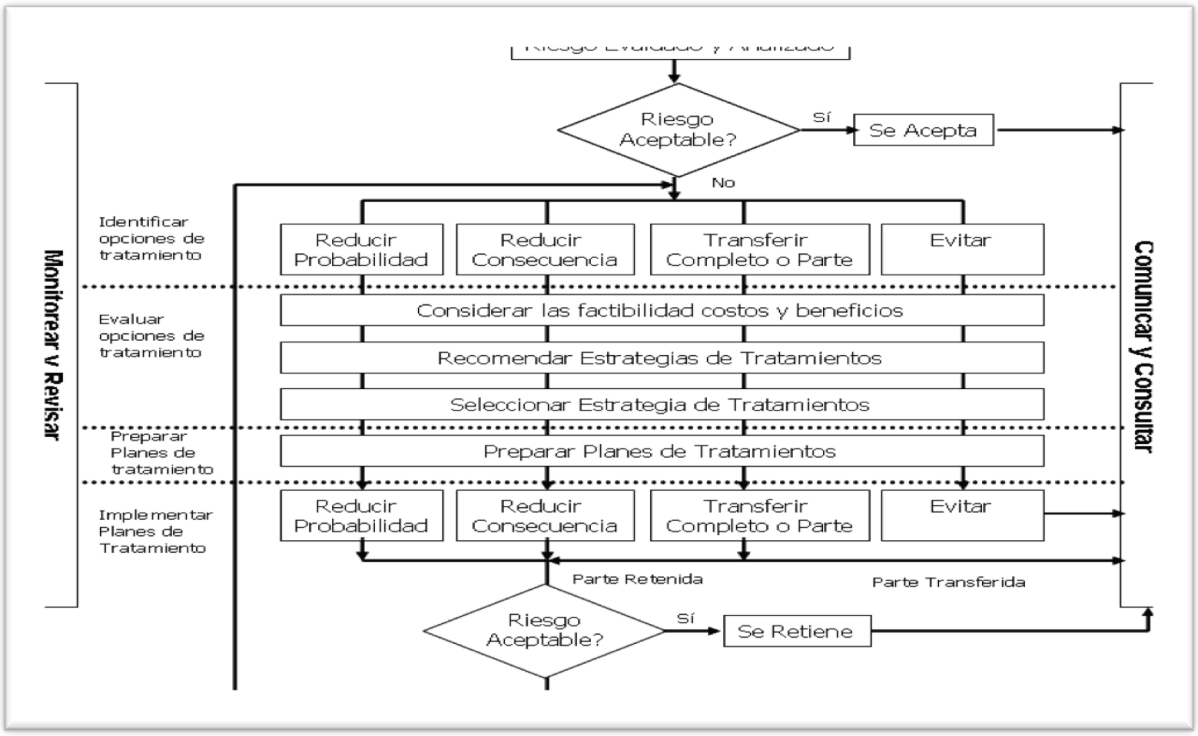
Fuente: tomada de (Isaca, 2017)

2. Análisis de Riesgos




Anexo 3: Proceso de Análisis de Riesgo

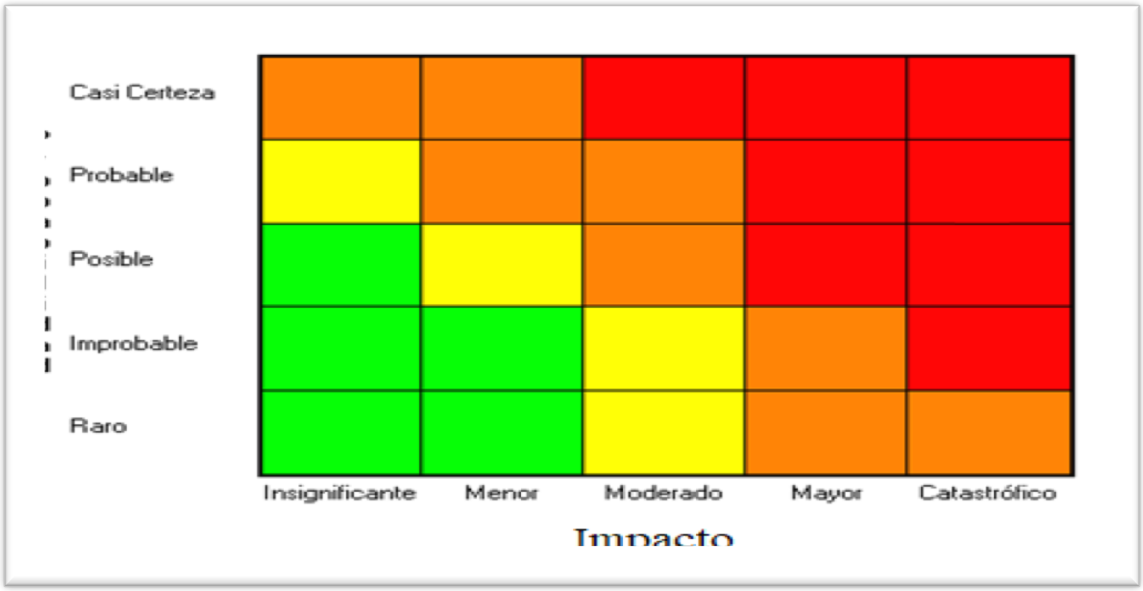
Fuente: tomada de (Isaca, 2017)




