RESOLUCIÓN PRESIDENCIAL Nº 051 - 2014 / OSINFOR

Lima, 11 JUL. 2014

VISTO:

El Memorándum N° 084-2014-OSINFOR/05.1 de la Oficina de Tecnología de la Información, el Informe N° 008-2014-OSINFOR/04.1.1 de la Sub Oficina de Planeamiento y el Memorándum N° 538-2014-OSINFOR/04.1 emitido por la Oficina de Planeamiento y Presupuesto, el Informe Legal N° 052-2014-OSINFOR/04.2, y;

CONSIDERANDO:

Que, mediante Decreto Legislativo N° 1085, se creó el Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre – OSINFOR como un Organismo Público Ejecutor adscrito a la Presidencia del Consejo de Ministros, con personería jurídica de derecho público interno, encargado a nivel nacional de supervisar y fiscalizar el aprovechamiento sostenible y la conservación de los recursos forestales y de fauna silvestre, así como de los servicios ambientales provenientes del bosque, entre otras facultades otorgadas;

Que, mediante Ley N° 28716, Ley de Control Interno de las Entidades del Estado, se establecen las normas para regular la elaboración, aprobación, implantación funcionamiento, perfeccionamiento y evaluación del control interno en las entidades del Estado, con el propósito de cautelar y fortalecer los sistemas administrativos y operativos con acciones y actividades de control previo, simultáneo y posterior, contra los actos y prácticas indebidas o de corrupción, propendiendo al debido y transparente logro de los fines, objetivos y metas institucionales;

Que, dicha norma establece en su artículo 4° que las entidades del Estado implantan obligatoriamente sistemas de control interno en sus procesos, actividades, recursos, operaciones y actos institucionales, orientando su ejecución al cumplimiento de los objetivos siguientes: a) Promover y optimizar la eficiencia, eficacia, transparencia y economía en las operaciones de la entidad, así como la calidad de los servicios públicos que presta, b) Cuidar y resguardar los recursos y bienes del Estado contra cualquier forma de pérdida, deterioro, uso indebido y actos ilegales, así como, en general, contra todo hecho irregular o situación perjudicial que pudiera afectarlos, c) Cumplir la normatividad aplicable a la entidad y sus operaciones, d) Garantizar la confiabilidad y oportunidad de la información, e) Fomentar e impulsar la práctica de valores institucionales, f) Promover el cumplimiento de los funcionarios o servidores públicos de rendir cuenta por los fondos y bienes públicos a su cargo y/o por una misión u objetivo encargado y aceptado, correspondiendo al Titular y a los funcionarios responsables de los órganos directivos y ejecutivos de la entidad, la aprobación de las disposiciones y acciones necesarias para la implantación de dichos sistemas y que éstos sean oportunos, razonables, integrados y congruentes con las competencias y atribuciones de las respectivas entidades;

Que, asimismo, mediante Resolución Ministerial N° 129-2012-PCM se aprobó el uso obligatorio de la Norma Técnica Peruana *"NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. Requisitos"* en todas las entidades integrantes del Sistema Nacional de Informática;

Que, la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática, establece la Política de Seguridad de la Información con el objeto de dirigir y dar soporte a la gestión de la seguridad de la información, en concordancia con los requerimientos de la institución y la normatividad vigente;

Que, acorde a lo señalado, las diversas unidades orgánicas del OSINFOR, en su constante compromiso de mejoramiento, vienen revisando su normativa a efectos de solicitar la aprobación de nuevos documentos de gestión, con la finalidad de mejorar y optimizar las labores de cada una de ellas;

Que, bajo ese contexto, la Oficina de Tecnología de la Información, en el marco de su competencia, ha elaborado el Plan de Contingencia Informático de la Oficina de Tecnología de la Información de OSINFOR, como un instrumento de gestión en pro de establecer las estrategias de respuesta que permitan atender de forma oportuna, eficiente y eficaz, el desastre, permitiendo así prever las medidas de seguridad que garanticen la continuidad del funcionamiento de nuestros sistemas;

Que, de conformidad al numeral 25.10 del artículo 25° del Reglamento de Organización y Funciones – ROF del OSINFOR, aprobado por Decreto Supremo N° 065-2009-PCM, la Sub Oficina de Planeamiento de la Oficina de Planeamiento y Presupuesto, mediante Informe N° 008-2014-OSINFOR/04.1.1 emite opinión favorable respecto del Plan de Contingencia Informático, manifestando que el mismo se adecua a la normatividad vigente;

Que, en ese sentido, resulta necesario expedir el acto que apruebe y disponga la implementación del Plan de Contingencia Informático;

Con las visaciones del Secretario General (e), los Jefes (e) de las Oficinas de Tecnología de la Información, Asesoría Jurídica, Planeamiento y Presupuesto, y;

De conformidad con lo dispuesto en el Decreto Legislativo N° 1085, que crea el Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre – OSINFOR, la Ley N° 28716 - Ley de Control Interno de las Entidades del Estado, la Resolución Ministerial N° 129-2012-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos", en todas las entidades integrantes del Sistema Nacional de Informática y el Reglamento de Organización y Funciones del OSINFOR, aprobado por Decreto Supremo N° 065-2009-PCM;

SE RESUELVE:

ARTÍCULO PRIMERO.- APROBAR el *"Plan de Contingencia Informático de la Oficina de Tecnología de la Información del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre - OSINFOR"*, que en anexo forma parte integrante de la presente Resolución.

ARTÍCULO SEGUNDO.- DISPONER la implementación del Plan de Contingencia Informático, a cargo de la Oficina de Tecnología de la Información, responsable de ejecutar el cumplimiento de lo establecido en el referido Plan de Contingencia, informándose al titular del pliego el resultado del mismo.

REPUBLICA DEL PERU

ARTÍCULO TERCERO.- NOTIFICAR la presente Resolución y anexos a todas las Unidades Orgánicas del OSINFOR, para conocimiento.

ARTÍCULO CUARTO.- ENCARGAR a la Oficina de Tecnología de la Información su publicación en el Portal Institucional (www.osinfor.gob.pe), dentro del día siguiente de haber sido emitida la presente Resolución.

Regístrese y comuníquese.

Ing. ROLANDO NAVARRO GÓMEZ
Presidente Ejecutivo (e)
Organismo de Supervisión de los Recursos
Forestales y de Fauna Silvestre – OSINFOR

PLAN DE CONTINGENCIA INFORMATICO

DE LA OFICINA DE TECNOLOGIA DE LA INFORMACION

OSINFOR

OFICINA DE TECNOLOGIA DE LA INFORMACION
V°B°
JEFE
OSINFOR

Oficina de Tecnología de la Información – OTI

Organismo de Supervisión de los Recursos Forestales y la Fauna Silvestre – OSINFOR

Perú, Mayo 2014

OFICINA DE TECNOLOGIA DE LA INFORMACION
V°B°
JEFE
OSINFOR

1 INTRODUCCION

El Plan de Contingencia Informático de la Oficina de Tecnologías de Información del Organismo Supervisor de Recursos Forestales y de Fauna Silvestre – OSINFOR, es resultado de un minucioso estudio de la planificación de prevención de desastres de las Tecnologías de Información y de Comunicaciones – TIC's de OSINFOR, cuando algunos de sus servicios se ve afectado negativamente por causa de algún incidente interno o externo a la organización, en pro de establecer las estrategias de respuesta que permitan atender en forma oportuna, eficiente y eficaz, el desastre , permitiendo así prever las medidas de seguridad que garanticen la continuidad del funcionamiento de nuestros sistemas.

Es así, que el presente Plan de Contingencias se identifican los riesgos a los que están expuestos los sistemas y precisan las medidas de contención para minimizarlos, pudiéndose apreciar del mismo, las diferentes estrategias para planificar y enfrentar desastres, así como aspectos conceptuales de las contingencias, que servirán como marco de referencia para la elaboración de las políticas, normas y otros documentos, que permitan salvaguardar o reducir los efectos de una falla, alteración o desastre que interrumpa o distorsione en forma parcial o total, el normal funcionamiento de los equipos y/o programas de cómputo poniendo en riesgo la integridad de la información.

OFICINA DE TECNOLOGIA DE LA INFORMACION V°B° JEFE OSINFOR

La información es nuestro patrimonio más importante, ante una alteración, es necesario contar con un Plan de Contingencias Informático que será el instrumento, que norme las acciones a desplegar ante situaciones diversas de contingencias; Es imprescindible que el potencial humano del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre - OSINFOR, se encuentre comprometido con este plan de contingencia, y para ello deben tener conocimiento.

2 ASPECTOS GENERALES DE LA SEGURIDAD DE LA INFORMACION

2.1 ALCANCE

El presente documento es administrado por la Oficina de Tecnologías de la Información del OSINFOR, siendo fuente de consulta y aplicación para atender situaciones de contingencia, permitiendo restaurar los sistemas o servicios por algún inconveniente que pudiera presentarse con los mismos.

A través de este plan se busca definir: I) las situaciones y escenarios que pudieran preverse con la finalidad de permitir la operación de los sistemas críticos de las institución a través de las acciones de contingencia, II) la formación del equipo humano y sus roles en casos de contingencia, III) El procedimiento de activación del plan de contingencia, IV) El procedimiento general de recuperación necesario para restaurar el

normal funcionamiento de los sistemas y servicios, que deben estar operando ya sea en el mismo computador al momento del suceso o en un computador alterno.

En tal sentido, El plan de contingencia es la aplicación y cumplimiento obligatorio en todas las unidades orgánicas del OSINFOR, a nivel de Sede Central y Oficinas Desconcentradas, donde se encuentren instalados los sistemas de información y comunicaciones.

2.2 BASE LEGAL

- **Ley N° 28716,** Ley de Control Interno de las Entidades del Estado.
- **Resolución Ministerial Nº 246-2007-PCM** "Uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI, Tecnología de la Información, Código de buenas prácticas para la gestión de la seguridad de la información 2da Edición". en todas las entidades integrantes del Sistema Nacional de Informática.
- **Resolución de Contraloría General de la República Nº 320-2006-CG:** Normas Técnicas de Control Interno para el Sector Público.
- **Resolución Jefatural Nº 386-2002-INEI**, del 31 de diciembre de 2002, que aprueba la Directiva N°016-2002-INEI/DTNP, "Norma Técnicas para el Almacenamiento y Respaldo de la Información procesada por las Entidades de la Administración Publica".
- **Resolución Jefatural Nº 347-2001-INEI**, del 07 de noviembre de 2001, que aprueba la Directiva N°018-2002-INEI/DTNP, "Norma Técnicas para garantizar la Garantizar la Seguridad de la Información pública por las Entidades de la Administración Publica".
- **Resolución Jefatural Nº 080-1999-INEI**, del 22 de febrero de 1999, que aprueba la Directiva N°004-1999-INEI/DTNP, "Lineamientos para la Formulación de Planes Informáticos Institucionales de Corto Plazo 1999".
- **Resolución Presidencial N° 016-2014-OSINFOR**, que aprueba el Plan Operativo Informático.

OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN V°B° JEFE OSINFOR

2.3 OBJETIVO

Garantizar el normal desarrollo de las operaciones, servicios y el cumplimiento de los objetivos Institucionales en caso de urgencias, siniestros y desastres, estableciendo los lineamientos para la integridad y disponibilidad de los sistemas informáticos del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre - OSINFOR.

2.4 FINALIDAD

Proponer y/o garantizar la continuidad de las operaciones realizadas a través de los procedimientos críticos del OSINFOR, a pesar de una posible falla en los sistemas informáticos, con el propósito de:

- Minimizar la pérdida de archivos de datos críticos para la continuidad de las operaciones del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre - OSINFOR.
- Minimizar el daño permanente a los recursos informáticos.
- Minimizar el número de decisiones a tomar ante la presentación de un desastre.

- Minimizar las dependencias específicas durante el proceso de recuperación.
- Minimizar la necesidad de probar acciones de recuperación corriendo el riesgo de cometer errores cuando ocurra una emergencia o desastre.
- Permitir la continuidad de las funciones desarrolladas por las Diferentes Unidades Orgánicas del OSINFOR, de la Sede Central y/o Oficinas Desconcentradas, que se hayan visto afectadas por una situación adversa.
- Iniciar un procedimiento de recuperación de los servicios informáticos ante un desastre o fallas.

2.5 CONCEPTOS GENERALES

2.5.1 TERMINOS DE USO

a) Privacidad: Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidas o transmitidas a otros.

b) Seguridad: Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.

El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.

c) Integridad: Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.

El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

d) Datos: Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de

palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), video (secuencia de tramas), etc.

e) Base de Datos: Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan.

También puede definirse, como un conjunto de archivos interrelacionados que es creado y manejado por un Sistema de Gestión o de Administración de Base de Datos (Data Base Management System-DBMS).

