REPÚBLICA DE HONDURAS

INSTITTUTO NACIONAL DE PREVISIÓN DEL MAGISTERIO
(INPREMA)

MEMORANDUM N. ADE/005-2018

PARA: LIC.CARLOS SALGADO
Jefe de Unidad de Atención al Usuario Financiero

DE: LIC. SONIA RAMÍREZ ALVARADO
Técnico del Directorio

ASUNTO: REMISION DE RESOLUCIONES PARA EL PORTAL DE TRANSPARENCIA

FECHA: 5 DE ENERO DEL 2018

Atendiendo su solicitud realizada por medio de Memorándum UAUF 544-217 del 18 de diciembre del 2017, sírvase encontrar adjunto las Resoluciones de los meses de noviembre y diciembre 2017. (se adjuntan las resoluciones de noviembre porque en la fecha de presentación correspondiente, aun no estaban firmadas dichas resoluciones):

CTA	178	31/10/2017	APROBACIÓN DE MODIFICACIÓN DE REGLAMENTO DE PRÉSTAMOS DEL INPREMA.
CTA	181	07/11/2017	APROBACIÓN DE INICIO DEL PROCESO DE LICITACIÓN PÚBLICA NACIONAL LPN 001 2017 "CONTRATACIÓN DE SERVICIOS DE LIMPIEZA Y ASEO PARA LAS OFICINAS DEL INPREMA EN TEGUCIGALPA, LA CEIBA Y SANTA ROSA DE COPÁN PARA EL AÑO 2018.
CTA	182	07/11/2017	APROBACIÓN DE INICIO DEL PROCESO DE LICITACIÓN PÚBLICA NACIONAL LPN 002 2017 "CONTRATACIÓN DE SERVICIOS DE INTERNET Y CANAL DE DATOS PARA EL INPREMA A NIVEL NACIONAL PARA EL PERIODO 2018.
GADMF	183	07/11/2017	APROBACIÓN DE PRECIO, COMERCIALIZACIÓN Y VENTA DE LOS LOTES REMANENTES DEL PROYECTO RESIDENCIAL JULIO ROMERO, UBICADO EN LA CIUDAD DE GRACIAS LEMPIRA.
USI	189	07/11/2017	APROBACIÓN DEL MANUAL DE POLITICAS DE LA TECNOLOGIA DE INFORMACION Y COMUNICACIONES
CTA	192	21/11/2017	APROBACIÓN DE INICIO DEL PROCESO DE LICITACIÓN PRIVADA LP 005-2017 "CONTRATACIÓN DE SERVICIOS DE ARRENDAMIENTO DE FOTOCOPIADORAS PARA EL INPREMA A NIVEL NACIONAL CORRESPONDIENTE AL PERÍODO 2018"
CTA	193	21/11/2017	APROBACIÓN DE INICIO DEL PROCESO DE LICITACIÓN PÚBLICA NACIONAL LPN 003-2017 "CONTRATACION DE SEGUROS CORPORATIVOS PARA EL INPREMA"
UAUF	209	06/12/2017	APROBACIÓN DE LA CERTIFICACIÓN DE FUNCIONAMIENTO DE GOBIERNO CORPORATIVO.
UR	211	06/12/2017	APROBACIÓN DEL MANUAL DE GESTIÓN DE RIESGO TECNOLÓGICO
CTA	220	06/12/2017	APROBACIÓN DE RENOVACIONES DE CONTRATOS DE ARRENDAMIENTO PARA EL AÑO 2018 : a. ARRENDAMIENTO DATA CENTER COLLOCATION EN SPS b. ARRENDAMIENTO DE LOCAL PARA OFICINA REGIONAL DE LA CEIBA c. ARRENDAMIENTO DE LOCAL PARA OFICINA REGIONAL DE SANTA ROSA DE COPÁN

Atentamente,

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

REPÚBLICA DE HONDURAS
INSTITUTO NACIONAL
DE
PREVISIÓN DEL MAGISTERIO

INPREMA

Número Piloto: 2232-4036
2232-5613
Técnico Financiero: 2232-5269
Fax Secretaría: 2232-4651
Tesorería: 2239-0776
Apartado Postal No. 92
Comayagüela, M.D.C.

Oficio Nº DE-221-2017
Tegucigalpa, M.D.C., 14 de diciembre de 2017

Abogada
Alejandra Isabel Medina Alcántara
Secretaria General
Presente

Abogada Medina:

Para su conocimiento y demás fines, transcribo a usted la Resolución No. **UR/211/06-12-2017** emitida por los Directores Especialistas del Instituto, en Sesión Ordinaria Celebrada el día 6 de diciembre de 2017, según **Acta Nº 38-2017.**

Resolución No. UR/211/06-12-2017. El Instituto Nacional de Previsión del Magisterio, a los 6 días del mes de diciembre del dos mil diecisiete (2017).

