plan de continuidad operativa

GUÍA PARA DESARROLLAR

Benemérito Cuerpo de Bomberos de Costa Rica

Gestión de Continuidad Operativa

Contenido

[Guía para desarrollar su Plan de Continuidad Operativa 3](#_Toc454993049)

[Propósito 3](#_Toc454993050)

[Marco referencia 4](#_Toc454993051)

[Directriz de Continuidad Operativa 4](#_Toc454993052)

[I Etapa 5](#_Toc454993053)

[Análisis de Criticidad 5](#_Toc454993054)

[Tabla N° 1. Identificación de Procesos 5](#_Toc454993055)

[Tabla N° 2. Registro de Sistemas 6](#_Toc454993056)

[Tabla N° 3. Registro de Activos 6](#_Toc454993057)

[Tiempo máximo de interrupción 7](#_Toc454993058)

[Tabla N° 4. Tiempo de Recuperación 7](#_Toc454993059)

[Nivel de Criticidad 8](#_Toc454993060)

[Tabla N° 5. Valoración del Impacto de los procesos en los objetivos y clientes de su organización 8](#_Toc454993061)

[Tabla N° 6. Nivel de Criticidad de los Procesos de su organización 9](#_Toc454993062)

[II Etapa 10](#_Toc454993063)

[Análisis de Impacto por amenazas 10](#_Toc454993064)

[**1-** **Análisis de Riesgo** 10](#_Toc454993065)

[**2-** **Vulnerabilidad** 10](#_Toc454993066)

[Tabla N° 7. Lista de Amenazas con potencial de afectar la Continuidad Operativa del Benemérito Cuerpo de Bomberos de Costa Rica 11](#_Toc454993067)

[**3-** **Evaluación de Riesgo** 13](#_Toc454993068)

[Tabla N° 8. Probabilidad de los Eventos vs su Impacto 13](#_Toc454993069)

[Tabla N° 9. Lista de impactos posibles sobre los procesos de las dependencias del Benemérito Cuerpo de Bomberos de Costa Rica 14](#_Toc454993070)

[Tabla N° 10. Frecuencia Acumulada de Impactos sobre amen azas 15](#_Toc454993071)

[4- Análisis de Impacto a la Operación 16](#_Toc454993072)

[Tabla N° 12. Análisis de Impacto a la Operación 18](#_Toc454993073)

[Tabla N° 13 Nivel de Criticidad (Impacto vs Probabilidad) 19](#_Toc454993074)

[Tabla N° 14. Severidad y Probabilidad Definiciones 20](#_Toc454993075)

[Tabla N° 15. Mitigación de Riesgos para los Impactos o Fallas 21](#_Toc454993076)

[Tabla N° 16. Hoja de Trabajo para el Plan de Mitigación 22](#_Toc454993077)

[5- Conclusiones 23](#_Toc454993078)

[Anexos 24](#_Toc454993079)

[Anexo I. DIRECTRIZ DE CONTINUIDAD DE LAS OPERACIONES DEL BENEMÉRITO CUERPO DE BOMBEROS DE COSTA RICA 25](#_Toc454993080)

[Anexo II. Lista de Procesos 27](#_Toc454993081)

[Anexo III. Misión, Visión, Valores 29](#_Toc454993082)

[Anexo IV. Objetivos Estratégicos del PLAN ESTRATEGICO INSTITUCIONAL 2014 – 2018. BENEMERITO CUERPO DE BOMBEROS DE COSTA RICA 30](#_Toc454993083)

[Anexo V. Glosario 31](#_Toc454993084)

[Anexo VI. Plan de Gestión de Incidentes Benemérito Cuerpo Bomberos de Costa Rica 40](#_Toc454993085)

# Guía para desarrollar su Plan de Continuidad Operativa

## Propósito

Es propósito de la Dirección General de Bomberos y una obligación de esta Institución, el tener definido las directrices a seguir antes, durante y después de una interrupción de nuestras operaciones. Estas directrices deben estar estructuradas de tal forma que respondan oportunamente ante los eventos que puedan afectar las operaciones y los servicios brindados por la organización. Y que permitan gestionar adecuadamente la continuidad y recuperación de los procesos críticos de nuestras dependencias, con el menor impacto de las operaciones.

El resultado de esta gestión tiene sus orígenes en lo actuado por la Comisión Institucional de Emergencias instaurada en Junio 2013, y en la aprobación de parte de la Dirección General de Bomberos de las actividades conexas para la creación de un Plan Institucional de Continuidad Operativa.

El presente documento es complemento y se da en cumplimiento con lo establecido en el plan original, como un producto requerido para la etapa de preparación y recuperación ante desastres o incidentes con posible impacto negativo en nuestras operaciones. Para el logro de ese objetivo, se requiere realizar los siguientes procesos:

1. Identificación de procesos críticos o funciones principales de la organización
2. Identificación de peligros y amenazas a la continuidad de nuestras operaciones
3. Evaluación de riesgos asociados a esas amenazas
4. Análisis para establecer el impacto potencial a las operaciones críticas de la Institución.
5. Diseño y planificación de las estrategias de mitigación
6. Planes de Respuesta y Recuperación

El conjunto de los resultados del análisis anterior, debe articularse y consolidarse en planes de mitigación, contingencia y continuidad para cada dependencia de nuestra organización.

## Marco referencia

Esta nueva gestión se encuentra en concordancia con lo dispuesto en la Ley General de Control Interno, Ley 8292, en correspondencia con la obligatoriedad de disponer de un sistema de control interno.

En primera instancia y como respuesta a ese requerimiento, la Institución gestionó evaluaciones de los riesgos generales en los niveles macros que podían o estaban en posición de afectar nuestra capacidad operativa. Esto capitalizó información muy valiosa en relación a la exposición al riesgo de nuestra organización, que dio fundamento a planes de mitigación para asuntos críticos, los cuales se han venido gestionando hasta el presente.

Ahora el enfoque ha evolucionado de tal forma que nos lleva a profundizar en niveles más operativos, permitiendo valorar los impactos en las Unidades y Áreas de la Institución. Esta nueva perspectiva permite identificar los procesos críticos, en consideración de los procedimientos formales establecidos, para valorar el impacto real que pueden sufrir esos procesos. Y en consecuencia, el planteamiento de acciones de mitigación. De esta forma la organización podrá realizar un seguimiento más cercano de esas acciones planeadas propiamente por los niveles evaluados de acuerdo a su autoevaluación.

## Directriz de Continuidad Operativa

En concordancia con este compromiso, el Consejo Directivo aprobó la Directriz de continuidad de las operaciones del Benemérito Cuerpo de Bomberos de Costa Rica en el Oficio de aprobación: CBCR-021280-2015-DGB-00716. Ver Anexo I.

Esta Directriz guía a la organización para que todas las actividades del proceso de gestión de la continuidad operativa se lleven a cabo e implementen de la forma acordada y con control. De tal manera que se consiga una capacidad de continuidad que cumpla con las necesidades y retos de la organización acorde con el tamaño y naturaleza de nuestra Institución. Y configura un marco claro y bien definido para lograr y mantener esa capacidad.

# I Etapa

## Análisis de Criticidad

Se trata de la identificación de los procesos críticos o funciones principales de la organización, incluyendo también a los proyectos en construcción o planeamiento que puedan llegar a convertirse en actividades críticas.

Con base en los procedimientos de las áreas de su dependencia y utilizando las herramientas que se dan a continuación, realice el análisis y la determinación de sus procesos críticos. Considere las variables de las herramientas que apliquen para su caso.

Empiece a partir de las Áreas específicas de cada Unidad, realizando el análisis de sus procesos, programas, funciones y procedimientos. Debe identificar otros procesos y sistemas de apoyo y los principales recursos necesarios para mantener las operaciones normales. El análisis debe incluir gente, sistemas, aplicaciones, requerimientos específicos de programas de cómputo, etc. Esto le ayudará a identificar áreas que pueden ser vulnerables durante tiempos de crisis.

El análisis debe incluir un enfoque de prioridad de recuperación de las actividades cuya pérdida tendrían el mayor impacto en el plazo más corto. También deben de identificarse las dependencias externas o internas sobre las cuales se tengan vínculos[[1]](#footnote-1) y que sean de ayuda a las operaciones normales de su Área/Unidad en tiempos de crisis.

1. **Empiece por la identificación de sus procesos con base en sus procedimientos.[[2]](#footnote-2)**

|  |
| --- |
| Tabla N° 1. Identificación de Procesos |
| **Dirección:**  | **Unidad:** |
| **Área:** | **Responsable:** |
| **Procedimiento** | **Código** | **Proceso. [[3]](#footnote-3)** | **Cliente[[4]](#footnote-4)** | **Impacto.[[5]](#footnote-5)** | **Controles[[6]](#footnote-6)** | **Responsable** |
| **1** |  |  |  |  |  |  |  |
| **2** |  |  |  |  |  |  |  |
| **3** |  |  |  |  |  |  |  |

1. **Enumere y describa los sistemas que se operan en cada proceso indicado**.