Las características que presenta un DBMS son las siguientes:

- Brinda seguridad e integridad a los datos.
- Provee lenguajes de consulta (interactivo).
- Provee una manera de introducir y editar datos en forma interactiva.
- Existe independencia de los datos, es decir, que los detalles de la organización de los datos no necesitan incorporarse a cada programa de aplicación.

f) Acceso: Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.

g) Ataque: Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

OFICINA DE TECNOLOGIA DE LA INFORMACION V°B° JEFE OSINFOR

h) Ataque activo: Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: El borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

i) Ataque pasivo: Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.

j) Amenaza: Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información

confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

k) **Incidente:** Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido

l) **Golpe (breach):** Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

m) **Contingencia:** Interrupción, no planificada, de la disponibilidad de recursos informáticos.

n) **Plan de Contingencia:** Estrategia planificada con procedimientos que facilita, orienta a una solución y/o alternativa que permite restituir rápidamente los servicios de la organización ante una la eventualidad que pueda parálizar, ya sea de forma parcial o total la organización.

2.5.2 PLAN DE CONTINGENCIA:

Es un documento específico que establece los procedimientos de coordinación, alerta, movilización y respuesta ante la ocurrencia o inminencia de un evento particular; de manera de poder actuar en forma oportuna y efectiva.

El Plan de Contingencia se subdivide en:

- **Plan de Emergencia:** Define la secuencia de las acciones a desarrollar para el control inicial de las emergencias y salvaguardar la integridad y en último término la vida de los miembros de la organización, la conservación de los bienes materiales ante los posibles riesgos que puedan materializarse.
- **Plan de Restauración (BACK UP):** Es el conjunto de acciones que tienen por objetivo restablecer a corto plazo las operaciones, procesos y recursos informáticos de uso crítico que fueron afectados por un evento de contingencia.
- **Plan de Recuperación:** Es el conjunto de acciones que tienen por objetivo restablecer oportunamente la capacidad total de las operaciones, procesos y recursos informáticos que fueron afectados por un evento de contingencia.

El Plan de Contingencia suele combinarse con planes de seguridad general.

TABLA 01 – TIPOS DE PLANES

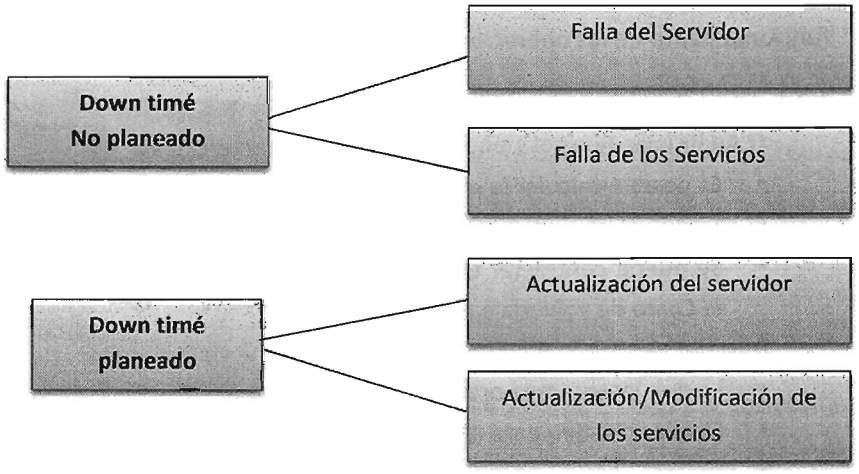
	EMERGENCIA	RESTAURACION	RECUPERACION
OBJETIVO	Limitar el daño.	Continuar con Procesos principales	Recuperar proceso total.
ACTUACION	Inmediata	A corto Plazo	A medio plazo
CONTENIDO	Evacuación	Alternativas de procesos principales	Estrategia para la recuperación de todos los recursos
RESPONSABILIDAD	OSINFOR	Usuarios	OTI

Fuente: OTI-OSINFOR.

2.5.3 TIEMPO DE INACTIVIDAD

El término tiempo de inactividad (downtime) es usado para definir cuándo el sistema no está disponible. Los casos DOWNTIME pueden ser Planeado o No planeados.

GRAFICO 01 – ESPERA Y RETARDO SEGÚN TIPO



Fuente: OTI-OSINFOR.

3 PLAN DE CONTINGENCIA

3.1 ESQUEMA GENERAL

El Plan de Contingencias implica un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputo y la información contenida en los diversos medios de almacenamiento, por lo que en este Manual haremos un análisis de los riesgos, cómo reducir su posibilidad de ocurrencia y los procedimientos a seguir en caso que se presentara el problema.

Pese a todas nuestras medidas de seguridad puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencias incluya un Plan de Recuperación de Desastres, el

cual tendrá como objetivo, restaurar el Servicio Informáticos en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo posible.

3.1.1 DIFUSIÓN Y PUBLICACIÓN

DIFUSIÓN: La Oficina de Tecnología de la Información se encargará de remitir una copia impresa y en formato digital del plan de contingencia de TIC's a la Unidad de Capacitación y Difusión quien se encargará de hacerlo de conocimiento de todo el personal de la sede central del OSINFOR.

PUBLICACIÓN: Esta Oficina se encargará de la publicación de una copia en medio digital y en formato PDF del Plan en el Portal Web.

3.2 ANALISIS DE RIESGO

Se define como riesgo a cualquier evento que puede interrumpir el normal funcionamiento de las operaciones y/o servicios especificados.

3.2.1 CARACTERISTICAS.

El Análisis de Riesgos tiene las siguientes características:

- Es posible calcular la probabilidad de que ocurran las cosas negativas.
- Se puede evaluar económicamente el impacto de eventos negativos.
- Se puede contrastar el Costo de Protección de la Informática y medios versus el Costo de volverla a producir.

Durante el estudio Análisis de Riesgo, se define claramente:

- Lo que intentamos proteger
- El valor relativo para la organización
- Los posibles eventos negativos que atentarían lo que intentamos proteger.
- La probabilidad de ataque.

Se debe tener en cuenta la probabilidad de suceso de cada uno de los problemas posibles, de tal manera de tabular los problemas y su costo potencial mediante un Plan adecuado. Los criterios que usaremos para tipificar los posibles problemas son:

TABLA 02 – TABLA DE VALORES PARA CRITERIOS DE POSIBLES PROBLEMAS

CRITERIOS	ESCALA			
Grado de Negatividad	Leve	Moderado	Grave	Muy severo
Posible Frecuencia del Evento negativo	Nunca	Aleatorio	Periódico	Continuo
Grado de impacto o consecuencias	Leve	Moderado	Grave	Muy severo
Grado de Certidumbre	Nunca	Aleatorio	Probable	Seguro

Fuente: Elaboración propia.

3.2.2 CLASES DE RIESGO

La tabla 03 proporciona el Factor de Probabilidad por Clase de Riesgo en función a la ubicación geográfica de la institución y a su entorno institucional; por ejemplo, si la institución:

- Se ubica en zona sísmica el factor de probabilidad de desastre por terremotos será alta.
- Se ubica en una zona marginal con alto índice de delincuencia, las probabilidades de robo, asalto o vandalismo será de un sesgo considerablemente alto.
- Se ubica en zona industrial las probabilidades de "Fallas en los equipos" será alto por la magnitud de variaciones en tensiones eléctricas que se generan en la zona.
- Cambia constantemente de personal, las probabilidades de equivocaciones y sabotaje será alto.
- En ese contexto, a continuación se detallan los posibles escenarios:

Identificación de Amenazas:

TABLA 03. ESCALA FACTOR DE PROBABILIDAD POR CLASE DE RIESGO

CLASE	FACTOR
Equivocaciones	27.30%
Falla en los equipos	19.94%
Acción virus informático	19.94%
Sabotaje	6.13%
Fenómenos naturales	5.92%
Manipulación y sabotaje	5.80%
Accesos no autorizados	4.60%
Robo de datos	3.68%
Robo común de equipos y archivos	3.07%
Incendio o Fuego	0.61%

Fuente: Elaboración propia.

Estos valores son estimados y corresponden a la apreciación de antecedentes históricos registrados en OSINFOR durante los últimos 04 años. Corresponde al presente Plan de Contingencia minimizar estos índices con medidas preventivas y correctivas sobre cada caso de Riesgo.

En lo que respecta a Fenómenos naturales, nuestra región está situada en zona sísmica y a pesar de no tener información estadística de este fenómeno existe una fuerte probabilidad de ocurra; sin embargo, existen otros fenómenos que afectan a nuestros servicios básicos de forma indirecta, Agua, fluido eléctrico, Internet, Telefonía, etc.

3.2.3 INCENDIO O FUEGO

Grado de Negatividad : Muy Severo
Frecuencia de Evento : Aleatorio
Grado de Impacto : Grave
Grado de Certidumbre : Probable

TABLA 04. ANALISIS DE LA SITUACION ACTUAL PARA INCENDIO O FUEGO

Situación actual	Acción correctiva
El área de Servidores de OSINFOR cuenta con un extintor cargado, ubicado dentro del Área de Servidores.	Se cumple
En todas la Oficinas de OSINFOR, cuentan con un extintor.	Se cumple
No se ejecuta un programa de capacitación sobre el uso de elementos de seguridad y primeros auxilios, lo que no es eficaz para enfrentar un incendio y sus efectos.	Implantar un Programa de Capitación para el manejo de extintores.

Fuente: elaboración propia

Una probabilidad máxima de contingencia de este tipo en el OSINFOR, puede alcanzar a destruir un 50% de las oficinas antes de lograr controlarlo, también podemos suponer que en el área de Servidores tendría un impacto Grave, por las medidas de seguridad y ambiente que lo protege.

Existen diversas clases de fuegos que se designan con las letras: A - B - C y D, y son:

CLASE A: fuegos que se desarrollan sobre combustibles sólidos, como ser madera, papel, telas, gomas, plásticos termoendurecibles y otros.

CLASE B: fuegos sobre líquidos combustibles, grasas, pinturas, aceites, ceras y otros.

CLASE C: fuegos sobre materiales, Instalaciones o equipos sometidos a la acción de la corriente eléctrica.

CLASE D: fuegos sobre metales combustibles, como ser el magnesio, titanio, potasio, sodio y otros.

Para la mejor protección de los dispositivos de almacenamiento, se está solicitando un ambiente en la Oficina anexa del Jr. Trujillo para colocar Estratégicamente, una Segunda Copia de Seguridad.

Uno de los dispositivos más usados para contrarrestar la contingencia de incendio, son los extinguidores. Su uso conlleva a colocarlos cerca de las posibles áreas de riesgo que se debe proteger. A continuación se detallan tipos de extintores y su uso que debe conocer todo el personal en el uso del extinguidor.

TABLA 05. TIPOS DE AGENTES DE EXTINCIÓN DE INCENDIOS

AGENTES EXTINTORES	CLASE A	CLASE B	CLASE C	CLASE D
Agua a chorro	**	X	X	X
Agua pulverizada	***	*	X	X
Espuma	**	**	X	X
Polvo polivalente ABC	**	**	**	X
Polvo normal BC	X	***	**	X
Anhídrido carbónico	*	*	X	X
Derivados Halogenados	*	*	X	X
Productos específicos	X	X	X	*
Leyenda:	X : INACEPTABLE * : ACEPTABLE ** : BUENO *** : EXCELETE			

Fuente: elaboración propia

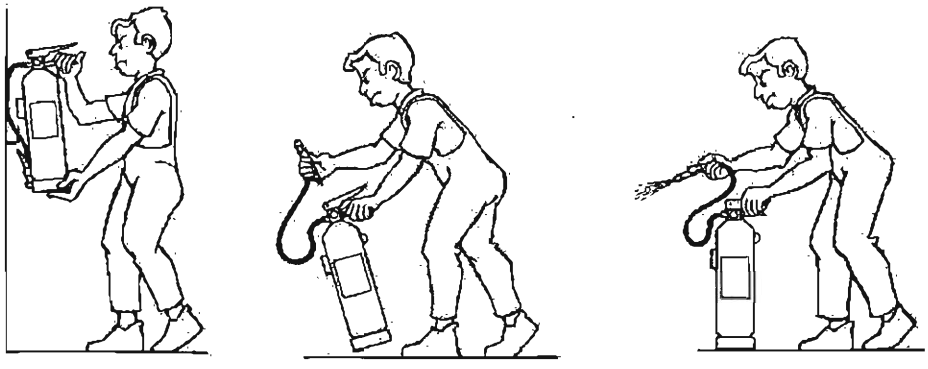
Para OSINFOR usa dos tipos de extintores los **extintores ABC**, que son adecuados para casi todos los tipos de incendio que pudiera producirse en el edificio. Son el tipo de extintor más difundido; dañan más los equipos delicados, pero son más eficaces, se usan en los ambientes de uso común, en donde no exista concentración de equipos informáticos.

Los **extintores CO2** Son apropiados para incendios en equipos informáticos y de comunicaciones ya que son los que estropean menos que otros agentes extintores, pero son menos eficaces que los extintores de polvo, estos extintores están ubicados en las oficinas donde hay una alta concentración de equipos Informáticos y de comunicaciones.