Anexo 4: Proceso de Análisis de Riesgo

Fuente: tomada de (Isaca, 2017)

## 3. Mapa de Calor




Anexo 5: Mapa de Calor

Fuente: tomada de (Isaca, 2017)

4. Categorización de Riesgos

| ID | Categoría | Riesgo |
|---|---|---|
| **ID_Cat1** | 11. Establecimiento y mantenimiento del portafolio | c) Riesgo de que no exista una evaluación previa del *software, hardware* o proceso interno al departamento de TI, no cumpliendo así con los requisitos necesarios de compatibilidad de la institución.<br>d) Riesgo de incorrecta asignación de los recursos e incumplimiento de los objetivos prioritarios del negocio. |
| **ID_Cat2** | 12. Pericia y habilidades de TI | c) Riesgo por ausencia de recursos competentes para realizar distintas actividades relacionadas algún rol de trabajo, presentando falta de entrenamiento y conocimiento adecuado ante nuevas tecnologías y procesos básicos.<br>d) Riesgo de no separación de roles y falta de personal con la capacidad de asumir otro puesto en caso de despido, ausencia o incapacidad del personal. |
| **ID_Cat3** | 13. Operaciones del personal (error humano e intento malicioso) | c) Riesgo de falta de compromiso por parte del personal, cometiendo errores o poniendo en peligro cualquier tipo de información, la misma infraestructura, *hardware, software*, entre otros, con intención. (Daño a equipos, pérdida de información, errores en la configuración o inserción de información, etc.)<br>d) Riesgo por daños en dispositivos críticos, como cuarto de servidores o dispositivos de seguridad, etc. |
| **ID_Cat4** | 14. Información (brecha de datos: daño, fuga y acceso) | d) Riesgo en el acceso de información sensitiva e importante de la institución poniendo en peligro la misma al robo o revelación a personas no autorizadas.<br>e) Riesgo por falta de respaldos, no pudiendo utilizarse en caso de presentar archivos corruptos o pérdida de datos.<br>f) Riesgo por mala manipulación de dispositivos de almacenamiento como USB, servidores, CD y discos portátiles. |
| **ID_Cat5** | 15. Infraestructura (hardware, sistemas operativos y tecnología de control) (selección/implementación, operaciones y des patrimonio) | c) Riesgo por fallas intermitentes en la electricidad o telecomunicaciones, que interrumpan las actividades de la institución.<br>d) Riesgo en la carencia de infraestructura para satisfacer nuevos servicios (redes, seguridad, base de datos, almacenamiento, etc.) necesarios para el cumplimiento de objetivos de TI. |

| ID | Categoría | Riesgos |
|---|---|---|
| **ID_Cat6** | 16. *Software* y aplicaciones comunes de forma interna | d) Riesgo de que el *software* aplicativo esté obsoleto (p.ej., tecnologías anticuadas, pobremente documentadas, costosas de mantener, difíciles de entender, no integradas en la arquitectura vigente).<br>e) Riesgo de que no existan procesos adecuados para retornar a versiones anteriores en caso de problemas de compatibilidad con nuevas versiones.<br>f) Riesgo a la mala administración de las bases de datos a nivel interno. |
| **ID_Cat7** | 17. Robo o destrucción de la infraestructura | c) Existe el riesgo de que se haya producido el robo de un dispositivo con datos sensibles o que dispositivos individuales se destruyan accidentalmente.<br>d) Riesgo de que personas sin los suficientes privilegios tengan acceso a las áreas restringidas donde solo el personal de TI debería de accesar. |
| **ID_Cat8** | 18. Código malicioso, Ataques lógicos | d) Riesgo relacionado al robo de datos de la institución a través de accesos no autorizados obtenidos mediante ataques como "*phishing*", troyanos, *ransomware,* virus, etc.<br>e) Riesgo de que usuarios no autorizados traten de forzar el ingreso a los sistemas de la institución.<br>f) Riesgo a la falta de actualizaciones de los equipos y sistemas necesarios (AV, Firmware, FW) |
| **ID_Cat9** | 19. Actos de la naturaleza | b) Existe el riesgo de que la institución se vea afectada por cualquier acto de la naturaleza, por ejemplo, inundaciones, terremoto, tormentas tropicales entre otros que puedan afectar a la institución de manera que no puedan fungir con sus actividades con normalidad. |
| **ID_Cat10** | 20. Innovación | b) No se investigan nuevas tendencias e importantes de TI. |