(Ver en Anexo IV –Glosario- la definición de Sistema Informático).

|  |
| --- |
| Tabla N° 2. Registro de Sistemas |
| **Dirección:**  | **Unidad:** |
| **Área:** | **Responsable:** |
| **Registro de sistema que contiene el Proceso** |
| Proceso | Nombre del Sistema | Descripción | Criticidad  | N° de equipos con la aplicación | Responsable | Contactos Técnicos |
|   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |

Criticidad: Se define en relación a la necesidad del sistema para el funcionamiento de la Unidad

**Rangos de Criticidad:**

|  |  |  |
| --- | --- | --- |
| **1** | El Proceso no puede funcionar sin el sistema | **Alta** |
| **2** | El Proceso puede funcionar parcialmente sin el sistema | **Media** |
| **3** | El Proceso puede funcionar sin el sistema | **Baja** |

1. **A continuación, se enlistan todos los activos que forman parte del proceso y que son necesarios para ejecutarlo.**

|  |
| --- |
| Tabla N° 3. Registro de Activos |
| **Dirección:**  | **Unidad:** |
| **Área:** | **Responsable:** |
| Proceso | Descripción de Activos | Criticidad | Localización |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |

Criticidad: Se define en relación a la necesidad del activo para el funcionamiento de la Unidad

**Rangos de Criticidad:**

1. El Proceso no puede funcionar sin el activo.
2. El Proceso puede funcionar parcialmente sin el activo.
3. El Proceso puede funcionar sin el activo.

## Tiempo máximo de interrupción

Para cada proceso, se determinará el tiempo máximo de interrupción, especificando cuántos días puede permanecer en interrupción el proceso sin incurrir en un impacto sustancial para la organización. Los de menor tiempo son más críticos.

|  |
| --- |
| Tabla N° 4. Tiempo de Recuperación |
| **Dirección:**  | **Unidad:** |
| **Área:** | **Responsable:** |
| **Proceso** | **Necesidades de Recuperación** | **Criticidad** |
|   |   |   |
|   |   |   |
|   |   |   |
|   |   |   |
|   |   |   |
|   |   |   |
|   |   |   |
|   |   |   |

**Necesidad de Recuperación y Criticidad**

|  |  |  |
| --- | --- | --- |
| **1** | Día cero, recuperación inmediata.Día 1-7: El proceso debe ser recuperado entre el primer y sétimo día después de un incidente. | **Alta** |
| **2** | Día 7-30: El proceso debe ser recuperado después de la primera semana y antes de un mes | **Media** |
| **3** | Más 30 días: El proceso puede esperar más de 30 días a ser recuperado | **Baja** |

## Nivel de Criticidad

Para seleccionar los procesos críticos, se puede realizar una evaluación de los procesos en el marco de la información anterior valorando de qué manera impactan en el giro de su operación.

Una vez listados los procesos actuales de su dependencia - utilice la lista de procesos derivados del análisis anterior-, puede evaluarlos según los dos criterios mostrados en la matriz mostrada abajo (Impacto en objetivos de la organización y en el cliente propio de la dependencia), y situarlos en la matriz según la combinación de resultados (cuadrantes). Los que queden situados en la línea roja y amarilla pueden ser considerados críticos para el éxito de la organización.

Los objetivos de la organización se refieren a los objetivos aprobados para su Área o dependencia en función de la Misión, los Objetivos y los Valores Institucionales.[[7]](#footnote-7)

Los clientes en la matriz, indica la razón de ser de la dependencia, a quienes dirige sus propios procesos y servicios.

|  |
| --- |
| Tabla N° 5. Valoración del Impacto de los procesos en los objetivos y clientes de su organización |
| **Impacto en los objetivos de la Organización** | *Alto* | MEDIO | ALTO | ALTO |
| *Medio* | BAJO | MEDIO | ALTO |
| *Bajo* | BAJO | BAJO | MEDIO |
|   |   | *Bajo* | *Medio* | *Alto* |
| **Impacto en sus Clientes** |

La evaluación del impacto de los procesos de su dependencia, se deberá realizar con este criterio (Tabla N° 5) y en consideración de los procedimientos pertinentes del proceso evaluado. En la Tabla N° 6 se ilustra cómo debería hacerse el análisis. Y es esta la Tabla para documentar los resultados.

|  |
| --- |
| Tabla N° 6. Nivel de Criticidad de los Procesos de su organización |
| **Dependencia:** | *Gestión de Recursos Económicos* |
| **Procesos** | **ProcedimientosPor Código o Nombre** | **Impacto en los Objetivos de la Organización** |  **Impacto en sus Clientes** | **Criticidad** |
| *ejemplo:* ***Captación*** | Procedimiento 1 (2-01-01-037) | M | B | BAJO |
| Procedimiento 2 | A | M | ALTO |
| Procedimiento 3 | B | A | MEDIO |
| Procedimiento 4 | M | M | MEDIO |
| Procedimiento 5 | M | B | BAJO |
| Procedimiento 6 | B | B | BAJO |
| Procedimiento 7 | B | M | BAJO |
| Procedimiento 8 |   |   |   |
| … |   |   |   |
| … |   |   |   |
| Procedimiento N | M | A | ALTO |

Esta matriz identifica los Procesos/Procedimientos que son críticos para su organización en función del servicio prestado por medio de ellos a sus clientes. Estos serán los procesos/procedimientos que van a utilizarse en el Análisis de impacto a la operación de su dependencia en la Tabla N° 12 Análisis de Impacto a la Operación.

*Fin I Etapa[[8]](#footnote-8)*

# II Etapa

## Análisis de Impacto por amenazas

El enfoque de la segunda etapa es identificar las amenazas para la continuidad operativa de nuestra organización y la evaluación de los riesgos correspondientes. Este proceso se realizará considerando principalmente el impacto que esas amenazas pudieran tener sobre la organización y no solamente en la probabilidad de ocurrencia. Esto logra poner al descubierto los riesgos de baja probabilidad, pero con consecuencias importantes.

1. **Análisis de Riesgo**

Para el análisis del riesgo expuesto por las amenazas a nuestra organización, vamos a estudiar la vulnerabilidad, el impacto y evaluar el riesgo real que nos afecta.

1. **Vulnerabilidad**

El objetivo del análisis de vulnerabilidad es lograr identificar aquellos eventos que se pueden convertir en una amenaza para la organización, en este sentido, este primer apartado se enfocará a identificar propiamente los eventos que se puedan convertir en amenazas reales y jerarquizarlas.

Con base en la experiencia de los análisis realizados por la organización anteriormente, complementado con la retroalimentación de la estadística histórica y las actuales condiciones de riesgo del ambiente nacional, así como las condiciones generales de la infraestructura y facilidades propias de la organización, se definió una amplia lista de amenazas posibles de afectar nuestra continuidad operativa.

Esta lista incluye eventos en las siguientes categorías de amenazas:

* Amenazas Naturales
* Amenazas Accidentales
* Ataques intencionados
* Amenazas Financieras
* Amenazas Tecnológicas
* Otras amenazas

 A continuación, se detallan aquellas que efectivamente pueden convertirse en amenaza real para el Cuerpo de Bomberos. Esta lista refleja la experiencia de la organización en análisis anteriores y se complementa con un análisis del entorno de las condiciones actuales. Así mismo fue validada -junto con los posibles impactos- por la organización en la figura del Comité de Continuidad Operativa.

### Tabla N° 7. Lista de Amenazas con potencial de afectar la Continuidad Operativa del Benemérito Cuerpo de Bomberos de Costa Rica

1 Abuso de privilegios de acceso

2 Acceso no autorizado a datos de la compañía

3 Accesos no autorizados al edificio

4 Accidentes del personal

5 Actividad Volcánica

6 Actos de vandalismo

7 Amenaza expresada hacia la Organización

8 Ataque cibernético deja internet inusable por una semana

9 Ataque cibernético destruye 50% de la información interna y o las aplicaciones

10 Capacidad inadecuada de las comunicaciones (teléfono, internet, fax, correo…)

11 Copias incontroladas de documentos/software/datos

12 Corrupción de datos

13 Descarga de software no controlada

14 Edificio no disponible por tres meses

15 Errores de operación

16 Errores en el mantenimiento

17 Errores intencionados

18 Exceso de humedad

19 Fallo de la UPS

20 Fallo de suministro eléctrico

21 Fallo del aire acondicionado

22 Fallo/degradación de las comunicaciones (teléfono, internet, fax, correo…)

23 Fallo/degradación del hardware

24 Fallos de los sistemas de autenticación/autorización

25 Fallos en las copias de seguridad de la base de datos temporal

26 Fraude

27 Huelgas y manifestaciones externas

28 Humo, gases tóxicos

29 Incendio

30 Incumplimientos legales intencionados

31 Incumplimientos legales no intencionales

32 Infraestructura Externa no disponible por una semana

33 Infraestructura Externa no disponible por tres meses

34 Interceptación de las líneas de comunicación

35 Introducción de virus en los sistemas

36 Inundación

37 Mal uso de equipo

38 Manipulación de datos/software

39 Manipulación de hardware

40 Manipulación de las líneas de comunicación

41 Pandemia

42 Pérdida de confidencialidad

43 Robo de documentos

44 Robo de equipos

45 Robo de software

46 Robos intencionados

47 Sabotaje

48 Secuestro

49 Sismo fuerte

50 Subida de tensión en el suministro eléctrico

51 Tormentas Eléctricas

52 Uso de software por personal no autorizado

53 Violencia en el Trabajo

*Nota. Esta lista inicialmente no tiene ningún orden preferencial, se indica alfabéticamente.*

1. **Evaluación de Riesgo**

El riesgo definido como la probabilidad de ocurrencia de un evento (amenaza) en relación con su impacto, consta de dos componentes que, al asociarse, permiten medir y priorizar los riesgos.