A continuación se describe gráficamente el procedimiento para el uso de extinguidores en caso de incendio:

OFICINA DE TECNOLOGIA DE LA INFORMACION V°B° JEFE OSINFOR

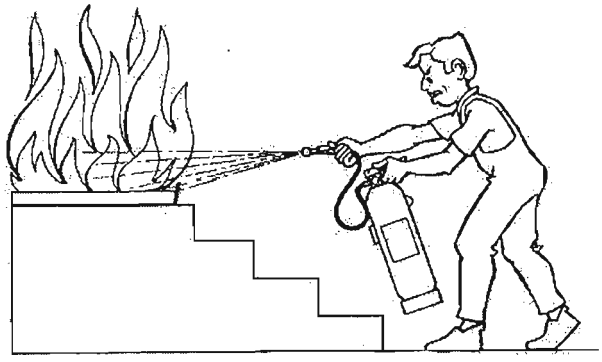
GRAFICO 02 – METODO DE USO DE EXTINTOR



Descolgar el extintor asiéndolo por la maneta o asa fija y dejarlo sobre el suelo en posición vertical.

2. Asir la boquilla de la manguera del extintor y comprobar, en caso que exista, que la válvula o disco de seguridad (V) está en posición sin riesgo para el usuario.
Sacar el pasador de seguridad tirando de su anilla.

3. Presionar la palanca de la cabeza del extintor y en caso de que exista apretar la palanca de la boquilla realizando una pequeña descarga de comprobación.



4. Dirigir el chorro a la base de las llamas con movimiento de barrido.
En caso de incendio de líquidos proyectar superficialmente el agente extintor efectuando un barrido evitando que la propia presión de impulsión provoque derrame del líquido incendiado.
Aproximarse lentamente al fuego hasta un máximo aproximado de un metro.

Fuente: elaboración propia

3.2.4 ROBO COMUN DE EQUIPOS Y ARCHIVOS

Grado de Negatividad : Grave
Frecuencia de Evento : Aleatorio
Grado de Impacto : Moderado
Grado de Certidumbre : Aleatorio

TABLA 06. ANALISIS DE LA SITUACION ACTUAL PARA ROBO COMUN DE EQUIPOS

SITUACIÓN ACTUAL	ACCIÓN CORRECTIVA
Vigilancia permanente.	Existe vigilancia. La salida de un equipo informático es registrada por el personal del área de patrimonio y por el personal de seguridad en turno.
Se verifica si el Personal de Seguridad cumple con la inspección de los usuarios, sobre su obligación de cerrar puertas y ventanas al finalizar su jornada.	Al respecto Personal de Seguridad emite recomendaciones sobre medidas de Alerta y seguridad.
Remitir aviso a la Oficina de Patrimonio y a la OTI, para retirar equipo informático.	Se Cumple

Fuente: elaboración propia

No se han reportado casos en la cual haya existido manipulación y reubicación de equipos sin el debido conocimiento y autorización debida entre el Jefe del Área funcional y encargado de patrimonio. Esto demuestra que los equipos se encuentran protegidos de personas no autorizadas y no identificables.

Según antecedentes de otras instituciones, es de conocer que el robo de accesorios y equipos informáticos, llegaron a participar personal propio de la empresa en colusión con el personal de vigilancia. Es relativamente fácil remover un disco duro del CPU, tarjeta, etc. y no darse cuenta del faltante hasta días después. Estas situaciones no se han presentado en OSINFOR, pero se recomienda siempre estar alerta.

3.2.5 VANDALISMO

Grado de Negatividad : Grave
Frecuencia de Evento : Aleatorio
Grado de Impacto : Grave
Grado de Certidumbre : Aleatorio

TABLA 07. ANALISIS DE LA SITUACION ACTUAL PARA VANDALISMO

SITUACIÓN ACTUAL	ACCIÓN CORRECTIVA
OSINFOR está en una zona donde el índice de vandalismo es bajo	Hay vigilancia.
Se presentan casos muy aislados de administrador que en el Proceso atención no están conformes con algunas normativas, tal que al efectuar sus reclamos personalmente asumen actitudes retroactivas, que muchas veces ofenden al trabajador, y sin medir las consecuencias pueden llegar a dañar alguna Instalación de OSINFOR.	Continuar con la política de Gestión de mejorar la Atención del Cliente, brindando mayor información a los administrados.
Alguna probabilidad de turbas producto de manipulaciones políticas.	No aplica

Fuente: elaboración propia

La destrucción del equipo puede darse por una serie de desastres incluyendo el vandalismo, robo y saqueo en simultáneo.

3.2.6 FALLA EN LOS EQUIPOS

Grado de Negatividad : Grave
Frecuencia de Evento : Periódico
Grado de Impacto : Leve
Grado de Certidumbre : Aleatorio

TABLA 08. ANALISIS DE LA SITUACION ACTUAL PARA FALLA DE EQUIPOS

SITUACIÓN ACTUAL	ACCIÓN CORRECTIVA
La Red de Equipos y Servidores en OSINFOR cuenta con una Red Eléctrica Estabilizada.	Solo los equipos servidores cuentan con una red estabilizada y pozo a tierra.
No existe un adecuado tendido eléctrico en algunas oficinas del OSINFOR	Tomar previsiones económicas para implementar un adecuado tendido eléctrico.
La falla en el hardware de los equipos, requiere un rápido mantenimiento o reemplazo.	Existe Mantenimiento de los equipos de cómputo. Contar con proveedores, en caso de

	requerir reemplazo de piezas, y de ser posible contar con repuestos.

Fuente: elaboración propia

De ocurrir esta contingencia las operaciones informáticas se detendrían, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño. Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente, pero si el corte se prolongara por tiempo indefinido provocaría un trastorno en las operaciones del día, sin afectar los datos.

El equipo de aire acondicionado y ambiente adecuado en el Área de Servidores, favorece su correcto funcionamiento.

Para el adecuado funcionamiento de las computadoras personales, necesitan de una fuente de alimentación eléctrica fiable, es decir, dentro de los parámetros correspondientes. Si se interrumpe inesperadamente la alimentación eléctrica o varia en forma significativa (fuera de los valores normales), las consecuencias pueden ser muy serias, tal como daño del HW y la información podría perderse.

La fuente de alimentación es un componente vital de los equipos de cómputo, y soportan la mayor parte de las anomalías del suministro eléctrico. Se ha identificado los siguientes problemas de energía más frecuentes:

- Fallas de energía.
- Transistores y pulsos.
- Bajo voltaje.
- Ruido electromagnético.
- Distorsión.
- Variación de frecuencia.

Para los cuales existen los siguientes dispositivos que protegen los equipos de estas anomalías:

- Supresores de picos.
- Estabilizadores.
- Sistemas de alimentación ininterrumpida (UPS).

Existen formas de prever estas fallas, con la finalidad de minimizar su impacto, entre ellas tenemos:

Tomas a Tierra o Puestas a Tierra

Se denomina así a la comunicación entre el circuito Eléctrico y el Suelo Natural para dar seguridad a las personas protegiéndolas de los peligros procedentes de una rotura del aislamiento eléctrico. Estas conexiones a tierra se hacen frecuentemente por medio de placas, varillas o tubos de cobre enterrados profundamente en tierra humedad, con o sin agregados de ciertos componentes de carbón vegetal, sal o elementos químicos, según especificaciones técnicas indicadas para las instalaciones eléctricas.

Para el OSINFOR solo se cuenta con un pozo a tierra que está conectado al ambiente de servidores y está aislado de otras oficinas.

Extensiones eléctricas y capacidades

Las computadoras ocupan rápidamente toda la toma de corriente. Pocas oficinas se encuentran equipadas con las suficientes placas de pared. Dado que es necesario conectar además algún equipo que no es informático, es fácil ver que son muy necesarias las extensiones eléctricas múltiples. El uso de estas extensiones eléctricas debe ser controlado con cuidado.

No solo para que no queden a la vista, sino también porque suponen un peligro considerable para aquellos que tengan que pasar por encima. A parte del daño físico que puede provocar engancharse repentinamente con el cable, apaga de forma rápida un sistema completo.

Por razones de seguridad física y de trabajo se recomienda tener en cuenta las siguientes reglas:

- Las extensiones eléctricas deben estar fuera de las zonas de paso, siempre que sea posible.
- Utilizar canaletas de goma adecuadas para cubrir los cables, si van a cruzar una zona de paso.
- No se debe encadenar sucesivos múltiples, ya que esto puede hacer que pase más corriente de la que los cables están diseñados para soportar. Se debe utilizar los enchufes de pared siempre que sea posible.
- Si es posible, utilizar extensiones eléctricas que incluyan fusibles o diferenciales. Esto puede ayudar limitar el daño ante fallas eléctricas.
- Se debe comprobar siempre la carga frente a las extensiones eléctricas. La mayor parte de ellas llevan los amperios que admite cada extensión, no debiendo superar esa cifra el amperaje total de todos los aparatos conectados a ellas.
- Adquirir toma de corrientes de pared y/o extensiones eléctricas mixtas, capaces de trabajar con enchufes de espigas planas, como cilíndricas.
- Tanto las tomas corrientes de pared como las extensiones eléctricas deben tener toma a tierra.

OFICINA DE TECNOLOGIA DE LA INFORMACION V°B° JEFE OSINFOR

3.2.7 EQUIVOCACIONES

Grado de Negatividad	: Moderado
Frecuencia de Evento	: Periódico
Grado de Impacto	: Moderado
Grado de Certidumbre	: Probable

TABLA 09. ANALISIS DE LA SITUACION ACTUAL PARA EQUIVOCACIONES

SITUACIÓN ACTUAL	ACCIÓN CORRECTIVA
Las equivocaciones que se producen en forma rutinaria son de carácter involuntario.	Capacitación inicial en el ambiente de trabajo. Instruir al nuevo usuario con el Manual de Procedimientos
Cuando el usuario es practicante y tiene conocimientos de informática, tiene el impulso de navegar por los sistemas.	En lo posible se debe cortar estos accesos, limitando su accionar en función a su labor de rutina.
La falta de institucionalizar procedimientos produce vacíos y errores en la toma de criterios para registrar información.	Reuniones y Actas de Trabajo para fortalecer los procedimientos.
Ante nuevas configuraciones se comunica a los usuarios sobre el manejo, claves, accesos y restricciones, tanto a nivel de Sistemas, Telefonía, Internet	Se envía por correo institucional Enviar oficios circulares múltiples comunicando los nuevos cambios y políticas. Convocar reuniones de capacitación antes nuevas opciones en los sistemas.

Fuente: elaboración propia

OFICINA DE TECNOLOGIA DE LA INFORMACION V°B° JEFE OSINFOR

3.2.8 ACCION DE VIRUS INFORMATICOS

Grado de Negatividad : Muy Severo
Frecuencia de Evento : Continuo
Grado de Impacto : Grave
Grado de Certidumbre : Probable

TABLA 10. ANALISIS DE LA SITUACION ACTUAL PARA ACCION ANTE VIRUS INFORMATICOS

SITUACIÓN ACTUAL	ACCIÓN CORRECTIVA
Se cuenta con un Software Antivirus corporativo. Pero no hay un contrato anual para su actualización.	Se cuenta con un Software Antivirus corporativo.
Todo Software (oficina, desarrollo, mantenimiento, drives, etc.) es manejado por personal de OTI, quienes son los encargados de su instalación en las PC's con su respectivo software corporativo.	Se cumple.
Se tiene un programa permanente de bloqueo acciones como cambiar configuraciones de red, acceso a los servidores, etc.	Se cumple a través de políticas de usuarios.
Se tiene instalado el antivirus de red y en estaciones de trabajo. Antes de logear una	Se cumple

maquina a la red (dominio) se comprueba al existencia de virus en la PC.	

Fuente: elaboración propia

En estos últimos años la acción del virus informático ha sido contrarrestada con la diversidad de productos que ofrece el mercado de software. Las firmas y/o corporaciones que proporcionan software antivirus, invierten mucho tiempo en recopilar y registrar virus, indicando en la mayoría de los casos sus características y el tipo de daño que puede provocar, por este motivo se requiere de una actualización periódica del software antivirus.

3.2.9 FENOMENOS NATURALES

Grado de Negatividad : Grave
Frecuencia de Evento : Aleatorio
Grado de Impacto : Grave
Grado de Certidumbre : Aleatorio

TABLA 11. ANALISIS DE LA SITUACION ACTUAL PARA FENOMENOS NATURALES

SITUACIÓN ACTUAL	ACCIÓN CORRECTIVA
La última década no se han registrado contingencias debido a fenómenos naturales como: terremotos, inundaciones, aluviones, etc.	Medidas de prevención.
Potencialmente existe la probabilidad de sufrir movimientos sísmicos debido a que estamos ubicados sobre la zona sísmica entre 15% y 30% de impacto medio.	Medidas de prevención.