Anexo 6: Categorización del Riesgo

Fuente: tomada después de la investigación que realizamos, para determinar cuáles son los riesgos que pueden vulnerar las actividades del IMN

## 5. Actividades Criticas

| Departamento de Meteorología Sinóptica y Aeronáutica | | | | |
|---|---|---|---|---|
| **Actividades** | **Criticidad** | **RPO** | **RTO** | **Dispositivos** |
| Disponibilidad de los servicios de Internet | ALTA | Inmediato | 30 min | Enlaces a internet |
| Disponibilidad de los servicios de electricidad | ALTA | Inmediato | 30min | Planta Eléctrica |
| Respaldo digital de la información sinóptica y aeronáutica que corresponda a cada departamento. | ALTA | 30 min | 1h | SAN (Servidor de archivos), NAS (Respaldos), y otros servidores |
| Funcionamiento y equipamiento del sistema de modelación numérica del tiempo. | ALTA | 1h | 5 - 6h | Servidores Web |
| Emitir productos claros, oportunos y eficaces en los ámbitos marino, aéreo y en nuestra área continental. | ALTA | 5-10min | 30min | Servidores Web |
| Funcionamiento, actualización, gestión e implementación del sistema de recepción del satélite GOES. | ALTA | Menos de 1h | 3h | 2 Servidores<br>2 Desplegadores |
| Atender a los medios de comunicación (prensa, radio, televisión, internet) en el departamento. | MEDIA | 24h | 12h | Todos los anteriores |

Anexo 7: Actividades Criticas

Fuente: tomada de Actividades Criticas IMN, referencia (Cuadro de Actividades Criticas y Grado de Criticidad, 2017)

## 6. Plan de Atención de Incidentes

| Actividades | En caso de fallo | Continuidad de la actividad |
|---|---|---|
| **Disponibilidad de los servicios de Internet** | Utilizar el segundo enlace de fibra óptica, si esta falla se llama al proveedor y por ser una institución de gran criticidad el problema lo resuelven casi de inmediato | Acudir a los números de atención inmediata del proveedor de servicios. En este caso el riesgo es aceptado y se debe esperar a que se restaure la conexión. |
| **Disponibilidad de los servicios de electricidad** | Se utiliza la segunda planta de electricidad, esta es un poco vieja (17 años), sin embargo, está en constante mantenimiento | El instituto cuenta con un protocolo bien establecido para la reanudación de la electricidad. El riesgo remanente es aceptado. |
| **Respaldo digital de la información sinóptica y aeronáutica que corresponda a cada departamento.** | Utilización de servidores asignados a respaldos, y en caso necesario acudir a los respaldos almacenados en un sitio alterno | Poner en funcionamiento con servidores alternos y reestablecer los respaldos |

| | | |
|---|---|---|
| **Funcionamiento y equipamiento del sistema de modelación numérica del tiempo.** | Utilización de servidores asignados a respaldos, y en caso necesario acudir a los respaldos almacenados en un sitio alterno | La reanudación del servicio dependerá de si la falla en el equipo es de software o hardware |
| **Emitir productos claros, oportunos y eficaces en los ámbitos marino, aéreo y en nuestra área continental.** | Utilización de servidores asignados a respaldos, y en caso necesario acudir a los respaldos almacenados en un sitio alterno | La reanudación del servicio dependerá de si la falla en el equipo es de software o hardware |
| **Funcionamiento, actualización, gestión e implementación del sistema de recepción del satélite GOES.** | La operación no se verá muy impactada ya que se tiene acceso a un servicio satelital por parte de un ente meteorológico ubicado en US | La reanudación del servicio dependerá de si la falla en el equipo es de software o hardware |
| **Atender a los medios de comunicación (prensa, radio, televisión, internet) en el departamento.** | Se solicita a los medios mantenerse informado por medio de la *página web* y redes sociales por un tiempo ni mayor a 24 horas | Cuando el IMN no se encuentra en alerta roja ya será posible atener a los medios de comunicación con normalidad |