Dada esta situación cada uno de los eventos o amenazas a la que se ve expuesta la organización, se convierte en un riesgo de nivel bajo, medio o alto dependiendo de la probabilidad y el impacto que pueda ocasionar.

Por lo que, para poder realizar el análisis, se hace necesario generar una matriz que permita medir el nivel de riesgo, haciendo coincidir la probabilidad con el impacto en relación a los eventos que fueron identificados, tal como se muestra a continuación.

|  |
| --- |
| Tabla N° 8. Probabilidad de los Eventos vs su Impacto |
| **Probabilidad**  | *Alto* | MEDIO | ALTO | ALTO |
| *Medio* | BAJO | MEDIO | ALTO |
| *Bajo* | BAJO | BAJO | MEDIO |
|   | *Bajo* | *Medio* | *Alto* |
| **Impacto** |

Para lograr el análisis planteado se han identificado una amplia lista de impactos posibles sobre los procesos de nuestras dependencias. Estos serán asociados con las amenazas para identificar aquellos impactos con más alta influencia potencial sobre nuestras operaciones y así hacer el correspondiente análisis de impacto en los procesos críticos para la continuidad operativa.

### Tabla N° 9. Lista[[9]](#footnote-9) de impactos posibles sobre los procesos de las dependencias del Benemérito Cuerpo de Bomberos de Costa Rica

|  |  |
| --- | --- |
| Id | Impactos[[10]](#footnote-10) |
| a | Afectación de la Calidad del Servicio |
| b | Incumplimiento Legal |
| c | Registro Financiero Erróneo |
| d | Práctica Contable Inaceptable |
| e | Interrupción de la Operación |
| f | Costo Excesivo |
| g | Pérdida Financiera |
| h | Pérdida de Activos |
| i | Desventaja Competitiva |
| j | Fraude/Conflicto de Intereses |
| k | Información Gerencial Errónea |
| l | Penalización Legal |
| m | Pérdida Total de un Departamento o Dependencia |
| n | Daño parcial significativo de un Departamento o Servicio |
| ñ | Fallo parcial significativo del Sistema de Tecnología de Información |
| o | Pérdida o daño de la información o datos |
| p | Pérdida o interrupción de instalaciones primarias |
| q | Pérdida personal (Pandemia) |
| r | Pérdida de Proveedores |
| s | Edificio no disponible por una semana |
| t | Edificio no disponible por tres meses |
| u | Ataque cibernético destruye 50% de la información interna y o las aplicaciones |
| v | Ataque cibernético deja internet inusable por una semana |
| x | Infraestructura Externa no disponible por una semana |
| y | Infraestructura Externa no disponible por tres meses |
| z | Pérdida de Imagen |

### Tabla N° 10. Frecuencia Acumulada de Impactos sobre amen azas

Para entender mejor cuales impactos son los más relevantes para la Institución, se hace un análisis de frecuencia de los impactos que podrían aparecer en nuestra institución derivados de las amenazas identificadas

|  |  |  |
| --- | --- | --- |
| **Impactos** | **Relevancia** | **Frecuencia Acumulada** |
| Infraestructura Externa no disponible por tres meses | 0% | 0% |
| Infraestructura Externa no disponible por una semana | 0% | 0% |
| Edificio no disponible por tres meses | 1% | 1% |
| Ataque cibernético destruye 50% de la información interna y o las aplicaciones | 1% | 2% |
| Ataque cibernético deja internet inusable por una semana | 1% | 2% |
| Pérdida personal (Pandemia) | 1% | 3% |
| Pérdida de Proveedores | 1% | 4% |
| Pérdida Total de un Departamento o Dependencia | 2% | 6% |
| Edificio no disponible por una semana | 2% | 8% |
| Pérdida o interrupción de instalaciones primarias | 3% | 11% |
| Práctica Contable Inaceptable | 3% | 14% |
| Pérdida Financiera | 3% | 17% |
| Pérdida de Activos | 4% | 21% |
| Desventaja Competitiva | 4% | 24% |
| Fallo parcial significativo del Sistema de Tecnología de Información | 4% | 28% |
| Registro Financiero Erróneo | 4% | 32% |
| Costo Excesivo | 4% | 36% |
| Incumplimiento Legal | 5% | 41% |
| Penalización Legal | 5% | 46% |
| Fraude/Conflicto de Intereses | 6% | 52% |
| Información Gerencial Errónea | 6% | 57% |
| Interrupción de la Operación | 6% | 64% |
| Daño parcial significativo de un Departamento o Servicio | 8% | 71% |
| Pérdida o daño de la información o datos | 9% | 80% |
| Pérdida de Imagen | 9% | 89% |
| Afectación de la Calidad del Servicio | 11% | 100% |
| **Total de interacciones Amenaza vs impactos = 428 eventos** | **100%** |

Los elementos dentro del rango crítico (+41%), son los impactos más relevantes para la organización, en función de su posible afectación de nuestras operaciones cuando se confrontan las amenazas potenciales. Esos impactos son los que vamos a considerar para la Evaluación de Riesgo e Impacto para los **procesos críticos** identificados anteriormente.

|  |
| --- |
| **Tabla N° 11. Impactos más Relevantes** |
| 1 | Afectación de la Calidad del Servicio |
| 2 | Pérdida de Imagen |
| 3 | Pérdida o daño de la información o datos |
| 4 | Daño parcial significativo de un Departamento o Servicio |
| 5 | Interrupción de la Operación |
| 6 | Información Gerencial Errónea |
| 7 | Fraude/Conflicto de Intereses |
| 8 | Penalización Legal |
| 9 | Incumplimiento Legal |

1. **Análisis de Impacto a la Operación**

El Análisis de Impacto a la Operación no es un ejercicio que se puede delegar a cualquier colaborador. El peso de las decisiones a tomarse en el curso del análisis es muy importante por lo que es recomendable que los responsables de los procesos participen personalmente (con el apoyo de expertos y analistas en el campo). El responsable del proceso es el que establece los requisitos y los criterios para su implementación, no necesariamente el que lo ejecuta.

Este es un proceso sistemático para realizar una evaluación de impacto y riesgo de las operaciones de su organización y desarrollar un plan de mitigación para aminorar aquellos que causan fallas en sus procesos críticos, antes de puedan ocurrir. El propósito es reducir o eliminar el impacto de una variedad de amenazas.

Se trata de determinar anticipadamente el efecto de los impactos en sus funciones críticas, para así maximizar la velocidad de retorno a la normalidad, después de un incidente.

Se indican aquellos impactos que identificamos con mayor probabilidad de ocurrencia después de analizar los efectos posibles que se derivarían de las amenazas (Tabla 10. Impactos más Relevantes)

Como herramienta para reunir toda la información relacionada, usted debe completar la Tabla #11 Análisis de Impacto a la Operación. En la columna B anotar cada proceso crítico. Inicie con los procedimientos que determinaron ser más críticos (Alto y Medio) a los procesos en el análisis anterior (Fase I, Tabla 6. Nivel de Criticidad de los Procesos de su organización) - Use líneas separadas-.

En la columna C anote los vínculos o dependencias críticas a este proceso. Considere Grupos internos y externos, proveedores, recursos críticos o subprocesos. Grupos con los que tiene dependencias o enlaces críticos con fin de mantener cada función o proceso anotado.

La columna D se describe cuáles controles tiene su dependencia para asegurar que el procedimiento se está realizando correctamente y/o que no se deja de hacer.

En la columna E debe valorar si esos controles que tiene implementados son realmente efectivos y mantienen el proceso dentro de las expectativas dictadas y requeridas por la organización.