Fuente: elaboración propia

La previsión de desastres naturales sólo se puede hacer bajo el punto de vista de minimizar los riesgos innecesarios en el ambiente para servidores, en la medida de no dejar objetos en posición tal que ante un movimiento telúrico pueda generar mediante su caída y/o destrucción la interrupción del proceso de operación normal.

Además, bajo el punto de vista de respaldo, se debe tener en claro los lugares de resguardo, vías de escape y de la ubicación de los archivos, dispositivos de almacenamiento, discos con información vital, todo ello como respaldo de aquellos que se encuentren aun en las instalaciones de la institución.

3.2.10ACCESO NO AUTORIZADO

Grado de Negatividad : Grave
Frecuencia de Evento : Aleatorio
Grado de Impacto : Grave
Grado de Certidumbre : Probable

TABLA 12. ANALISIS DE LA SITUACION ACTUAL PARA ACCESO DE AUTORIZADO

SITUACIÓN ACTUAL	ACCIÓN CORRECTIVA
Se controla el acceso al Sistema de Red mediante la definición de "Cuenta" o "Login" con su respectiva clave	Se cumple
A cada usuario de Red se le asigna los "Atributos de confianza" para el manejo de archivos y acceso a los sistemas.	Se cumple
Cuando el personal cesa en sus funciones y/o es asignado a otra área, se le redefinen los accesos y autorizaciones, quedando sin efecto la primera.	Se cumple en la medida que la OTI es informado de actualizar los accesos al momento de producirse el cese o cambio.
Se forman Grupos de usuarios, a los cuales se le asignan accesos por conjunto, mejorando la administración de los recursos	Se cumple
Se acostumbra a confiar la clave de acceso (uso personal) a compañeros de área, sin medir la implicación en el caso de acceso no autorizado. En algunos casos los usuarios escriben su contraseña (Red o de Sistemas) en sitios visibles.	Capacitar al personal sobre la confidencialidad de sus contraseñas, recalcando la responsabilidad e importancia que ello implica.
No se tiene un registro electrónico de Altas/Bajas de Usuarios, con las respectivas claves	Se debe implementar

Fuente: elaboración propia

Todos los usuarios sin excepción tienen un "login" o un nombre de cuenta de usuario y una clave de acceso a la red con un mínimo de cinco (5) dígitos. No se permiten claves en blanco. Además están registrados en un grupo de trabajo a través del cual se otorga los permisos debidamente asignados por el responsable de área.

Cada usuario es responsable de salir de su acceso cuando finalice su trabajo o utilizar un bloqueador de pantalla.

3.2.11ROBO DE DATOS

Grado de Negatividad : Grave
Frecuencia de Evento : Aleatorio
Grado de Impacto : Grave
Grado de Certidumbre : Probable

TABLA 13. ANALISIS DE LA SITUACION ACTUAL PARA ROBO DE DATOS

SITUACIÓN ACTUAL	ACCIÓN CORRECTIVA
Las Oficinas tienen disponible disqueteras, quemadoras de CD/DVD, puertos USB, pero no se lleva un control sobre la información que ingresa y/o sale del ordenador.	Personal de Planta debe manejar información delicada de la Oficina.
El servicio de Internet es potencialmente una ventaja abierta para el robo de información electrónica	Existen políticas que regulan el uso y acceso del Servicio de Internet.
Los documentos impresos (informes, reportes, contratos, etc.) normalmente están expuestos al robo por que no se acostumbra guardarlos como debe ser. Si no se toma conciencia que esta es una manera de atentar contra el Sistema Informático del OSINFOR el problema persistirá.	Resguardar la información en archivos. Destruir los reportes malogrados, sobre todo de contenido relevante. (Existen papeleros que convierten el papel en picadillo).
El acceso a los terminales se controla, mediante claves de acceso, de esta manera se impide el robo de información electrónica. A través de las políticas se seguridad se impide el ingreso a los Servidores.	Se cumple parcialmente

Fuente: elaboración propia

El Robo de datos se puede llevarse a cabo bajo tres modalidades:

- La primera modalidad consiste en sacar "copia no autorizada" a nuestros archivos electrónicos aun medio magnético y retirarla fuera de la institución.
- La segunda modalidad y tal vez la más sensible, es la sustracción de reportes impresos y/o informes confidenciales.
- La tercera modalidad es mediante acceso telefónico no autorizado, se remite vía Internet a direcciones de Correo que no corresponden a la Gestión Empresarial.

OFICINA DE TECNOLOGIA DE LA INFORMACION V°B° JEFE OSINFOR

3.2.12MANIPULACION Y SABOTAJE

Grado de Negatividad : Grave
Frecuencia de Evento : Aleatorio
Grado de Impacto : Grave
Grado de Certidumbre : Probable

TABLA 14. ANALISIS DE LA SITUACION ACTUAL PARA MANIPULACION Y SABOTAJE

SITUACIÓN ACTUAL	ACCIÓN CORRECTIVA
Existe el problema de la inestabilidad laboral, la misma que podría obligar a personas frustradas, o desilusionadas a causar daños físicos y lógicos en el sistema de información de la institución. Esto se puede traducir desde el registro de operaciones incorrectas por parte de los usuarios finales, hasta la operación de borrar registros en el sistema y conductas de sabotaje	La protección contra el sabotaje requiere: Una selección rigurosa del personal. Buena administración de los recursos humanos Buenos controles administrativos Buena seguridad física en los ambientes donde están los principales componentes del equipo. Asignar a una persona la responsabilidad de la protección de los equipos en cada área.
No se comunica el movimiento de personal a la OTI, para restringir accesos del personal que es reubicado y/o cesado de OSINFOR.	Es conveniente la comunicación anticipada del personal que será reubicado y/o cesado con el objeto de retirar los derechos de operación de escritura para otorgarle los derechos de consulta antes de desactivar la cuenta.
Existe el antecedente de origen sabotaje interno. Como es el caso de trabajadores que han sido despedidos y/o están enterados que van a ser rescindidos su contrato, han destruidos o modificado archivos para su beneficio inmediato o futuro.	Hay que protegerse también ante una posible destrucción del hardware o software por parte de personal no honrado.

Fuente: elaboración propia

Instituciones que han intentado implementar Programas de Seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más difíciles y duros. Este puede ser un trabajador o un sujeto ajeno a la propia institución. Un acceso no autorizado puede originar sabotajes. Los riesgos y peligros deben ser identificados y evaluados, para conocer las posibles pérdidas y para que pueda ponerse en práctica los adecuados métodos de prevención.

Una mejora en la seguridad produce, a menudo, importantes beneficios secundarios. Por ejemplo, el cambio de metodología aplicada a determinadas operaciones conduce frecuentemente a una reducción del índice de errores, a una mejora en calidad, a una mejor planificación y a resultados más rápidos.

No existen un plan idóneo o una recomendación simple para resolver el problema de la seguridad. Realmente no es una situación estática o un problema "puntual", sino que requiere un constante y continuo esfuerzo y dedicación.

- **Riegos naturales.-** Como mal tiempo, terremoto, etc.
- **Riesgos Tecnológicos.-** Como fallas de energía eléctrica y malas configuraciones de equipos de comunicación.
- **Riesgo social.-** Como actos terrorista y desordenes.

3.3 IDENTIFICACION DE RIESGO

La evaluación de riesgos supone imaginarse lo que puede ir mal y a continuación estimar el coste que supondría. Se ha de tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.

Para cada riesgo, se determinó la probabilidad del factor de riesgo. Como ejemplo se mencionan algunos factores de riesgo que se consideraron:

- Factor de riesgo muy bajo.
- Factor de riesgo bajo.
- Factor de riesgo medio.
- Factor de riesgo alto.
- Factor de riesgo muy alto.

Luego se efectuará un resumen de los riesgos ordenados por el factor de riesgo de cada uno se representa en el siguiente cuadro:

OFICINA DE TECNOLOGIA DE LA INFORMACION V°B° JEFE OSINFOR

TABLA 15. IDENTIFICACION DE RIESGOS Y MEDIDAS PREVENTIVAS

CAUSAS	PROBABILIDAD DE OCURRENCIA	ESCENARIOS
• Fallas corte de Cable UTP. • Fallas de Tarjeta de Red. • Fallas IP asignado. • Fallas de Punto de Switch. • Fallas Punto Patch Panel. • Fallas Punto de Red.	BAJA	FALLA DE COMUNICACIÓN CLIENTE-SERVIDOR.
• Fallas de componentes de Hardware del servidor. • Falla del UPS (Falta de Suministro Eléctrico). • Insuficiente espacio de almacenamiento en disco.	MEDIA	FALLA DE SERVIDOR

• Computador personal funcionando como servidor.		
• Accidente. • Renuncia intempestiva.	BAJA	AUSENCIA PARCIAL O PERMANENTE DEL PERSONAL DE TECNOLOGIA DE LA INFORMACION
• Robo sistemático de información. • Fraude o Alteración de información. • Fallas Provocada sin intensión. • Fallas Provocada intencionalmente • Equivocaciones • Infección de virus	**ALTA**	PERSONA INTERNA O EXTERNA
• Corte General del Fluido Eléctrico. • Equipo Dañados.	BAJA	INTERRUPCION DEL FLUIDO ELECTRICO.
• Falla de equipos de comunicación: SWITCH, Fibra Óptica. • Fallas de conexión de acceso a internet. • Perdida de comunicación con proveedores de internet.	BAJA	PERDIDA DE SERVICIO DE INTERNET
• Incendio. • Sabotaje. • Corto Circuito. • Terremoto. • Vandalismo • Accesos no Autorizados • Incendios	BAJO	INDISPONIBILIDAD DEL CENTRO DE COMPUTO

Fuente: OTI-OSINFOR.

3.4 MEDIDAS PREVENTIVAS PARA LA GESTION DE LA SEGURIDAD

La seguridad de la información tiene dos aspectos. El primero consiste en negar el acceso a los datos a aquellas personas que no tengan derecho a ellos, al cual también se le puede llamar protección de la privacidad, si se trata de datos personales, y mantenimiento de la seguridad en el caso de datos institucionales.

Un segundo aspecto de la protección es garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad de proteger los datos que se les ha confiado.

Por otro lado, es importante incorporar dispositivos de seguridad durante el diseño del sistema en vez de añadirlas después. Los diseñadores de sistemas deben entender que las medidas de seguridad han llegado a ser criterios de diseño tan importantes como otras posibilidades funcionales, así como el incremento de costos que significa agregar funciones, después de desarrollado un Sistema de Información.

3.4.1 SEGURIDAD Y ACCESO A LOS EQUIPO DE CÓMPUTO.

Se debe crear las cuentas de los usuarios en el Servidor de Dominio, para que cada trabajador pueda tener su nombre con su respectiva contraseña.

Los usuarios a quien se le asignó el acceso de usuario y clave, no deben de compartir con su compañero trabajo y/o personal externa; el usuario es responsable de cualquier perdida, alteración de la información.

Con el grupo de Trabajo definido; se compartirán carpetas para que solo los usuarios del grupo puedan acceder a la información disponible según el área correspondiente.

Para el buen uso de la PC's y de los programas; el personal deberá de tener un mínimo de conocimiento a nivel de usuario final y de ser necesario se adiestrara por el personal de informática en lo que sea necesario.

Fallas de conectividad en la red, por deterioro del cableado y conector, se debe mencionar que, su reparación está sujeta a la disponibilidad de material para recablear el tramo defectuoso o la contracción del especialista. Para evitar deterioró los punto de red, los escritorios con las Pc's se deben adecuar a los puntos donde están instalado, ni por ningún motivo mover.

En el área informática se designara al responsable de la coordinar de las acciones y planes de referencia al mantenimiento, reparación y soporte informático.

3.4.2 POLITICAS DE SEGURIDAD

La Seguridad debe ser considerada desde la fase de diseño de los sistemas, como parte integral del mismo. Debe darse mayor importancia a la toma de medidas de seguridad, teniendo siempre presente que es indispensable, no sólo para el buen funcionamiento sino también para el mantenimiento del sistema.

Las políticas de seguridad deben ser definidas por los funcionarios de alto nivel, los cuales deben ser motivados de manera que tengan un rol importante.

La Oficina de Tecnologías de la Información, a través del encargado de soporte, asegura la gestión la seguridad informática en OSINFOR, ha de considerar las siguientes medidas:

- **Distribuir las reglas de seguridad**: Escribir en una lista las reglas básicas de seguridad que los usuarios han de seguir, para mantener la seguridad y ponerlas en un lugar público destacado. Se puede incluir un dibujo en un póster para dar mayor referencia. Se debe considerar la posibilidad de distribuir las reglas por todas las computadoras personales.

- **Hacer circular regularmente avisos sobre la seguridad**: Utilice ejemplos de daños y problemas procedentes de periódicos, revistas, para ilustrar la necesidad de la vigilancia por mantener la seguridad. Intente que estos avisos sean interesantes, sin entrar en muchos detalles, ya que en caso contrario podría inspirar imitaciones.