Anexo 8: Plan de Atención de Incidentes

Fuente: tomada de la investigación y análisis realizado en conjunto con el departamento de TI

## 7. Aplicación de Contramedidas

| Categoría | Contramedidas |
|---|---|
| **1. Establecimiento y mantenimiento del portafolio** | a) Revisión previa de una forma exhaustiva y tomando en cuenta cualquier detalle para la implementación de nuevas tecnologías a nivel interno tanto *software* como *hardware,* para que cumplan con los requerimientos básicos.<br>b) Evaluación de todos los recursos antes de darles cualquier asignación, siguiendo el plan ya existe para que se cumplan los objetivos de forma satisfactoria. |
| **2. Pericia y habilidades de TI** | a) Evaluar las necesidades de personal de forma regular o en cambios importantes en la empresa u operativos o entorno a TI para garantizar que la empresa cuenta con los recursos humanos suficientes para apoyar las metas y objetivos de la empresa. En el personal se incluye tanto los recursos internos como los externos.<br>b) Evaluar continuamente los roles y responsabilidades de cada empleado para verificar que se esté cumpliendo de forma adecuada. |
| **3. Operaciones del personal (error humano e intento malicioso)** | a) Constante capacitación para el personal haciéndoles comprender su responsabilidad en el negocio.<br>b) Administrar las instalaciones de forma periódica, incluyéndose los equipos de comunicaciones y de energía, de acuerdo con las leyes y reglamentos, requisitos técnicos y comerciales, las especificaciones del fabricante, y las directrices de seguridad e higiene. |
| **4. Información (brecha de datos: daño, fuga y acceso)** | a) Definir y mantener las responsabilidades de la propiedad de la información (datos) y de los sistemas de información.<br>b) Asegúrese que los usuarios toman las decisiones clasificando la información y los sistemas y revisan la protección de acuerdo con dicha clasificación.<br>c) Establecer un proceso para el resguardo de la información que se encuentre en dispositivos externos o cuando se de errores en la extracción de los mismos. |
| **5. Infraestructura (hardware, sistemas operativos y tecnología de control) (selección/ implementación, operaciones y des patrimonio)** | a) Elaborar un plan para realizar mantenimientos y conocer el estado de los sistemas, así como de la información que maneja el departamento de TI.<br>b) Dar manteniendo y constantes revisiones a los sistemas eléctricos y proveedores de telecomunicaciones.<br>c) Analizar las tecnologías emergentes identificadas y / o otras sugerencias de innovación de TI.<br>d) Trabajar con las partes interesadas para validar las hipótesis sobre el potencial de las nuevas tecnologías y la innovación. |

| Categorias | Contramedidas |
|---|---|
| **6. *Software* y aplicaciones comunes de forma interna** | a) Se realizan pruebas de aceptación de los usuarios y entrenamiento personalizado antes de decisiones de la puesta en marcha, asegurando una transición fluida del nuevo software y que continúe la generación de valor para el negocio. |
| **7. Robo o destrucción de la infraestructura** | a) Los componentes clave de la infraestructura se monitorean 24x7 para hacer un seguimiento del desempeño, disponibilidad, etc.<br>b) Se disparan alarmas en caso de irregularidades y se actúa en forma inmediata.<br>c) El centro de datos se protege adecuadamente, permitiendo sólo el acceso del personal autorizado de TI. |
| **8. Código malicioso, Ataques lógicos** | a) La infraestructura de TI se protege de forma apropiada por medio de *firewalls* y monitoreo continuo de la red, para asegurar la ejecución de las actividades diarias |
| **9. Actos de la naturaleza** | a) Contar con un sitio alterno para reanudar las tareas |
| **10. Innovación** | a) Se impulsa y avala la innovación y la atención a las tendencias, asegurando que se evalúen en forma oportuna las nuevas tecnologías para identificar su impacto en el negocio y que se adopten, si fuera necesario |

Anexo 9: Aplicación de Contramedidas

Fuente: tomada de la investigación y análisis realizado en conjunto con el departamento de TI

# Apéndice

A continuación, encontrará la mención de alguna documentación que logramos identificar y crear a lo largo de la aplicación del Plan de Continuidad, cabe mencionar que solo haremos un listado de productos logrados por motivos de confidencialidad, sin embargo, el IMN tiene cada uno de los documentos sumamente identificados y bien archivados.

a) Plan de políticas para el departamento de TI
b) Clasificación del inventario dependiendo de su criticidad, así como su respectivo responsable
c) Categorización de sus riesgos
d) Videos de simulacros de evacuación de las instalaciones