Con base en los impactos que se facilitan en la tabla columna F y que fueron identificados válidos para toda la organización (Ver Tabla 10), evalúe cualquier otro impacto específico adicional asociado a las funciones de sus procesos críticos y procedimientos de apoyo que podrían causar un fallo. Haga las siguientes preguntas para evaluar si esos impactos específicos a su dependencia son probables:

¿Qué es lo peor que podría suceder? ¿Qué es lo peor que le ha sucedido a esta organización? ¿Cuáles son las interfaces críticas con otros grupos internos que le más le preocupan? ¿Por qué? ¿Cuáles son sus expectativas sobre los acuerdos de nivel de servicio con grupos internos? Después de realizar este ejercicio, agregue cualquier otro impacto adicional a la función o proceso crítico que corresponda.

Evalúe cada uno de los procesos y procedimientos críticos y sus recursos de apoyo. Valórelos contra los impactos listados en la columna F para determinar la severidad del impacto y la probabilidad de ocurrencia. Anote sus calificaciones en columnas G y H.

* Utilice las categorías y definiciones descritas en la Tabla N° 14. Definiciones, que se adjunta abajo como una guía para definir las categorías de severidad y probabilidad del impacto. Recuerde es solo una guía para ayudarle, no necesariamente debe cumplirse de la forma indicada en la tabla, úsela solamente como referencia.
* Asegúrese de que la clasificación de la severidad del impacto y la probabilidad de ocurrencia que usted indica, refleja los impactos con los controles indicados funcionando.
* Defina la gravedad potencial del impacto, por ejemplo, A = alto, M = medio, B = bajo
* Defina la posibilidad de que este impacto o fallo ocurra, por ejemplo, A = alto, M = medio, B = bajo
* Si un impacto no aplica, simplemente indíquelo así mismo (n/a).

Con base en su clasificación para la severidad del impacto y probabilidad de ocurrencia, indique si se requiere la mitigación del riesgo anotando un "Sí" o un "No" en la columna I.

* Todos los elementos con una calificación alta/alta y/o alto/medio serán sujetos de un Plan de Mitigación.[[11]](#footnote-11)
* Su organización también puede actuar sobre elementos con calificaciones más bajas, especialmente si hay una solución económica viable y evidente para eliminar completamente o reducir la probabilidad y/o el impacto.

Continúe trabajando con la matriz de análisis de impacto hasta que haya completado toda la información para cada proceso crítico. Utilice la lista de dependencias para validar las expectativas de lo que otras organizaciones y sus proveedores serán capaces de proporcionar durante una crisis. Esto le facilitará desarrollar consecuentemente sus planes. Es importante comprender lo que ellos serán capaces de ofrecer durante una emergencia y que tan bien preparados están para afrontar posibles interrupciones de las operaciones, a corto plazo y largo plazo.

### Tabla N° 12. Análisis de Impacto a la Operación

|  |
| --- |
| **Tabla N° 12. Análisis de Impacto a la Operación** |
| **Organización***~~: ejemplo~~*= Servicios FinancierosGestión de Recursos Financieros | **Hecho por** |  |
| **Fecha** |  | **Fecha de Revisión** |  |
| **Aprobado por** |  | **Fecha de Aprobación** |  |
| **Misión de la Organización** |  |
| **Proceso o función** | Captación | **Responsable** |  |
| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** |
|  | **Procesos Críticos** | **Vínculos y Recursos** | **Describa los controles existentes** | **¿Son estos controles efectivos?****(Si o No)** | **Impactos** | **Severidad del Impacto A/M/B** | **Probabilidad de Ocurrencia A/M/B** | **Requiere Mitigación****Si/No** |
| 1.1 | Depósitos no Identificados | BancosContabilidad....Otros | Doble chequeo de lo realizado (dos personas)Hecho por, revisado por, aprobado por.Conciliaciones bancarias. |  | Afectación de la Calidad del Servicio | A | B | Si |
| Pérdida de Imagen | A | B | Si |
| Pérdida o daño de la información o datos | A | B | Si |
| Daño parcial significativo de un Departamento o Servicio | B | B | No |
| Interrupción de la Operación | A | M | Si |
| Información Gerencial Errónea | B | B | No |
| Fraude/Conflicto de Intereses | B | M | No |
| Penalización Legal | B | B | No |
| Incumplimiento Legal | A | B | Si |
| 1.2 | Gestión de Cobro |  |  |  |  |  |  |  |

**Criterio de selección:** Para determinar el nivel de criticidad e identificar cuáles son sus procesos que requieren ser mitigados. Los procesos que coincidan con niveles Medio y Alto serán sujetos de Planes de Mitigación.

### Tabla N° 13 Nivel de Criticidad (Impacto vs Probabilidad)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nivel del Impacto sobre los objetivos de la Organización**(Severidad) | *Alto* | MEDIO (SI) | ALTO (SI) | ALTO (SI) |
| *Medio* | BAJO | MEDIO(SI) | ALTO (SI) |
| *Bajo* | BAJO | BAJO | MEDIO (SI) |
| **NIVEL DE CRITICIDAD***Los que coincidan con niveles Medio y Alto serán sujetos de Planes de Mitigación.* | *Baja* | *Media* | *Alta* |
| **Probabilidad de Ocurrencia** |

### Tabla N° 14. Severidad y Probabilidad Definiciones



### Tabla N° 15. Mitigación de Riesgos para los Impactos o Fallas

|  |
| --- |
| **Tabla N° 15. Mitigación de Riesgos para los Impactos o Fallas** |
| **(#) Área:** | **Proceso crítico: 1.1 Depósitos no Identificados** |
| **Ref. #**  | **Impactos/Fallas** *Describa y anote solo los ítems que requieren Plan de Mitigación* | **Suposiciones o consideraciones[[12]](#footnote-12)***.* | **Opciones[[13]](#footnote-13)** | **CostoEstimado** | **Reducción del Riesgo**[[14]](#footnote-14) |
| a)       | Incumplimiento Legal |   | Opción 1 – No hacer nada  |   | 0% |
|   | Opción 2-  |   |   |
|   | Opción 3 –  |   | 100% |
|   | Opción 4 – Hacer todo |   |   |
| b)       | Penalización Legal |   | Opción 1– No hacer nada |   |   |
|   | Opción 2 –  |   |   |
|   | Opción 3 -  |   |   |
|   | Opción 4 – Hacer todo |   |   |
| c)        | Información Gerencial Errónea |   | Opción 1– No hacer nada |   |   |
|   | Opción 2 |   |   |
|   | Opción 3 |   |   |
|   | Opción 4 –Hacer todo |   |   |
| e)       | Fraude/Conflicto de Intereses |   | Opción 1– No hacer nada |   |   |
|   | Opción 2 |   |   |
|   | Opción 3 |   |   |
|   | Opción 4 –Hacer todo |   |   |
| i)         | Afectación de la Calidad del Servicio |   | Opción 1– No hacer nada |   |   |
|   | Opción 2 |   |   |
|   | Opción 3 |   |   |
|   | Opción 4 –Hacer todo |   |   |

### Tabla N° 16. Hoja de Trabajo para el Plan de Mitigación

|  |  |  |  |
| --- | --- | --- | --- |
| Organización (Dependencia)  | ***Servicios Financieros******Gestión de Recursos Financieros*** | Proceso | ***Captación*** |
| Proceso Crítico | ***Depósitos no Identificados*** | Impacto/falla | ***Incumplimiento Legal*** |
| Fecha |  | Fecha de Revisión |  |
| Aprobado por |  | Fecha de Aprobación |  |
| Opción 2: \_\_\_\_\_\_\_\_\_\_\_\_\_ | **1st Semestre** | **2nd Segundo Semestre** | **Siguientes años** |
| **Actividades de Reducción del Riesgo** | * **Actividad 1**
* **Actividad 2**
* **Actividad 3**
 | * **Actividad 4**
* **Actividad 5**
* **Actividad 6**
 | * **Actividad 7**
* **Actividad 8**
* **Actividad 9**
 |
| **Resultado esperado de Reducción de Riesgo** | * **Resultado 1**
* **Resultado 2**
* **Resultado 3**
 | * **Resultado 4**
* **Resultado 5**
* **Resultado 6**
 | * **Resultado 7**
* **Resultado 8**
* **Resultado 9**
 |

1. **Conclusiones**

Después de haber realizado el Análisis de Criticidad con lo cual se identificaron sus procesos críticos en la I Etapa de este estudio, y concluido el Análisis de Impacto a la Operación en la Etapa II. Se ha logrado definir cuáles de sus procesos críticos requieren un plan de mitigación y consecuentemente se ha planteado ese plan para su dependencia.

Ese plan se establece en una línea de tiempo que incluye la planificación de los recursos requeridos, en concierto con el alcance o logro final de mitigación propuesto en sus planteamientos.

Considerando toda esta valiosa información y en función de los impactos más comunes que pudieran afectar su dependencia -a pesar de la mitigación lograda-. Cuando se materialice un incidente con impacto en nuestra organización, su dependencia debe estar preparada para dar una respuesta inicial que minimice los efectos negativos en su misión. Ahora procede desarrollar su propio Plan de Gestión de Incidente. Para este efecto se adjunta como Anexo el formato aprobado.