- **Establecer incentivos para la seguridad:** Las personas que rompen la seguridad poseen un incentivo para hacerlo. Dé a las personas de su organización un incentivo para mantenerla. Establezca premios para las ideas que supongan trucos de seguridad y que apoyen las medidas de seguridad oficiales. Haga que los responsables ofrezcan recompensas sustanciosas a los ganadores

- **Establezca una línea de comunicación sobre seguridad**: El personal debe conocer dónde puede obtener consejos sobre los temas de seguridad. También deben de poder informar sobre violaciones de la seguridad o actividades sospechosas de forma anónima. Por otro lado, ofrezca recompensas por informar de las violaciones de seguridad.

3.4.3 ADMINISTRACION DE LA RED

La administración de la red comprende las siguientes tareas:

Atención de consultas en línea a través del correo electrónico sobre temas relacionados al organismo de Supervisión de Recursos Forestales y de Fauna Silvestre.

Mantenimiento de la Pagina Web (acorde con las normas legales vigentes)

La implementación de la Intranet Institucional, propiciara la aplicación del servicio de telefonía IP, video conferencia y uso de los sistemas de información.

Coordinar todo tipo de implementación de nuevas tecnologías de cableado: para el cableado estructurado, Fibra Óptica o Inalámbrica para el tendido de la Red de la Institución.

Mantenimiento del soporte de fluido eléctrico a los servidores, coordinando acciones para proveer un servicio estable y "limpio de energía eléctrica (pozo a tierra, Convertidores, estabilizadores, UPS, etc.).

Capacitación de los usuarios en temas de Red.
Realización de los Back up en forma regular y periódica.
Generación de reportes de páginas no productivas.
Informar sobre posible vulnerabilidad de la seguridad de la información (Anticipación)
Creación del Sistema de Información.

3.4.4 DESARROLLO DE LAS TAREAS DE SOPORTE TÉCNICO DE CÓMPUTO.

Cada oficina desconcentrada deberá contar con una persona de apoyo informático capacitado para atender los requerimientos más comunes.
El personal de soporte técnico, asisten a requerimiento de cada unidad orgánica y/o oficina desconcentrada.
Seguir el procedimiento establecido en MAPRO-2013, en atención por los distintos medio de comunicación (teléfono, correo y/o documento forman del requerimiento).

3.4.5 PERSONAL SOPORTE TÉCNICO

El personal debe estar en constantemente capacitado tanto en los aspectos técnicos como en las normas y procedimientos que rijan sus actividades. Ya que por la naturaleza de su trabajo sus acciones pueden abarcar a equipo costoso.
Tareas de Mantenimiento Lógico – Preventivo de computadoras a ser realizadas por el equipo de soporte Técnico.
Realizar Back up de los archivos necesarios en un disco u otro dispositivo de almacenamiento limpio de virus y sin errores para garantizar el respaldo.
Configuración de políticas de seguridad en la protección del antivirus.
Borrar archivos innecesarios del disco duro (Temporales, música, video y etc.)
Instalación del sistema operativo ya sea por infección de virus, fallas de aplicativos con el sistema operativo.
Instalación de Software Ofimática y aplicativos adquiridos.
Verificación de software instalado en la computadora (Depuración de software pirata).
Realizar un inventario de Operatividad de los equipos.
Realizar configuración, limpieza para el buen funcionamiento de impresora y optimización de recurso.
Proponer la reubicación de los equipos.
Realizar un inventario físico de las computadoras comprobando su antigüedad y ubicación.

3.4.6 SEGURIDAD DE LOS DATOS

La información por su naturaleza es función de interés de la institución puede clasificarse en critica.
Determinar la unidad lógica, donde se guardara la información, y procedimiento para salvaguardar la información crítica.
Respaldar periódicamente la información existente en los servidores.

El respaldo de información debe estar salvaguardo en una ambiente fuera de la institución con adecuado infraestructura para la preservación de la información.
El personal de cada unidad orgánica y/o oficina desconcentradas responsable que tengan servicios de acceso a internet activan mecanismos de seguridad que garanticen el funcionamiento de la red o estación de trabajo, evitando del mal uso de la red entrando a página indebida que vulnere la seguridad informática.

Seguridad Interna y/o Vigilancia

Se integran por el personal de vigilancia, seguridad interna y Policía Nacional; De cual deberá estar capacitado para:
Conocer los componentes y detectar sustracciones.
Conocer los procedimientos de control de movilización de equipos y componentes de cómputo fuera o dentro de la institución.
Conocer los horarios y exigencias de los trabajos de los usuarios para detectar horarios indebidos.
Enfrentar resolver un problema ocasionado por un corto circuito, un incendio, un rayo, etc.
Tener el criterio para definir y aplicar el procedimiento de resguardo de los sistemas de información acorde con la gravedad de la contingencia (agitación, vandalismo, saqueo, movilización social, etc.)
La información es el patrimonio o bien más preciado de la institución; representa miles de horas hombres de trabajo intelectual plasmada en los archivos de información que se encuentran almacenados en los discos duros de las computadoras de la entidad. Dicha información es actualizada globalmente cada segundo, por ello, su valor en términos económico es incalculable, y porque además es la fuente de la que se nutren los más altos niveles en la entidad para la toma de decisiones.

OFICINA DE TECNOLOGIA DE LA INFORMACION V°B° JEFE OSINFOR

Actualmente la información de OSINFOR esta almacenada y distribuida en dos tipos de dispositivos:

- **Disco duro de cada unidad orgánica y/o oficinas desconcentradas.**
- **Disco duros de servidores de Archivos de la Red.**

El respaldo de la información y los parámetros de configuración contenida en los Discos Duros de los Servidores de la Red es de responsabilidad de la Oficina de Tecnología de la Información.
Respecto a los discos duros de cada usuario, su respaldo (Backup) serán programadas con el jefe inmediato o el personal responsable de tener un control de la copia de su respectiva unidad orgánica y/o Oficina desconcentrada.

Los procedimiento descrito en el presente documento, servirán como instrumento para la ejecución de tareas que tuviesen que desarrollarse a fin de

brindar una solución en caso de presentarse fallas en los equipos de cómputo por motivos fortuitos o intencionales.

La oficina de tecnología de la Información emitirá una cartilla de sugerencias o instructivo como guía, para el responsable de la información de cada área, coordine las acciones para la realización del respaldo de la información de su unidad orgánica y/o oficina desconcentrada. A su vez se tendrá una personal designado por el superior quien se haga cargo de la copia de seguridad. La oficina de tecnología de la información, se encargara de supervisar y vigilar el cumplimiento del cronograma establecido por unidad orgánica y/o oficina desconcentradas.

Equivocaciones

La dinámica diaria del trabajo y la exigencia por el cumplimiento de la tarea asignada, u otros factores extra laborales o personales pueden generar desconcentración y consecuente mal uso de los recursos de cómputo. Siendo este un aspecto poco llamativo, sin embargo puede constituirse en fuga importante de gastos.

Por ello, la orientación, las dinámicas grupales, y otro programas de estímulo y aprecio al trabajo, que se desarrollen en especial promovidas por el área de recursos Humanos, redundaran en la disminución de este factor de riesgo.

Tener siempre presente a la normatividad interna que tipifica las sanciones por los daños que devengan error o equivocación.

Virus.

Siendo nuestros sistemas de cómputo orientados a productos conocidos y certificados no por ello están fuera de la ocurrencia constante de la presencia de virus que interfieren con el buen funcionamiento del sistema de cómputo y pueden ocasionar perdida de información importante o fallas físicas en los equipos.

Los virus ocasionan fallas desde el tipo de simples mensajes, perdidas de información o daño permanente en el hardware de cómputo.

Los virus al ser programados por personas son archivos magnéticos que se adhieren o se esconden en otros archivos y por lo tanto pueden ser transmitidos al igual que los archivos que comúnmente se transportan vía disquetes, redes o de cualquier tipo de comunicación entre computadoras.

La filtración de virus está ligado a programas instalado o alojado en dispositivos, que son usado en la institución o externo que son desarrollado por los llamados Hacker, Crakers, Lamers, etc.)

Con la implementación de una seguridad perimetral y configuraciones en los servidor, que nos lleva a una política de seguridad definida vía Firewall o de Hardware con tecnología de encriptación tipo WEP (Redes inalámbrico). Con el despliegue y configuración del antivirus en cada una de la computadora y

servidores nos da una seguridad del no ingreso de virus u otros gusanos en el sistema informático del OSINFOR.

3.4.7 ESTRATEGIAS DE CONTINGENCIA

Estrategia para el Robo de Información

CASO 1: CONFINAMIENTO DEL PROGRAMA DE UNA PC O SERVIDOR

Paso 1: llamar al personal del área de Instalación y Mantenimiento

Paso 2: Revisión de alguna carpeta compartida en el computador o Servidor.

Paso 3: Búsqueda por medio de un Software especializado de algún troyano que este robando los archivos (Avast, AVG, Kaspersky, Nod32, entre otros)

Paso 4: Eliminación del programa.

Paso 5: Parchar el Sistema Operativo en caso sea necesario.

CASO 2: ROBO DE INFORMACIÓN POR INTRUSIÓN EN LA BASE DE DATOS

Paso 1: Llamar al personal del área de Telemática

Paso 2: Revisión de los accesos.

Paso 3: Revisión de los log del Sistema.

Paso 4: Anulación de la vulnerabilidad.

CASO 3: ROBO DE INFORMACIÓN POR USURPACIÓN DE IDENTIDAD

Paso 1: Llamar al personal del área de Instalación y Mantenimiento

Paso 2: Cambio de Contraseña del Usuario Comprometido.

Estrategia para el Ataque de denegación en el servicio de servidores

CASO 1: ATAQUE DE DENEGACIÓN DE SERVICIO EN LOS DIFERENTES SERVIDORES.

Paso 1: llamar al personal del área de Instalación y Mantenimiento.

Paso 2: Revisión de los log's del sistema.

Paso 3: Revisión de los puertos abiertos del Servidor para la resolución de problemas / Utilización del Netstat)

Paso 4: Levantar un sniffer en el Proxy Firewall y realizar el análisis del tráfico para analizar el ataque.

Paso 5: Identificar el ataque y tomar las acciones correctivas para cortarlo.

Paso 6: Restablecer la operatividad del Servicio.

Estrategia contra Virus

CASO 1: IDENTIFICACIÓN DE VIRUS EN UNA PC

Paso 1: Llamar al personal del Área de Instalación y Mantenimiento

Paso 2: Sacar el Cable de Red de la PC comprometida

Paso 3: Pasar el antivirus que contenga la PC en ése momento

Paso 4: En caso el antivirus no elimine el virus, actualizar la versión o instalar un antivirus más potente,

Paso 4.1: En caso elimine el virus, realizar una actualización de la máquina.

Paso 4.2: En caso de no eliminarse el virus, revisar los puertos abiertos para la resolución de problemas / Utilización del Netstat), y contactarse con el administrador de red para ver si percibe alguna anomalía.

Paso 5: De no encontrarse en la Internet la solución al problema, se procederá a formatear la máquina comprometida,

CASO 2: PROPAGACIÓN DE UN VIRUS EN LA RED

Paso 1: Llamar al personal del área de Instalación y Mantenimiento.

Paso 2: Sacar el Cable de Red de las PC comprometidas para evitar el contagio del resto de PCs.

Paso 3: Pasar el antivirus que contenga la PC en ese momento

Paso 4: En caso el antivirus no elimine el virus, actualizar la versión o instalar un antivirus más potente.

Paso 4.1: En caso elimine el virus, realizar una actualización de la máquina.

Paso 4.2: En caso de no eliminarse el virus, revisar los puertos abiertos para la resolución de problemas / Utilización del Netstat, y contactarse con el administrador de red para ver si percibe alguna anomalía.

Paso 5: De no encontrarse en la Internet la solución al problema, se procederá a formatear todas aquellas máquinas comprometidas.

Estrategia del Error Humano

CASO 1: BORRADO INVOLUNTARIO DE ARCHIVOS

Paso 1: Llamar al personal del área de instalación y Mantenimiento.

Paso 2: Coordinar con el usuario que solo se asegura la recuperación a un 70 % de los archivos eliminados.

Paso 3: Instalar la herramienta de recuperación de archivos

Paso 4: indicar la ruta y el tipo de archivos borrados.

Estrategia en el Sismo

CASO 1: ANTE UN MOVIMIENTO TELÚRICO

Paso 1: Mantener la Calma

Paso 2: Ubicarse en bajo columnas o marco de las puertas

Paso 3: De preferencia evacuar la infraestructura por las salidas de emergencias indicadas.

Estrategia Incendio

CASO 1: ANTE UN INCENDIO DE GRAN MAGNITUD

Paso 1: Mantener la Calma.

Paso 2: En ese momento cualquiera que sea(n) el (los) procesos (s) que se esté(n) ejecutando los servidores, se deberá enviar un mensaje o avisar

vía telefónica (solo si el tiempo lo permite) advirtiendo el apagado de los servidores de OSINFOR.

Paso 3: Se apagará la caja principal de corriente ubicado en el primer piso – Entrada principal.

Paso 4: Tomando en cuenta que se trata de un incendio de mediana o mayor magnitud se debe tratar en lo posible de trasladar el servidor fuera del local.

Paso 5: Se abandonará el edificio en forma ordenada, lo más rápido posible, por las salidas destinadas para ello.

CASO 2: ANTE UN INCENDIO DE POCA MAGNITUD

Paso 1: Mantener la Calma.

Paso 2: En ese momento cualquiera que sea(n) el (los) procesos (s) que se esté(n) ejecutando los servidores, se deberá enviar un mensaje o avisar vía telefónicamente (solo si el tiempo lo permite) advirtiendo el apagado de los servidores de OSINFOR.

Paso 3: Se apagará la caja principal de corriente del edificio.

Paso 4: Tomando en cuenta que se trata de un incendio de poca mediana o mayor magnitud se debe tratar en lo posible de apagar el incendio utilizando los extinguidores ubicados en las zonas de emergencia.

Paso 5: En caso de no apagarse el fuego, se abandonará el edificio en forma ordenada, lo más rápido posible, por las salidas destinadas para ello.

OFICINA DE TECNOLOGIA DE LA INFORMACION V°B° JEFE OSINFOR

Estrategia contra Inundaciones

CASO 1: ANTE UNA INUNDACIÓN CON CORTO CIRCUITO

Paso 1: Mantener la Calma.

Paso 2: Pedir el cierre de la llave general de agua.

Paso 3: Revisar Constantemente que el agua no llegue a la puerta de escape, en caso de cercanía del agua, evacuar inmediatamente o subir a superficie aislante.

Paso 4: En caso exista en tiempo suficiente, se deberá enviar un mensaje o avisar vía telefónica (solo si el tiempo lo permite) advirtiendo el apagado de los servidores de OSINFOR.

Paso 5: Se apagará la caja principal de corriente del primer piso Entrada principal OSINFOR.

Paso 6: En caso de encontrar artefactos eléctricos en el suelo, se levantarán sobre una superficie alta, para evitar su contacto con el agua.

Estrategia de Averías de Hardware

CASO 1: ERROR EÍSICO DEL DISCO EN UNA ESTACIÓN DE TRABAJO

Paso 1: Ubicar el disco malogrado

Paso 2: Apagar el equipo

Paso 3: Retirar el disco defectuoso y probarlo en otro computador para asegurarnos de la avería.

Paso 4: En caso el disco este efectivamente defectuoso reemplazarlo por uno de las mismas características que el sustraído.

Paso 5: Formatear el nuevo disco y darle partición.

Paso 6: Colocar back up del usuario en el nuevo disco y verificar su buen estado.

CASO 2: ERROR FÍSICO DEL DISCO EN UN SERVIDOR

Paso 1: Ubicar el disco malogrado

Paso 2: Avisar a los usuarios que deben salir del sistema, para lo cual se enviarán correo electrónico, aviso telefónico vía anexos de OSINFOR.

Paso 3: Deshabilitar entrada al sistema para evitar que usuarios reintente ingreso.

Paso 4: Bajar el sistema y apagar el equipo. Paso 5: Retirar el disco defectuoso.

Paso 6: Reemplazar el disco por uno de las mismas características que el sustraído y colocarlo dentro del Servidor.

Paso 7: Formatear el nuevo disco y darle partición.

Paso 8: Restaurar último back up en nuevo disco y verificar su estado. Luego restaurar las modificaciones efectuadas desde esa fecha a la actualidad.

Paso 9: Habilitar las entradas al sistema para los usuarios.

CASO 3: ERROR DE MEMORIA EN UNA ESTACIÓN DE TRABAJO

Paso 1: Retirarla memoria de computador y colocarla nuevamente.

Paso 2: Iniciar la máquina nuevamente y revisar el estado de la memoria.

Paso 3: En caso persista la falla con la memoria, probarlas en otra PC con las mismas características para ubicar la memoria defectuosa.

Paso 4: En caso de ser problema de memoria, reemplazar por una memoria de las mismas características.

CASO 4: ERROR DE MEMORIA EN UN SERVIDOR

Paso 1: Avisar a los usuarios que deben salir del sistema, para lo cual se enviarán correo electrónico, aviso telefónico vía anexos de OSINFOR.

Paso 2: Deshabilitar entrada al sistema para que usuarios no reintenten ingreso.

Paso 3: Bajar el sistema y apagar el equipo.

Paso 4: Retirar la memoria de computador y colocarla nuevamente.

Paso 5: Iniciar la máquina nuevamente y revisar el estado de la memoria.

Paso 6: En caso persista la falla con la memoria, reemplazarla por una memoria de las mismas características.

CASO 5: ERROR DE TARJETAS CONTROLA DORAS

Paso 1: Avisar a los usuarios que deben salir del sistema, para lo cual se enviarán correo electrónico, aviso telefónico vía anexos de OSINFOR.

Paso 2: El servidor debe estar apagado, dando un correcto apagado del sistema.

Paso 3: Ubicar la posición de la tarjeta controladora.

Paso 4: Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar.

Paso 5: Retirar la conexión del Servidor con el concentrador, ésta ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.

Paso 6: Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar las entradas para estaciones de trabajo en las cuales se realizarán las pruebas.

Paso 7: Habitar las entradas al sistema para los usuarios.

CASO 6: ERROR DE IMPRESORA

Paso 1: Llamar al personal del área de instalación y Mantenimiento

Paso 2: Hacer revisión de la impresora sin perjudicar el contrato de la garantía de contar.

Paso 3: En caso sea necesario llamar al proveedor de la Impresora para su revisión.

OFICINA DE TECNOLOGIA DE LA INFORMACION
JEFE
OSINFOR

Estrategia en Falla General de Servidores principales o de producción.

CASO 1: ANTE LA FALLA GENERAL DE ALGUNO DE LOS SERVIDORES PRINCIPALES, SE PROCEDERÁ A LEVANTAR EL SERVIDOR BACKUP QUE CORRESPONDA.

Paso 1: ubicar el servidor back up correspondiente.

Paso 2: Cambiar el IP del Servidor Back up por el del Servidor Principal.

Paso 3: Revisar que los servicios estén trabajando correctamente.

Paso 4: Comenzar con los trabajos de recuperación de Datos del Servidor Principal.

Estrategia en la falla del Software

CASO 1: FALLA EN EL SOFTWARE

Paso 1: Llamar al personal del Equipo Funcional de Plataforma Tecnológica

Paso 2: Revisar el software instalado y verificar si contiene errores

Paso 3: Según el listado de licencia de software revisar si corresponde la instalación del software, y de ser así instalarlo en la máquina usuaria.

Estrategia en la falla del Portal Web e Intranet de OSINFOR

CASO 1: PORTAL WEB

Paso 1: Comunicarse con el administrador de Red de OSINFOR

Paso 2: Revisión de los servicios del servidor (US), PHP, MySql y SQL Server

Paso 3: Revisión general del Servidor

Estrategia sobre Interrupciones de Servicio o Suministros Esenciales

CASO 1: CORTE DEL FLUIDO ELÉCTRICO

Paso 1: Comunicarse con el administrador del Edificio para saber las causas del corte de fluido eléctrico.

3.5 PLAN DE RECUPERACION DE FALLAS Y/O DESASTRES

Es importante definir los procedimientos y planes de acción antes durante y después de la ocurrencia de la falla, siniestro o desastre dentro del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre –OSINFOR a fin de recuperar la total o mayor parte de información, archivos y equipos informáticos, evitando así la pérdida de tiempo y reducción del costo que tendría rehacer todo de nuevo.

Las actividades a realizar en el Plan de Recuperación de fallas y/o desastres se pueden clasificar en tres etapas:

3.5.1 ACTIVIDADES PREVIAS.

Se refiere al planeamiento, preparación, entrenamiento y ejecución de actividades de resguardo de información y equipos informáticos, que nos aseguren el proceso de recuperación de ser necesario

3.5.1.1 ESTABLECIMIENTO DE PLAN DE ACCIÓN.

En esta fase de planeamiento se debe de establecer los procedimientos relativos a:

A) Sistema de Información

Se deberá tener una relación de los Sistemas de información con los que se cuenta, tanto los realizados por el centro de cómputo como los hechos por las áreas usuarias, debiendo identificar toda información sistematizada o no, que sea necesario para la buena marcha de la institución.

La relación de Sistemas de Información deberá detallar los siguientes datos:

- Nombre del Sistema
- Lenguaje o Paquete con el que fue creado el Sistema, programas que lo conforman (tanto programas fuentes como programas objetos, rutinas, macros etc.).

- Las unidades orgánicas o de línea que usan la información del Sistema.
- El equipamiento necesario para un manejo optimo del sistema.
- Manual de configuración del sistema.

B) Equipos de Cómputo

Se tendrá en cuenta:

- Inventario actualizado de los equipos de manejo de información (Computadoras, impresoras, etc.), especificando su contenido (Software que usa), Su ubicación.

C) Obtención y Almacenamiento de los Respaldos de Información.

Se deberá de establecer los procedimientos para la obtención de copias de seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los Sistemas o aplicativos de la Institución.

3.5.1.2 FORMACIÓN DE EQUIPOS OPERATIVOS.

Todas las unidades Orgánicas o de líneas del organismo de supervisión de los recursos Forestales y de Fauna Silvestre, deberán designar un responsable de la seguridad de dicha información. Este puede ser el jefe del área o el Trabajador que administre la información.

Las acciones a tomar en conjunto en el Área de Informática y las oficinas serán:

- Proporcionar soporte técnico para las copias de respaldo de las aplicaciones.
- Supervisar procedimiento de respaldo y restauración.
- Supervisar la realización periódica de los back up's, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.
- Planificar y establecer los requerimientos de los sistemas operativos en cuanto a archivos, bibliotecas, utilitarios, etc., para los principales sistemas y subsistemas.
- Establecer procedimientos de seguridad en los sitios de recuperación.
- Organizar la prueba de hardware y software.
- Ejecutar trabajos de recuperación.
- Participar en las pruebas y simulacros de desastres.

3.5.2 ACTIVIDAD DURANTE EL DESASTRE

Cuando se presente la contingencia, se deberá ejecutar las siguientes actividades, las que fueron planificadas previamente:

3.5.2.1 PLAN DE EMERGENCIAS

Este plan deberá incluir todas las actividades a realizar por cada una de las personas que se pueden encontrar presentes en el área donde ocurre la contingencia.

Para la implementación del plan de emergencia, es conveniente prever la ocurrencia del Siniestro tanto durante el día o la noche o incluso en la madrugada. Para ello el plan deberá incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, debiendo detallar:

- Vías de salida o escape.
- Plan de Evacuación del Personal.
- Plan de puesta a buen recaudo de los activos (incluyendo los activos de Información) de la Institución (si las circunstancias del siniestro lo posibilitan)
- Ubicación y señalización de los elementos contra el siniestro (extinguidores, cobertores contra agua, etc.)
- Secuencia de llamadas en caso de siniestro, tener a la mano: elementos de iluminación (linternas), lista de teléfonos de Bomberos / Ambulancia, Jefatura de Seguridad y de su personal (equipos de seguridad) nombrados para estos casos.

Si bien es cierto que la integridad de las personas es lo primordial, se deben adoptar medidas con el fin de asegurar la información:

- Apagar los equipos al momento de detectar el siniestro.
- Desconectar el equipo para su retiro del lugar del siniestro.
- Proteger y cubrir los equipos.
- Enseñanza del manejo de extintores.

En las contingencias de equipos de cómputo, fallas humanas, acción de virus, etc.; se debe solicitar ayuda del personal de informático, si es que en el área no existe una persona capacitada para resolver el problema.

3.5.2.2 FORMACIÓN DE EQUIPOS

Establecer claramente cada equipo (nombres, puestos, ubicación, etc.) con funciones claramente definidas a ejecutar durante el siniestro.

3.5.2.3 ENTRENAMIENTO

Establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestros, de acuerdo a los roles que se le hayan asignado en los planes de evacuación del personal o equipos,

para minimizar costos se puede aprovechar fechas de recarga de extinguidores, charlas de los proveedores, etc.

Un aspecto importante es que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los elementos directivos, dando el ejemplo de la importancia que la alta dirección otorga a la Seguridad Institucional.

3.5.3 ACTIVIDADES DESPUÉS DEL DESASTRE.

Después de ocurrido el Siniestro o Desastre es necesario realizar las actividades, Inmediatamente después que el siniestro ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que sistemas se están afectando, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.

3.5.3.1 PRIORIZACIÓN DE ACTIVIDADES DEL PLAN DE ACCIÓN.

El Plan de acción es general y contempla una pérdida total, la evaluación de daños reales y su comparación contra el Plan, nos dará la lista de las actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra Institución.