La base de su Plan de Gestión de Incidente, se realiza en consideración de las siguientes situaciones que podrían generarse durante una emergencia:

I. Pérdida de espacio o área de la oficina

II. Pérdida de red y conectividad

III. Pérdida o daño de la información o datos

IV. Pérdida de infraestructura externa (Electricidad, Agua, Accesos).

V. Daño parcial significativo de un Departamento o Servicio

VI. Pérdida parcial y significativa del Recurso Humano

El objetivo principal de este Plan, es reestablecer la capacidad del personal de su dependencia, para continuar brindando un servicio profesional y oportuno al Benemérito Cuerpo de Bomberos de Costa Rica cuando un evento o situación de emergencia impacte nuestra capacidad de operación. El enfoque de esta respuesta se hace en función de evitar o minimizar al máximo:

1 Afectación de la Calidad del Servicio

2 Pérdida de Imagen

3 Interrupción de la Operación

4 Información Gerencial Errónea

5 Penalización y o incumplimiento Legal

6 Otros vinculados o derivados de las situaciones planteadas anteriormente

# Anexos

**Anexo I. DIRECTRIZ DE CONTINUIDAD DE LAS OPERACIONES DEL BENEMÉRITO CUERPO DE BOMBEROS DE COSTA RICA**

Propósito

Definir las directrices a seguir antes, durante y después de una interrupción de las operaciones del Cuerpo de Bomberos, que respondan oportunamente ante eventos que afecten las operaciones y servicios brindados por la organización, así como gestionar la continuidad y recuperación de los procesos, con el menor impacto de las operaciones.

Generalidad

La presente normativa se encuentra en concordancia con lo dispuesto en la Ley General de Control Interno, Ley 8292, en correspondencia con la obligatoriedad de disponer de un sistema de control interno.

Alcance y ámbito de aplicación

Esta directriz deberá cumplirse a nivel institucional, en consideración primeramente de la protección de la vida humana, el patrimonio y el medio ambiente.

Competencia de aprobación

El Consejo Directivo como dirección superior del Cuerpo de Bomberos, es el llamado a la aprobación de la presente directriz, de conformidad con la importancia del proceso de continuidad de las operaciones del Cuerpo de Bomberos y la responsabilidad emanada por la misión organizacional.

Responsabilidades

**Consejo Directivo**

Dicta la normativa pertinente para el cumplimiento de la Ley del Cuerpo de Bomberos, de manera que se garantice la prestación de los servicios que brinda la organización de forma ininterrumpida.

**Administración del Cuerpo de Bomberos**

Generar los procesos y verifica el cumplimiento de lo correspondiente de conformidad con las funciones que describe la Ley del Cuerpo de Bomberos.

**Directriz de continuidad de las operaciones**

El Consejo Directivo reconoce que es responsabilidad del Cuerpo de Bomberos de Costa Rica, promover la prestación ininterrumpida de los servicios de protección, cuando la vida, los bienes y el medio ambiente se encuentran amenazados por incendios y situaciones de emergencia; por tanto, instruye a la Dirección General de Bomberos, gestionar la continuidad de las operaciones necesarias para el cumplimiento de este fin.

Esta gestión requiere una preparación permanente de todos los miembros del Cuerpo de Bomberos, de sus procesos y sistemas, por lo que la Administración deberá adoptar formas de interiorizar la continuidad de las operaciones al quehacer diario e integrarla en las decisiones y programas, como una guía para el logro de los objetivos institucionales.

Se crea la Comisión del Plan de Continuidad Operativa, como ente responsable de este proceso, bajo la coordinación del Director General de Bomberos, Director Operativo, el Director Administrativo y el encargado de Planificación.

Expectativas para la organización

1.  Mantener el Programa de Continuidad Operativa, como un elemento principal de nuestros valores.

2.  En todos los niveles se debe interiorizar los principios de la continuidad de las operaciones, enfatizando en los procesos críticos de la organización.

3. En todo nuevo proceso, función o proyecto de relevancia institucional, deben ser incluidas las medidas de mitigación del riesgo asociado.

4.  Determinar y proporcionar los recursos necesarios para establecer, operar y mantener el Sistema de Gestión de Continuidad Operativa.

5. Actualizar de forma anual el Sistema de Gestión de Continuidad Operativa.

**Anexo II. Lista de Procesos**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dirección | **Unidad** | **Área** | **Proceso** | **Proc.** |
| **Dirección Administrativa** | Servicios Financieros | Gestión de Recursos Financieros | Captación | 8 |
| Presupuesto | 8 |
| Inversiones | 5 |
| Tesorería | Adquisición de Bienes y Servicios | 6 |
| Registros Económicos | 2 |
| Obligaciones Institucionales | 2 |
| Contabilidad | Elaboración de Estados Financieros | 10 |
| Consultas y Solicitudes | 4 |
| Reportes | 2 |
|  Total de Procedimientos | **47** |
| Servicios Generales | Servicios Logísticos | Contratación Administrativa | 2 |
| Control de Acceso | 2 |
| Flotilla | 4 |
| Planilla | 1 |
| Seguros | 2 |
| Servicios Públicos | 3 |
| Tarjetas Institucionales | 1 |
| Viáticos | 1 |
| Aprovisionamiento | Control de Inventarios | 7 |
| Pagos | 1 |
| Edificaciones | Compras | 1 |
| Construcciones | 7 |
| Materiales y Herramientas | 2 |
| Total de Procedimientos | 34 |
| Proveeduría |   | Control de Gestión de Garantía, Conciliaciones, Caja Fuerte | 2 |
| Control de Correspondencia | 2 |
| Control de Gestión | 18 |
| Control de Pago | 2 |
| Control de Orden de Compra | 1 |
| Control de Multas y Control de Reajuste de precio | 1 |
| Control de Muestras | 1 |
| Sistema de Registro de Proveedores | 1 |
| Plan Anual de Compras | 1 |
|  Total de Procedimientos | **29** |
| Recursos Humanos | Gestión del Cliente Interno | Administración de Personal | 7 |
| Reclutamiento y Selección de Personal | 4 |
| Planillas | 4 |
| Servicios de Gestión y Apoyo | 1 |
| Administrativo | 2 |
|   |  Total de Procedimientos |   | **18** |
| Mantenimiento de Vehículos |   | Reportes | 1 |
| Mantenimiento Correctivo | 1 |
| Mantenimiento Preventivo | 1 |
| Total de Procedimientos   | **3** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Dirección Operativa** | Academia Nacional de Bomberos | Administrativo | 12 |
| Campo de Entrenamiento | 3 |
| Docente | 11 |
| Servicios de Capacitación Empresarial | 3 |
|   |   |   |  **29** |
| Prevención e Investigación de Incendios | Control Preventivo | Visado de Planos | 7 |
| Control de Proyectos | 5 |
| Hidrantes | 6 |
| SINEPCI | 1 |
| Salud Ocupacional | 1 |
|   | **20** |
| Promoción e Investigación | Caravana de la Rana | 1 |
| Investigación de Incendios | 6 |
| Administrativos | 5 |
|   | **12** |
|   |   |   | 61 |
| Tecnologías de Información y Telecomunicaciones | Oficina de Comunicaciones (Área de OCO) |  Pendiente |   |
|   |   |   |
| Servicios Técnicos (Área de Soporte Técnico) |  Pendiente |   |
|   |  |   |
| Proyectos y Sistemas (Área de Sistemas de Información) |  Pendiente |   |
|   |  |   |
| Área de Infraestructura |  Pendiente |   |
|   |  |   |
| Área de Apoyo Administrativo |  Pendiente |   |
|   |  |   |
| Procedimiento Normativa |  Pendiente |   |
|   |   |   |
|   |   |   |   |
| Operaciones | Jefes de Batallón Permanentes |  Pendiente |   |
| Jefes de Estación |  Pendiente |   |
| Jefatura de Bomberos Voluntarios |  Pendiente |   |
| Jefes de Batallón Voluntarios |  Pendiente |   |
| Jefes de Compañía |  Pendiente |   |
|   |   |

**Anexo III. Misión, Visión, Valores**

**MISION**

Brindar a la sociedad costarricense protección cuando la vida, los bienes y el medio ambiente se encuentren amenazados por incendios y situaciones de emergencia, basados en los más altos principios humanos y en la búsqueda permanente de la excelencia.

**VISION**

Ser una organización estatal de primera respuesta reconocida por sus altos estándares de calidad, eficacia y eficiencia, al atender las emergencias de su competencia y proveer servicios de prevención de incendios que integralmente contribuyan al desarrollo del país, mediante la mejora de los índices de protección a la vida, la propiedad y el medio ambiente.

VALORES DEL CUERPO DE BOMBEROS

1. Abnegación: Actitud voluntaria para ayudar a las personas sin esperar nada a cambio.

2. Honor: Cualidad para comportarse apropiadamente ante el deber.

3. Disciplina: Actitud para acatar las normas, protocolos, lineamientos y procedimientos que rigen las actividades que realiza la organización.

4. Trabajo en Equipo:

Actitud de participación en forma conjunta de todos sus miembros en la ejecución de sus actividades.

5. Solidaridad:

Actitud de fraternidad para identificarse con las personas afectadas por condiciones adversas.

6. Servicio

Disposición de respuesta con actitud de entrega, colaboración y espíritu de atención.

7. Responsabilidad:

Cumplir los deberes y competencias del Benemérito Cuerpo de Bomberos de Costa Rica, realizando de manera correcta las actividades encomendadas.

8. Preservación del Patrimonio:

Actitud de legar el conocimiento, costumbres, tradiciones y salvaguardar los bienes de la organización para concienciar y preservar la historia.

9. Honestidad:

Actuar con apego a los principios y valores éticos.

**Anexo IV.** Objetivos Estratégicos del PLAN ESTRATEGICO INSTITUCIONAL 2014 – 2018. BENEMERITO CUERPO DE BOMBEROS DE COSTA RICA

1. **Sostenibilidad Financiera**. Fortalecer el sistema financiero administrativo, de manera que acreciente su capacidad de gestión eficiente de los recursos económicos y responda a la satisfacción de las necesidades de la ciudadanía.
2. **Mejora de la capacidad de respuesta operativa**. Dotar de la infraestructura, plataforma tecnológica, equipo y recurso humano que la organización requiere, para el cumplimiento de su misión, de conformidad con los acuerdos tomados por el Consejo Directivo y la disponibilidad de recursos
3. **Desarrollo de gestión organizacional.** Promover el alineamiento estratégico de la estructura organizativa, el desarrollo de competencias, capacidades de gestión, normativa y ambiente laboral, adecuado para el logro de objetivos coherentes con el marco estratégico institucional.
4. **Desarrollo de una cultura de prevención.** Contribuir al desarrollo de una cultura de prevención, para la reducción de la frecuencia e impacto de las emergencias propias de la competencia del Cuerpo de Bomberos, acorde con los recursos y legislación existente.
5. **Posicionamiento de la Imagen institucional.** Posicionar la imagen del Benemérito Cuerpo de Bomberos de Costa Rica de acuerdo con el marco estratégico de la organización, logrando percepciones, actitudes y comportamientos en pro del cumplimiento de los objetivos de la Organización.
6. **ESTRATEGIAS TRANSVERSALES**
* Mantener altos estándares de capacitación
* Actuación con responsabilidad social
* Gestión comprometida con el uso sostenible del ambiente