3.5.3.2 EJECUCIÓN DE ACTIVIDADES.

La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el Plan de acción. Cada uno de estos equipos deberá contar con un coordinador que deberá reportar el avance de los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato a la jefatura a cargo del Plan de Contingencias.

Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de la Institución, y la segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio de nuestro Sistema e imagen Institucional.

3.5.3.3 EVALUACIÓN DE RESULTADOS.

Una vez concluidas las labores de Recuperación del (los) Sistema(s) que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo, etc.

De la Evaluación de resultados y del siniestro en sí, deberían de salir dos tipos de recomendaciones:

- Una la retroalimentación del plan de Contingencias y.
- Una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

3.5.3.4 RETROALIMENTACIÓN DEL PLAN DE ACCIÓN.

Con la evaluación de resultados, debemos de optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

El otro elemento es evaluar cuál hubiera sido el costo de no haber tenido nuestra Institución el plan de contingencias llevado a cabo.

4 ACCIONES FRENTE A LOS TIPOS DE RIESGO

4.1 INCENDIO O FUEGO

Cuando el daño del edificio ha sido mayor, evaluar el traslado a un nuevo local, hasta considerar la posibilidad del traslado. El procedimiento de respuesta a esta emergencia Cuando el daño ha sido menor:

a) Tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones. Responsable encargado de Soporte y Mantenimiento

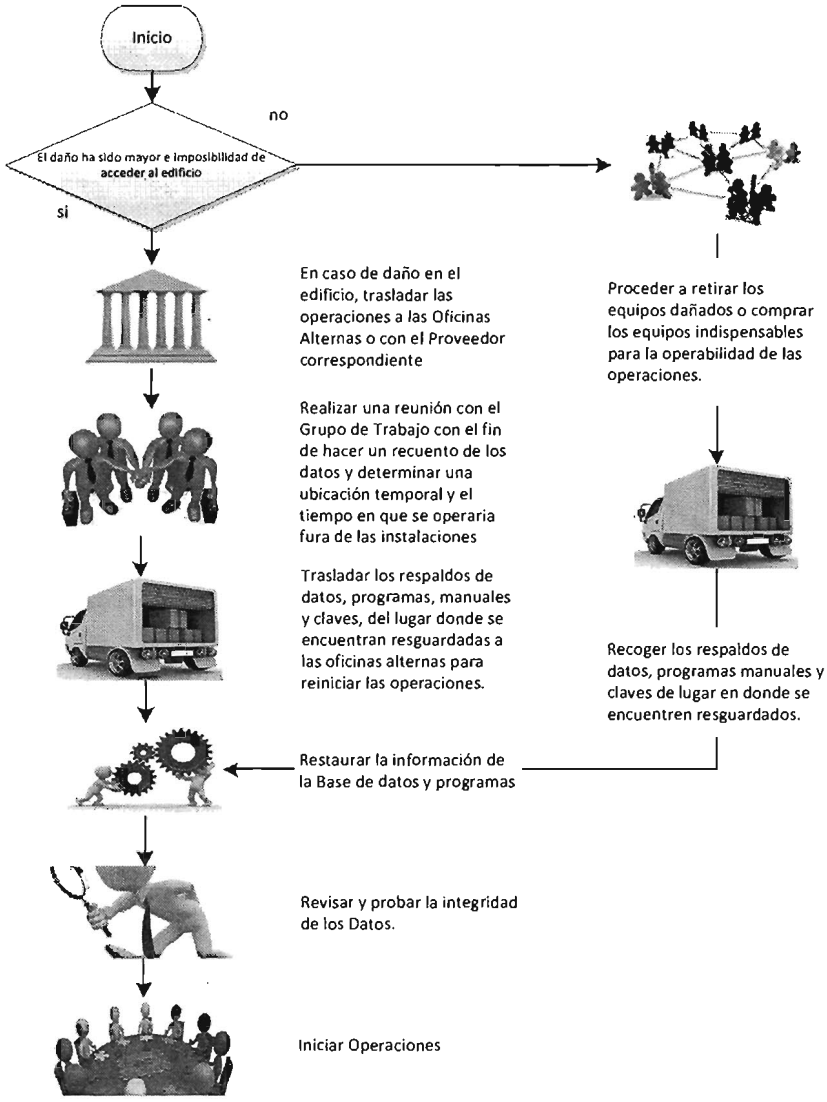
b) Se recoge los respaldos de datos, programas, manuales y claves. Responsable encargado de Redes.

c) Instalar el sistema operativo. Responsable encargado de Soporte y Mantenimiento

d) Restaurar la información de las bases de datos y programas. Responsable encargado de Desarrollo.

e) Revisar y probar la integridad de los datos. Responsable encargado de Desarrollo.

GRAFICO 03 – DIAGRAMA DE RESPUESTA DE EMERGENCIA DE "INCENDIO"



Fuente: OTI-OSINFOR.

¿QUE HACER? Antes, Durante y Después de un INCENDIO.

ANTES:

- Verificar periódicamente que las instalaciones eléctricas estén en perfecto estado.
- No concentrar grandes cantidades de papel, ni fumar cerca de químicos o sustancias volátiles.
- Verificar las condiciones de extintores e hidratantes y capacitar para su manejo.
- Si se fuma, procurar no arrojar las colillas a los cestos de basura, verificar que se hayan apagado bien los cigarrillos y no dejarlos en cualquier sitio, utilizar ceniceros.
- No almacenar sustancias y productos inflamables.
- No realizar demasiadas conexiones en contactos múltiples, evitar la sobrecarga de circuitos eléctricos.

- Por ningún motivo mojar las instalaciones eléctricas, recordar que el agua es un buen conductor de la electricidad.
- Si se detecta cualquier anomalía en los equipos de seguridad (extintores, hidratantes, equipo de protección personal, etc.) y en las instalaciones eléctricas, reportar de inmediato al encargado de Seguridad.
- Mantener siempre el área de trabajo limpia y en orden, ya que no hacerlo es una de las causas que provocan incendios.
- Tener a la mano los números telefónicos de emergencia.
- Portar siempre el fotocheck de identificación.

DURANTE

- Ante todo se recomienda conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.
- En ese momento cualquiera que sea(n) el (los) proceso(s) que se esté(n) ejecutando
- en el Computador Principal, se deberá (si el tiempo lo permite) "Salir de Red y Apagar Computador": Down en el (los) servidor(es), apagar (OFF) en la caja principal de corriente de la sala de servidores de la OTI .
- Si se conoce sobre el manejo de extintores, intenta sofocar el fuego, si este es considerable no trates de extinguirlo con los propios medios, solicitar ayuda.
- Si el fuego esta fuera de control, realizar evacuación del inmueble, siguiendo las indicaciones del Personal de bomberos.
- No utilizar elevadores, descender por las escaleras pegado a la pared que es donde posee mayor resistencia, recuerda: No gritar, No empujar, No correr y dirigirse a la zona de seguridad.
- Si hay humo donde nos encontramos y no podemos salir, mantenernos al ras del piso, cubriendo tu boca y nariz con un pañuelo bien mojado y respira a través de el, intenta el traslado a pisos superiores.
- Las personas que se encuentren en los últimos pisos, deberán abrir ventanas para que el humo tenga una vía de salida y se descongestionen las escaleras.
- Si es posible mojar la ropa.
- Verifica si las puertas están calientes antes de abrirlas, si lo están, busca otra salida.

DESPUES

- Retirarse inmediatamente del área incendiada y ubícate en la zona de seguridad externa que te corresponda.
- No obstruir las labores del personal especializado, dejar que los profesionales se encarguen de sofocar el incendio.
- El personal calificado realizara una verificación física del inmueble y definirá si esa en condiciones de ser utilizado normalmente.
- Colaborar con las autoridades.

4.2 ROBO COMÚN DE EQUIPOS Y ARCHIVOS.

Analizar las siguientes situaciones:

- En qué tipo de vecindario se encuentra la Institución
- Las computadoras se ven desde la calle
- Hay personal de seguridad en la Institución y están ubicados en zonas estratégicas
- Cuánto valor tienen actualmente las Bases de Datos
- Cuánta pérdida podría causar en caso de que se hicieran públicas
- Asegurarse que el personal es de confianza, competente y conoce los Procedimientos de seguridad.
- Trabajo no supervisado, especialmente durante el turno de noche, malas
- técnicas de contratación, evaluación y de despido de personal.

4.3 VANDALISMO.

- Si el intento de vandalismo es mayor, se presenta un grave riesgo dentro del área del Centro de Cómputo ya que puede dañar los dispositivos perdiendo toda la información y por consecuencia las actividades se verían afectadas en su totalidad, así como el servicio proporcionado.
- A continuación se menciona una serie de medidas preventivas:
  - Establecer vigilancia mediante cámaras de seguridad en el Site, el cual registre todos los movimientos de entrada del personal.
  - Instalar identificadores mediante tarjetas de acceso.
  - Determinar lugares especiales, fuera del centro de datos, para almacenar los medios magnéticos de respaldo y copia de la documentación de referencia y procedimientos de respaldo y recuperación (se puede contratar una caja de seguridad bancaria donde se custodiaran los datos e información crítica).
- Los principales conflictos que pudieran presentarse son:
  - En cuanto a la red, si el sistema llegará a presentar una falla no habría personal que atendiera la problemática y por consecuencia se detendrían las operaciones a falta del monitoreo a los distintos sistemas.
  - Respecto a los dispositivos de almacenamiento, si se mantienen los respaldos únicamente dentro de la Delegación Miguel Hidalgo, sería imposible reanudar las actividades que un momento dado fueran críticas, como la nómina, contabilidad, etc.; en un sitio alterno, ya que no contarían con copia de la información.

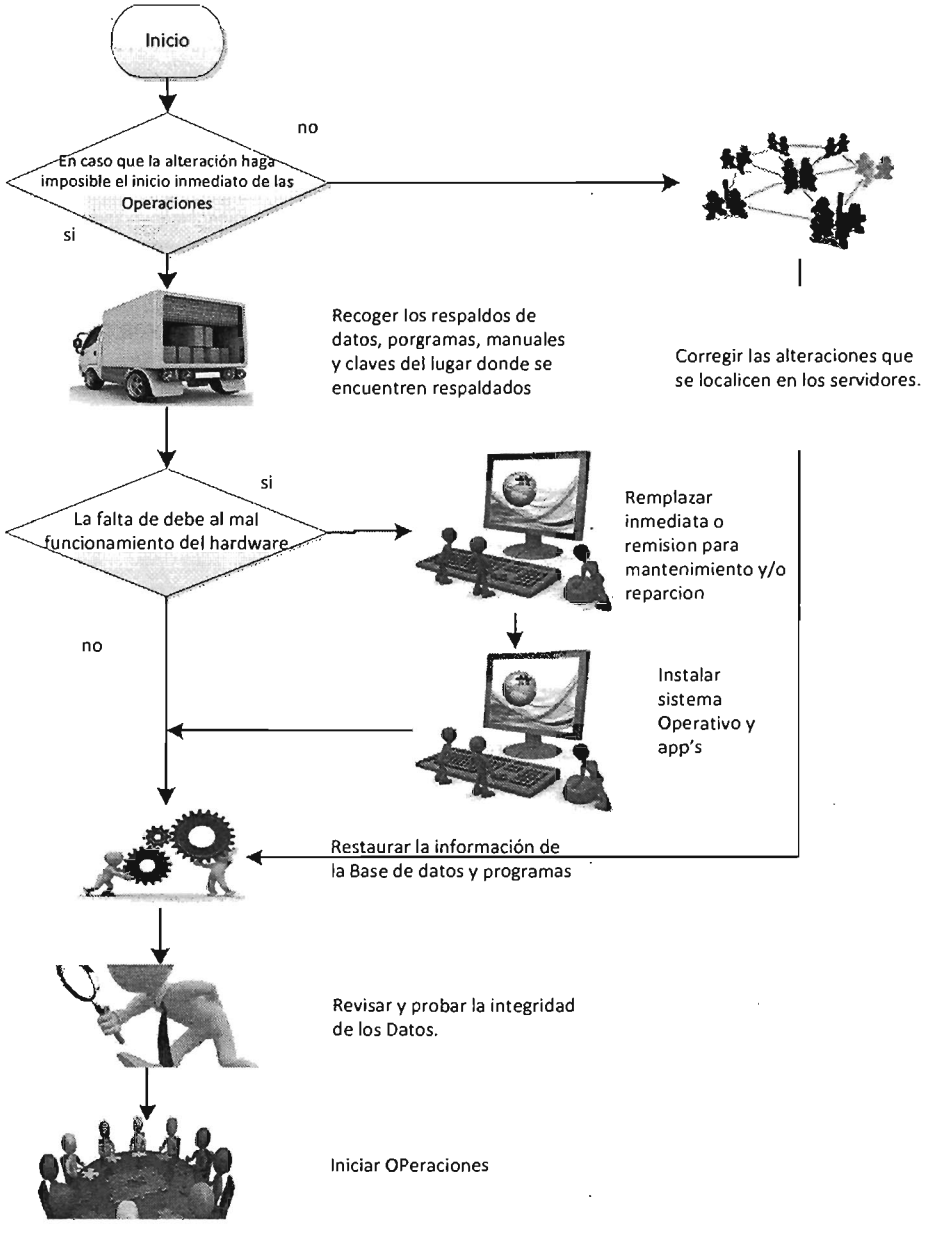
4.4 EQUIVOCACIONES.