**Anexo V. Glosario**

|  |  |  |
| --- | --- | --- |
| 1 | ***Abuso de privilegios de acceso***  | *Uso inapropiado o no autorizado de la administración de usuarios, grupos u otros privilegios, así como los permisos otorgados, en contradicción con la configuración y la estrategia puesta en práctica por el administrador de su sistema* |
| 2 | ***Acceso no autorizado a datos de la compañía***  | *Un acceso no autorizado es producto de la explotación de una vulnerabilidad en el sistema.En el caso de Tecnología de Información se refiere al acceso del servidor o en alguna de sus aplicaciones o la utilización de algún otro método para subir privilegios como fuerza bruta, Software malicioso (malware), sniffers (analizador de paquetes) u obteniendo información confidencial a través de la manipulación de usuarios legítimos (ingeniería social), entre otros.* |
| 3 | ***Accesos no autorizados al edificio***  | *Explotación de una vulnerabilidad del sistema de custodia y control del edificio* |
| 4 | ***Accidentes del personal***  | *Todo accidente que le suceda al trabajador como causa de la labor que ejecuta o como consecuencia deésta, durante el tiempo que permanece bajo la dirección y dependencia del patrono o sus representantes, y que puede producirle la muerte o pérdida o reducción, temporal o permanente, de la capacidad para el trabajo. Ver Artículo 196 de La Ley sobre Riesgos del Trabajo.* |
| 5 | ***Actividad*** | *Proceso o conjunto de procesos realizados por la organización o en su nombre que produzca o apoye uno o más productos o servicios* |
| 6 | ***Actividad Volcánica*** |  *Es la salida de productos gaseosos, líquidos y sólidos lanzados por las explosiones o erupciones de un volcán*  |
| 7 | ***Actividad Volcánica*** |  *Es la salida de productos gaseosos, líquidos y sólidos lanzados por las explosiones o erupciones de un volcán*  |
| 8 | ***Actividades criticas*** | *Actividades que tendrán que llevarse a cabo para entregar los productos y servicios fundamentales que permiten a una organización cumplir sus objetivos más importantes y sensibles al cumplimiento de plazos.* |
| 9 | ***Actos de vandalismo***  | *Designa la hostilidad hacia la propiedad, llegando al deterioro e, incluso, destrucción voluntaria de activos. Para Tecnologías de la Información y Comunicación se refiere a las modificaciones no autorizadas ni deseadas de páginas web mediante “crackeo o cracking”.*  |
| 10 | ***Afectación de la Calidad del Servicio*** | *Cuando se afecta negativamente la capacidad de la organización para satisfacer plenamente los servicios a los clientes externos e internos.* |
| 11 | ***Amenaza*** | *Eventos que atenten directa o indirectamente la capacidad de la organización para cumplir con nuestra misión* |
| 12 | ***Amenazas accidentales*** | *Son aquellos eventos que tienen relación con la actividad humana, en la cual no media una intención de causar un daño, por lo que se puede establecer como accidental, por lo general es difícil identificar un causante* |
| 13 | ***Amenazas Financieras*** | *Aquellos eventos relacionados con la actividad financiera de la organización, para el caso específico del Cuerpo de Bomberos, aquellos que atenten directamente con el oportuno manejo de recursos financieros o la estabilidad de los ingresos de la organización* |
| 14 | ***Amenazas Naturales*** | *Son aquellas que tienen un origen en un evento que se presenta en la naturaleza, el cual tiene una predicción, de días y en algunos casos son totalmente impredecibles* |
| 15 | ***Amenazas por ataques intencionados*** | *Aquellos eventos también relacionados con la actividad humana, en el cual existe un componente de delito, existiendo intención de causar daño y puede ser factible identificar al individuo causante del mismo.*  |
| 16 | ***Análisis de Impacto*** | *Procesos de análisis de funciones de la organización y el efecto que una interrupción podría tener sobre dichas funciones* |
| 17 | ***Ataque cibernético deja internet inusable por una semana*** | *Evento malintencionado que deja sin internet a la organización o dependencia por una semana.* |
| 18 | ***Ataque cibernético destruye 50% de la información interna y o las aplicaciones*** | *Evento malintencionado que destruye el 50% de la información y datos de la organización o dependencia*  |
| 19 | ***Ataques intencionados*** | *Eventos dirigidos hacia la organización con el objetivo de dañar ya sea a sus procesos, funcionarios, los activos asignados, productos o servicios o la imagen, que pueden causar una paralización de las operaciones* |
| 20 | ***Auditoría*** | *Examen sistemático para determinar si las actividades y los resultados relacionados se ajustan a las previsiones planificadas y si estas previsiones se ponen en práctica de forma eficaz y son aptas para alcanzar la directriz y los objetivos de continuidad operativa de la organización* |
| 22 | ***Capacidad inadecuada de las comunicaciones*** | *Hoy en día mantener la comunicación por los medios tales como teléfono, internet, fax o correo, es indispensable, una capacidad inadecuada, se presenta cuando existe personal clave de la organización que no tiene acceso a estos medios, o existen lugares aislados de comunicación.* |
| 23 | ***Capacidad inadecuada de las comunicaciones (teléfono, internet, fax, correo…)***  | *Cuando la capacidad instalada es insuficiente para atender los servicios de la organización.* |
| 24 | ***Contingencia:***  | *Situación que puede o no suceder* |
| 25 | ***Continuidad Operativa*** | *Capacidad estratégica y táctica de la organización de planificar y responder ante incidentes e interrupciones para continuar las operaciones en un nivel aceptable predefinido* |
| 26 | ***Copias incontroladas de documentos/software/datos***  | *Cuando el control de documentos físicos o digitales, software y datos no garantiza el manejo confidencial y por autorización.* |
| 27 | ***Corrupción de datos***  | *Errores en los datos informáticos que se producen durante la transmisión o la recuperación, la introducción de cambios no deseados a los datos originales.* |
| 28 | ***Costo Excesivo*** | *Costo que supera lo presupuestado o que se manifiesta en forma desmesurada* |
| 29 | ***Daño parcial significativo de un Departamento o Servicio*** | *Cuando se limita a una dependencia y tiene efectos importantes en su capacidad y desempeño* |
| 30 | ***Daños accidentales*** | *Aquéllas pérdidas que ocurren con la incidencia de eventos causados de forma accidental, bien por funcionarios de la organización como por terceras personas y que causan la paralización de las operaciones* |
| 31 | ***Desastres naturales*** | *Eventos o fenómenos naturales como terremotos, inundaciones, deslizamientos de tierra, deforestación, contaminación ambiental y otros. Los fenómenos naturales, como la lluvia, terremotos, huracanes o el viento, se convierten en desastre cuando superan un límite de normalidad, medido generalmente a través de un parámetro* |
| 32 | ***Descarga de software no controlada***  | *Ver Acceso no autorizado* |
| 33 | ***Desventaja Competitiva*** | *Acto o evento que se manifiesta en una disminución de la capacidad de la organización para mantener la excelencia de los servicios.* |
| 34 | ***Edificio no disponible por tres meses*** | *Cuando un evento no permite la plena utilización de uno de nuestros edificios por ese periodo.* |
| 35 | ***Edificio no disponible por una semana*** | *Cuando un evento no permite la plena utilización de uno de nuestros edificios por ese periodo.* |
| 36 | ***Ejercicio*** | *Actividad en la que el plan o los planes de continuidad operativa se ensayan en parte o íntegramente para procurar que el plan o los planes contengan la información apropiada y que produzcan el resultado deseado cuando se lleven a cabo. (Simulaciones o simulacros)* |
| 37 | ***Emergencias Médicas*** | *Se denominan así a las situaciones donde está en riesgo la vida del paciente y se hace necesaria su atención en forma inmediata* |
| 38 | ***Errores de operación***  | *Cuando hay una desviación en los protocolos aprobados para la operación y manipulación de los sistemas y activos propios, y que derivan en consecuencias no deseadas.* |
| 39 | ***Errores de operación:***  | *Desviación sobre los procesos o métodos aceptados que provoca una inexactitud o equivocación en los resultados, productos o servicios pactados* |
| 40 | ***Errores en el mantenimiento***  | *Cuando hay una desviación en los protocolos aprobados para el mantenimiento de los sistemas y activos propios y que derivan en consecuencias no deseadas.* |
| 41 | ***Errores intencionados*** | *Esto se pueden presentar en el manejo de cualquier información, en la confección de cualquier informe, en la inclusión de datos falsos en salidas, o información financiera* |
| 42 | ***Errores intencionados***  | *Cuando hay una desviación intencional en los protocolos aprobados para la operación y manipulación de los sistemas y activos propios con consecuencias no deseadas* |
| 43 | ***Estrategia de continuidad operativa*** | *Enfoque de la organización que proporciona recuperación y continuidad ante un desastre u otro incidente importante con interrupción de las operaciones* |
| 44 | ***Evaluación de Riesgos*** | *Identificación de los riegos, determinación de la probabilidad de ocurrencia y la vulnerabilidad de las personas, propiedades, medio ambiente y de la entidad misma ante aquellos riesgos.*  |
| 45 | ***Exceso de humedad***  | *Cuando las condiciones y grado de humedad puedan o afecten negativamente sistemas o activos propios sensibles* |
| 46 | ***Fallo de la UPS*** | *Se entiende aquella situación, que se da cuando ante la falta de fluido eléctrico por cualquier motivo, la UPS de respaldo no se activa* |
| 47 | ***Fallo de la UPS***  | *Se entiende aquella situación, que se da cuando ante la falta de fluido eléctrico por cualquier motivo, la UPS de respaldo no se activa* |
| 48 | ***Fallo de suministro eléctrico***  | *Evento con impacto negativo en la capacidad de operación de nuestros equipos o edificios.* |
| 49 | ***Fallo del aire acondicionado*** |  *Se entiende aquella situación, que se da cuando un aire acondicionado que se considera indispensable para el funcionamiento de un equipo presenta problemas de funcionamiento, por ejemplo, aires acondicionados en Data Center* |
| 50 | ***Fallo del aire acondicionado***  |  *Se entiende aquella situación, que se da cuando un aire acondicionado que se considera indispensable para el funcionamiento de un equipo presenta problemas de funcionamiento, por ejemplo, aires acondicionados en Data Center* |
| 51 | ***Fallo parcial significativo del Sistema de Tecnología de Información*** | *Cuando la capacidad de operación del sistema se ve disminuida con efectos negativos importantes en los procesos y tareas pertinentes* |
| 52 | ***Fallo/degradación de las comunicaciones*** | *Puede que se tengan los medios de comunicación, sin embargo, los mismos pueden fallar por múltiples razones como sistemas o cortes accidentales de cables. También debe considerarse la obsolescencia de los equipos.* |
| 53 | ***Fallo/degradación de las comunicaciones (teléfono, internet, fax, correo…)*** | *Puede que se tengan los medios de comunicación, sin embargo, los mismos pueden fallar por múltiples razones como sistemas o cortes accidentales de cables* |
| 54 | ***Fallo/degradación del hardware***  | *Deterioro lento del desempeño del software con el tiempo o su decreciente capacidad de respuesta que conducirá eventualmente a convertirse en defectuoso, inusable, u obsoleto y en necesidad de ser actualizado.* |
| 57 | ***Fraude***  | *1. Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete.2. Acto tendente a eludir una disposición legal en perjuicio del Estado o de terceros.3. Delito que comete el encargado de vigilar la ejecución de contratos públicos, o de algunos privados, confabulándose con la representación de los intereses opuestos.* |
| 58 | ***Fraude/Conflicto de Intereses*** | *Ver Fraude* |
| 59 | ***Fuego fortuito*** |  *Incendio que se origina de una manera fortuita, por ejemplo, una mala instalación eléctrica* |
| 60 | ***Fuego fortuito*** |  *Incendio que se origina de una manera fortuita, por ejemplo, una mala instalación eléctrica* |
| 62 | ***Gestión de continuidad operativa*** | *Proceso de gestión integral que identifica amenazas potenciales para la organización y el impacto en las operaciones que dichas amenazas, caso de materializarse, puedan causar, y que proporciona un marco para aumentar la capacidad de reacción de la organización con capacidad para dar una respuesta eficaz que salvaguarde los intereses de sus grupos de interés, reputación, imagen y actividades de creación de valores fundamentales.* |
| 64 | ***Humo, gases tóxicos*** | *Estos se pueden generar por un incendio cercano, por actividades externas cercanas a nuestras instalaciones o por el uso de sustancias peligrosas, que podrían ocasionar una suspensión de las actividades.* |
| 65 | ***Humo, gases tóxicos***  | *Estos se pueden generar por un incendio cercano, por actividades externas cercanas a nuestras instalaciones o por el uso de sustancias peligrosas, que podrían ocasionar una suspensión de las actividades.* |
| 66 | ***Impacto*** | *Consecuencia evaluada de un resultado en particular* |
| 67 | ***Incidente*** | *Situación que pudiera ser, o podría redundar en una interrupción operativa, pérdida, emergencia o crisis* |
| 68 | ***Incumplimiento Legal*** | *Delito de acción u omisión realizado por uno o más Funcionarios Públicos, en contra de la Administración Pública o de particulares.* |
| 69 | ***Incumplimientos legales intencionados*** | *ver incumplimiento legal* |
| 70 | ***Incumplimientos legales no intencionales*** | *ver incumplimiento legal* |
| 71 | ***Información Gerencial Errónea*** | *Información que por sus características puede inducir a la gerencia a ejercer una mala toma de decisiones con perjuicio de la organización* |
| 72 | ***Infraestructura Externa no disponible por tres meses*** | *Cuando un evento o condición no permite la plena utilización de la infraestructura pública con afectación de los servicios y operaciones de la organización por el lapso señalado.* |
| 73 | ***Infraestructura Externa no disponible por una semana*** | *Cuando un evento o condición no permite la plena utilización de la infraestructura pública con afectación de los servicios y operaciones de la organización por el lapso señalado.* |
| 74 | ***Interceptación de las líneas de comunicación***  | *Cuando se da un acceso no autorizado en los sistemas de comunicación con posible mala intención.* |
| 75 | ***Interrupción*** | *Acontecimiento, previsto o imprevisto, que causa una desviación negativa no planificada con respecto a la entrega esperada de productos o servicios según los objetivos de la organización* |
| 76 | ***Interrupción de la Operación*** | *Acontecimiento, previsto o imprevisto, que causa una desviación negativa no planificada con respecto a la entrega esperada de productos o servicios según los objetivos de la organización* |
| 77 | ***Introducción de virus en los sistemas*** | *Como un evento intencionado es una de las formas de afectar los sistemas* |
| 80 | ***Inundación fortuita*** |  *A diferencia de una inundación normal, ésta se produce por causas tales como ruptura de tuberías, problemas con canoas o techos.* |
| 81 | ***Inundaciones*** | *Es la ocupación por parte del agua de zonas que habitualmente están libres de ésta, ya sea por desbordamiento de ríos, por lluvias torrenciales, o subida de las mareas por encima del nivel habitual* |
| 82 | ***Invocación*** | *Acto de declarar que el plan de continuidad operativa debe ponerse en marcha para seguir entregando productos y servicios fundamentales* |
| 85 | ***Manipulación de hardware*** | *Como evento intencionado, existe la posibilidad de que una persona que desee dañar a la organización, dañe alguno de los equipos esenciales principalmente que brindan sostenimiento a los sistemas.* |
| 88 | ***Objetivo de plazo de recuperación*** | *Plazo marcado para la reanudación de entrega de productos, servicios o actividad tras producirse un incidente. Debe ser inferior que el periodo máximo de interrupción tolerable.* |
| 89 | ***Otras amenazas*** | *Aquellos eventos que puedan afectar la imagen de la organización o representar una demanda por responsabilidad civil ante las acciones ejecutadas por miembros del Cuerpo de Bomberos en el manejo de las emergencias.* |
| 90 | ***Pandemia*** | *Se trata de una enfermedad epidémica que afecta a diversos países y que ataca a casi todas las personas de una región geográfica. Se llama pandemia a la propagación mundial de una nueva enfermedad. Se produce una pandemia de gripe cuando surge un nuevo virus gripal que se propaga por el mundo y la mayoría de las personas no tienen inmunidad contra él.*  |
| 91 | ***Pandemia*** | *Se trata de una enfermedad epidémica que afecta a diversos países y que ataca a casi todas las personas de una región geográfica. Se llama pandemia a la propagación mundial de una nueva enfermedad. Se produce una pandemia de gripe cuando surge un nuevo virus gripal que se propaga por el mundo y la mayoría de las personas no tienen inmunidad contra él.*  |
| 95 | ***Pérdida de imagen*** | *La imagen de la organización, es una de las más fuertes a nivel nacional, por lo tanto, un evento noticioso que involucre de mala manera a un miembro de nuestra organización repercutiría inmediatamente.* |
| 103 | ***Periodo máximo de interrupción tolerable*** | *Tiempo tras el cual la viabilidad de la organización estará irrevocablemente amenazada si no puede reanudarse la entrega de productos y servicios* |
| 104 | ***Plan de Contingencia***  | *Conjunto de procedimientos alternativos al funcionamiento normal de la Organización, cuando alguna de sus funciones usuales se ve perjudicada por una contingencia interna o externa.*  |
| 105 | ***Plan de Continuidad Operativa*** | *Conjunto de procedimientos e información documentados que se desarrolla, compila y mantiene preparado para uso en caso de producirse un incidente, para permitir a la organización seguir desempeñando sus actividades críticas a un nivel aceptable predefinido* |
| 107 | ***Prevención*** | *Actividades, tareas, programas y sistemas que tienen por objeto evitar o intervenir para detener un incidente o evitar que ocurra* |
| 110 | ***Resiliencia*** | *Capacidad de reacción. Capacidad de la organización de resistir los efectos de un incidente* |
| 111 | ***Responsabilidad Civil*** | *Hoy en día estamos expuestos a responder ante la comunidad costarricense por nuestras acciones, las cuales pueden causar un perjuicio creando por ende una responsabilidad de nuestra parte.* |
| 112 | ***Riesgo alto*** | *Cuando al presentare un evento, los daños son extensos con media o alta probabilidad de ocurrencia, o daños moderados con alta probabilidad, atentando contra la continuidad operativa de la organización* |
| 113 | ***Riesgo bajo*** | *Aquellos eventos que tienen una baja o media probabilidad y sus daños en caso de presentarse serian mínimos.* |
| 114 | ***Riesgo medio*** | *Espectro de eventos que tienen alta probabilidad, pero su impacto sería mínimo, o tiene una probabilidad media con impactos medios o pocas probabilidades, pero en caso de presentarse los daños serian extensos.* |
| 121 | ***Sismo*** | *Fenómeno de sacudida brusca y pasajera de la corteza terrestre producida por la liberación de energía acumulada en forma de ondas, las cuales pueden causar dependiendo de la intensidad daños en la infraestructura.* |
| 123 | ***Sistema de gestión de continuidad operativa*** | *Es la parte del sistema de gestión general que establece, implementa, opera, supervisa, revisa, mantiene y mejora la continuidad de operativa de la organización. El sistema de gestión incluye la estructura organizativa, directrices, actividades de planificación, responsabilidades, procedimientos, procesos y recursos.* |
| 124 | ***Sistema Informático*** | *Un sistema informático (SI) es un sistema que permite almacenar y procesar información; es el conjunto de partes interrelacionadas: hardware, software y personal informático. El hardware incluye computadoras o cualquier tipo de dispositivo electrónico, que consisten en procesadores, memoria, sistemas de almacenamiento externo, etc. El software incluye al sistema operativo, firmware y aplicaciones, siendo especialmente importante los sistemas de gestión de bases de datos. El soporte humano incluye al personal técnico que crean y mantienen el sistema (analistas, programadores, operarios, etcétera) y a los usuarios que lo utilizan.* |
| 126 | ***Suspensión, o subida de tensión en eléctrica*** | *No solo la suspensión del servicio eléctrico puede generar problemas de continuidad operativa, también se pueden dar por cambios en la tensión, de ingreso al edificio, situación que puede quemar nuestros equipos.* |
| 128 | ***Urgencias Médicas*** | *Se denomina urgencia médica a las situaciones en las cuales la vida del paciente no está en riesgo, ni están comprometidos sus órganos vitales, pero su situación puede agravarse si no es atendido en un tiempo breve*  |
| 129 | ***Uso de software por personal no autorizado*** | *Esta amenaza es muy común, hoy en día, sin embargo, existen medio para limitarla. Acceso no autorizado a datos de la organización. Nuestra organización genera mucha información, la cual se debe manejar con mucha discreción, principalmente por aspectos legales.* |
| 131 | ***Uso mal intencionado de los equipos*** | *Un funcionario podría operar un equipo de una manera errónea buscando causarle algún daño al mismo equipo o causar un daño con éste.* |
| 133 | ***Vulnerabilidad*** | *Las vulnerabilidades son debilidades que pueden ser explotadas para convertir una amenaza en un riesgo real que puede causar daños graves en una compañía. Las vulnerabilidades en sí mismas no causan daño alguno, sino que es una condición o un conjunto de condiciones que pueden permitir a una amenaza afectar a un activo* |