- Cuánto saben los empleados de computadoras o redes.
- Durante el tiempo de vacaciones de los empleados, ¿qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?
- Difusión de Manuales de Usuario y operación del correcto uso del software y el hardware a todo el personal que labora de manera directa con los equipos informáticos.

4.5 FALLAS EN LOS EQUIPOS.

- Las fallas del sistema de red pueden deberse al mal funcionamiento de los equipos o a la pérdida de configuración de los mismos por lo que se deben evaluar las fallas para determinar si estas se derivan del mal funcionamiento de un equipo o de la pérdida de su configuración. El procedimiento de respuesta a esta emergencia se ve en la figura adjunta.

GRAFICO 04 – DIAGRAMA DE FALLA EN LOS EQUIPOS



Fuente: OTI-OSINFOR.

4.6 ACCIÓN DE VIRUS INFORMÁTICO.

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

Para servidor:

- Se contará con antivirus para el sistema; aislar el virus para su futura investigación.
- El antivirus muestra el nombre del archivo infectado y quién lo usó.
- Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

Para computadoras fuera de red:

- Utilizar los discos de instalación que contenga sistema operativo igual o mayor en versión al instalado en el computador infectado.
- Insertar el disco de instalación antivirus, luego instalar el sistema operativo, tal forma que revise todos los archivos y no sólo los ejecutables. De encontrar virus, dar la opción de eliminar el virus. Si es que no puede hacerlo el antivirus, recomendará borrar el archivo, tomar nota de los archivos que se borren. Si éstos son varios pertenecientes al mismo programa, reinstalar al término del Scaneado. Finalizado el scaneado, reconstruir el Master Boot del disco duro

4.7 ACCESOS NO AUTORIZADOS.

Enfatiza los temas de:

- Contraseñas. Las contraseñas son a menudo, fáciles de adivinar u obtener mediante ensayos repetidos. Debiendo implementarse un número máximo (3) de intentos infructuosos. La OTI implementa la complejidad en sus contraseñas de tal forma que sean más de siete caracteres y consistentes en números y letras.
- Entrampamiento al intruso. Los sistemas deben contener mecanismos de entrampamiento para atraer al intruso inexperto. Es una buena primera línea de detección, pero muchos sistemas tienen trampas inadecuadas.
- Privilegio. En los sistemas informáticos de la OTI, cada usuario se le presenta la información que le corresponde. Para un intruso que busque acceder a los datos de la red, la línea de ataque más prometedora será una estación de trabajo de la red. Estas se deben proteger con cuidado. Debe habilitarse un sistema que impida que usuarios no autorizados puedan conectarse a la red y copiar información fuera de ella, e incluso imprimirla. Por supuesto, una red deja de ser eficiente si se convierte en una fortaleza inaccesible. En este punto el administrador de la red ha clasificado a los usuarios de la red en "Grupos" con el objeto de adjudicarles el nivel de seguridad y perfil adecuado.

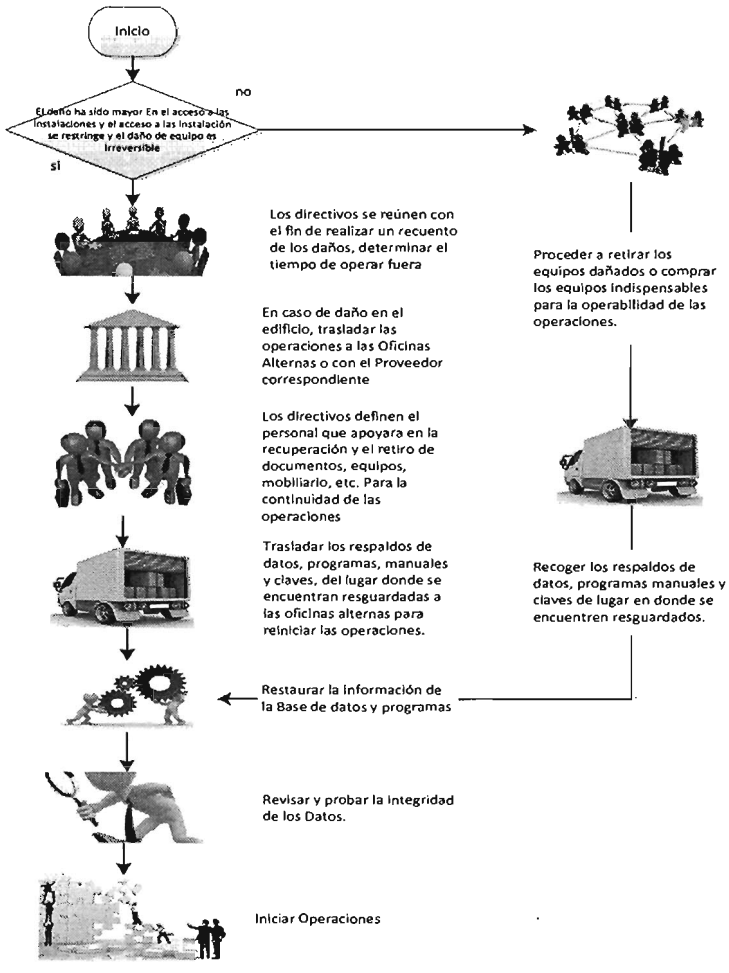
4.8 FENÓMENOS NATURALES.

a) Terremoto e Inundación

- Para evitar problemas con inundaciones ubicar los servidores a un promedio de 50 cm. de altura.

- En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.
- Cuando el daño del edificio ha sido mayor, evaluar el traslado a un nuevo local, hasta considerar la posibilidad del traslado.
- Cuando el daño ha sido menor se procede:
  a) Tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones. Responsable encargado de Soporte y Mantenimiento
  b) Recoger los respaldos de datos, programas, manuales y claves. Responsable encargado de Redes.
  c) Instalar el sistema operativo. Responsable encargado de Soporte y Mantenimiento
  d) Restaurar la información de las bases de datos y programas. Responsable
  e) encargado de Desarrollo.
  f) Revisar y probar la integridad de los datos. Responsable encargado de Desarrollo

GRAFICO 05 – DIAGRAMA DE RESPUESTA PARA FENOMENOS NATURALES



Fuente: OTI-OSINFOR.

4.9 ROBO DE DATOS.

Se previene a través de las siguientes acciones:

- **Acceso no Autorizado**: Sin adecuadas medidas de seguridad se puede producir accesos no autorizados a:
  - Área de Sistemas.
  - Computadoras personales y/o terminales de la red.
  - Información confidencial.
- **Control de acceso al Área de Sistemas**: El acceso al área de Informática estará restringido:
  - Sólo ingresan al área el personal que trabaja en el área.
  - El ingreso de personas extrañas solo podrá ser bajo una autorización.
- **Acceso Limitado a los Terminales**: Cualquier terminal que puede ser utilizado como acceso a los datos de un Sistema, las siguientes restricciones pueden ser aplicadas:
  - Determinación de los períodos de tiempo para los usuarios o las terminales.
  - Designación del usuario por terminal.
  - Limitación del uso de programas para usuario o terminales.
  - Límite de tentativas para la verificación del usuario, tiempo de validez de las señas, uso de contraseñas, cuando un terminal no sea usado pasado un tiempo predeterminado (5 - 10 minutos).
- **Niveles de Acceso**: Los programas de control de acceso deberán identificar a los usuarios autorizados a usar determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidos a la lectura o modificación en sus diferentes formas.
  - Nivel de consulta de la información.- privilegio de lectura.
  - Nivel de mantenimiento de la información.- El concepto de mantenimiento de la información consiste en: Ingreso, Actualización, Borrado.

4.10 MANIPULACIÓN Y SABOTAJE.

- **La protección contra el sabotaje requiere:**
  a) Una selección rigurosa del personal.
  b) Buena administración de los recursos humanos.
  c) Buenos controles administrativos.
  d) Buena seguridad física en los ambientes donde están los principales componentes del equipo.
  e) Asignar a una persona la responsabilidad de la protección de los equipos en cada área.
- **A continuaciones algunas medidas que se deben tener en cuenta para evitar acciones hostiles:**
  a) Mantener una buena relación de trabajo con el departamento de policía local.
  b) Mantener adecuados archivos de reserva (back ups).
  c) Planear para probar los respaldos (back ups) de los servicios de procesamiento de datos.

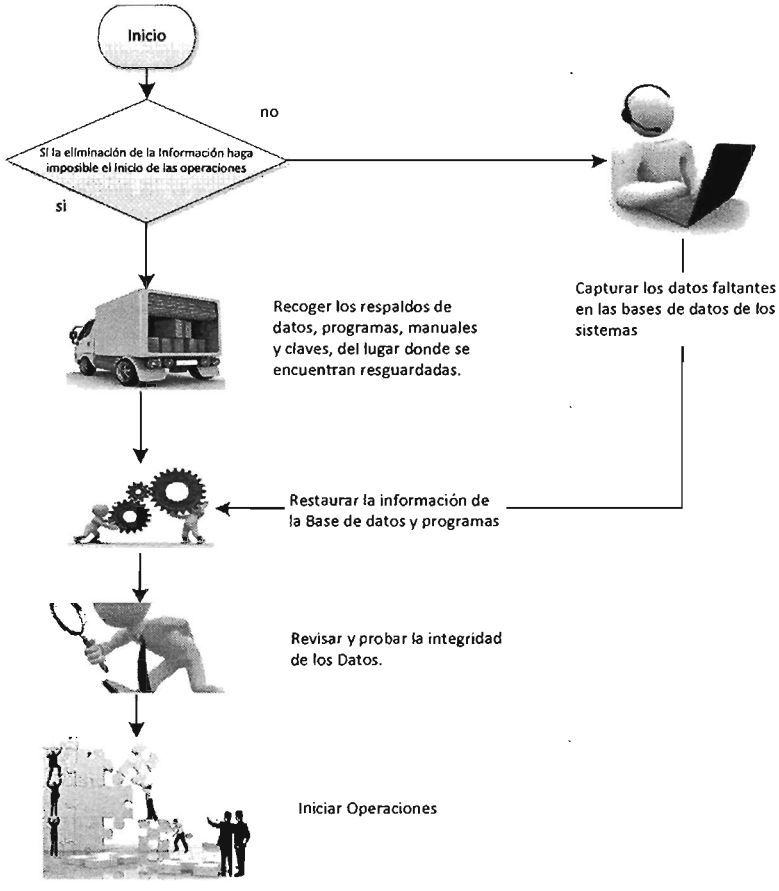
d) Identificar y establecer operaciones criticas prioritarias cuando se planea el respaldo de los servicios y la recuperación de otrás actividades.

e) Usar rastros de auditorías o registros cronológicos (logs) de transacción como medida de seguridad.

- **Cuando la información eliminada se pueda volver a capturar, se procede con lo siguiente:**
  - Capturar los datos faltantes en las bases de datos de los sistemas. Responsable: Áreas afectadas
  - Revisar y probar la integridad de los datos. Responsable: Desarrollo de Sistemas.

La eliminación de la información, puede volverse a capturar en la mayoría de los casos, sin embargo en algunas ocasiones, las pérdidas demandan demasiado tiempo requerido para el inicio de las operaciones normales, por tal motivo es recomendable acudir a los respaldos de información y restaurar los datos pertinentes, de esta forma las operaciones del día no se verían afectados.

GRAFICO 06 – DIAGRAMA DE RESPUESTA PARA MANIPULACION Y SABOTAJE



Fuente: OTI-OSINFOR.

5 RECOMENDACIONES

- Programar las actividades propuestas en el presente Plan de Contingencias y Seguridad de Información.
- Hacer de conocimiento general el contenido del presente Plan de Contingencias y Seguridad de Información, con la finalidad de instruir adecuadamente al personal de OSINFOR.
- Adicionalmente al plan de contingencias se debe desarrollar reglas de control y pruebas para verificar la efectividad de las acciones en caso de la ocurrencia de los problemas y tener la seguridad de que se cuenta con un método seguro.
- Se debe tener una adecuada seguridad orientada a proteger todos los recursos informáticos desde el dato más simple hasta lo más valioso que es el talento humano; pero no se puede caer en excesos diseñando tantos controles y medidas que desvirtúen el propio sentido de la seguridad, por consiguiente, se debe hacer un análisis de costo/beneficio evaluando las consecuencias que pueda acarrear la pérdida de información y demás recursos informáticos, así como analizar los factores que afectan negativamente la productividad de OSINFOR.