**Anexo VI. Plan de Gestión de Incidentes Benemérito Cuerpo Bomberos de Costa Rica**

***Dependencia: \_\_\_\_\_\_\_\_\_\_\_\_\_***

Revisión: 0.0

Fecha de Revisión: \_\_\_\_\_\_\_\_\_

1. Vínculos se refiere a las relaciones o dependencias importantes que tiene el proceso con otras áreas o unidades internas y también con terceros externos. [↑](#footnote-ref-1)
2. Utilice el formato en Excel facilitado. [↑](#footnote-ref-2)
3. Proceso al cual pertenece el procedimiento. Si no tiene definido un proceso formal, considere cual sería un proceso natural al que debería incluirse este procedimiento. Proceso: Conjunto de actividades o eventos que se realizan o suceden –alternativa o simultáneamente- con un determinado fin. Estas actividades se distinguen porque son sujetas de Planeación, Organización, Dirección y Control administrativo y generan resultados. Para nuestros fines, cada proceso se ejecuta por medio de procedimientos [↑](#footnote-ref-3)
4. Cliente: A quienes se debe el proceso. El elemento dentro de la organización, que toma el resultado o producto de un proceso como recurso para realizar su propio proceso. [↑](#footnote-ref-4)
5. Descripción de cuál es el riesgo o impacto probable que pueda derivarse de la ejecución incorrecta de este procedimiento. [↑](#footnote-ref-5)
6. Los controles que tiene su área sobre cada procedimiento para asegurar su cumplimiento y aplicación correcta. Controles para evitar el desvío de la línea del procedimiento. [↑](#footnote-ref-6)
7. Ver Anexo IV: Objetivos Estratégicos del PLAN ESTRATEGICO INSTITUCIONAL 2014 – 2018. BENEMERITO CUERPO DE BOMBEROS DE COSTA RICA [↑](#footnote-ref-7)
8. Hasta aquí la fase de identificación de los procesos críticos para ser llevados al análisis. Pueden agregarse otros a criterio de su dependencia. [↑](#footnote-ref-8)
9. La lista inicialmente no tiene ningún orden preferencial [↑](#footnote-ref-9)
10. Estos impactos se medirán en función de su posibilidad de ocurrencia en los escenarios que presentan cada una de las amenazas identificadas como posibles de afectar la organización. [↑](#footnote-ref-10)
11. Puede utilizar también la Tabla N° 13. Nivel de Criticidad adjunta abajo para facilitar este análisis. [↑](#footnote-ref-11)
12. Anote si es necesario, cualquier situación que limite o influya las opciones [↑](#footnote-ref-12)
13. Puede agregar más opciones si es necesario. Para otras opciones no indicadas, redacte su propuesta en forma general. En la siguiente Tabla #15 se dará el detalle requerido. [↑](#footnote-ref-13)
14. Use Alto: A, Medio: M, Bajo: B o indique el porcentaje de reducción [↑](#footnote-ref-14)