CONSIDERANDO (1): Que mediante Decreto Legislativo No. 247-2011, de fecha catorce (14) de diciembre de dos mil once (2011), se aprobó la Ley del Instituto Nacional de Previsión del Magisterio, la cual establece en el artículo 9 que el Órgano Superior de Administración y Ejecución, será el Directorio de Especialistas para la Administración del INPREMA, que para efectos de la Ley se denominará el Directorio.- **CONSIDERANDO (2):** Que en sesión del ocho (8) de Mayo de dos mil doce (2012), y mediante Resolución CI No. 243/08-05-2012, se nombró, con base al artículo 128 del Decreto Legislativo 247-2011, como Directores Especialistas del Instituto Nacional de Previsión del Magisterio a los señores **ERNESTO EMILIO CARÍAS CORRALES, NESSY ELDENIDA MARTÍNEZ HERNÁNDEZ** y **CÉSAR GUIOVANY GUIFARRO**, designando como Presidente al Licenciado **ERNESTO EMILIO CARIAS CORRALES**.- **CONSIDERANDO (3):** Que mediante Instrumento Público No. 34 autorizado en la ciudad de Tegucigalpa, M.D.C., en fecha once (11) de Mayo del 2012, por el Notario **JOSE ANTOLÍN CAYETANO BERNARDEZ**, e inscrito bajo el Número 96 del Tomo 104 del Registro Especial de Poderes del Registro de la Propiedad de Francisco Morazán, se confirió Poder General de Administración y Representación a favor del Señor Ernesto Emilio Carías Corrales, Director Presidente del INPREMA.**- CONSIDERANDO (4):** Que la Asamblea de Participantes y aportantes del INPREMA como órgano de planificación y dirección del INPREMA, mediante la resoluciones APA/009/08-05-2017 y APA/010/05-06-2017, determinó prorrogar el desempeño de las funciones y atribuciones establecidas en la Ley del INPREMA al Directorio de Especialistas conformado por los Licenciados Ernesto Emilio Carias Corrales, Nessy Eldenida Martínez Hernández y Cesar Guiovany Guifarro Rivera hasta haberse nombrado el nuevo Directorio de Especialistas de este instituto previsional; con fundamento en los Artículos: 262 Constitución de la República; 23, 24, 25, 26 y 72 de la Ley de Procedimiento Administrativo; 48, 116, 120 y 122 de la Ley de Administración Pública; 1, 4, 6, 7,, 10, 20 y demás aplicables a la Ley del INPREMA..**- CONSIDERANDO (5):** Que la Comisión Nacional de Bancos y Seguros emitió la Resolución No.1301/22-11-2005 donde establece las "NORMAS PARA REGULAR LA ADMINISTRACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES EN LAS INSTITUCIONES DEL SISTEMA FINANCIERO".**- CONSIDERANDO (6):** Que la Comisión Nacional de Bancos y Seguros emitió la Resolución SB No.1321/02-08-2011 donde establece a "NORMA DE GESTIÓN DE RIESGO OPERATIVO".**- CONSIDERANDO (7):** Que dicha norma en su ARTÍCULO 8.- FACTORES DE RIESGO OPERATIVO, considera en el numeral C a la Tecnología como uno de los factores que pueden detonar un riesgo operativo.-**CONSIDERANDO (8):** Que la misma Norma en su ARTICULO 21 manda

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

Número Piloto: 2232-4036
2232-5613
Técnico Financiero: 2232-5269
Fax Secretaría: 2232-4651
Tesorería: 2239-0776
Apartado Postal No. 92
Comayagüela, M.D.C.

a las instituciones supervisadas a implementar un sistema de gestión de la continuidad del negocio y un sistema de gestión de la seguridad de la información orientado a garantizar la integridad, confidencialidad y la disponibilidad de la información**. CONSIDERANDO (9):** Que es atribución del Directorio de Especialistas: Dirigir el Instituto; definir la estructura y organización de las dependencias necesarias para su correcto funcionamiento; vigilar el cumplimiento de la gestión administrativa; Resolver y dictaminar sobre los asuntos que, en debido tiempo y forma, presenten para análisis los Gerentes de Área o Jefe de División, entre otras. **POR TANTO:** El Directorio de Especialistas del Instituto Nacional de Previsión del Magisterio (INPREMA), en aplicación de los artículos 14, numeral 1), 2) y 5) del decreto 247-2011 y del Acta No 7 de fecha 28 de noviembre de 2017 del Comité de Riesgos, **RESUELVE: PRIMERO:** Aprobar el siguiente:

MANUAL DE ADMINISTRACIÓN DE RIESGO TECNÓLOGICO
INSTITUTO NACIONAL DE PREVISIÓN DEL MAGISTERIO
TEGUCIGALPA MDC
NOVIEMBRE 2017

1. INTRODUCCIÓN

El avance acelerado al que se han enfrentado diversas organizaciones, está estrechamente vinculado con el incremento en el uso de la tecnología de la Información, así como la evolución en la forma de su utilización. Este progreso ha permitido que la tecnología de Información se convierta en una herramienta trascendental para diseñar e implementar mejores y más efectivos procesos, generando oportunidades de crecimiento, así como la posibilidad de contar con Información veraz y oportuna para una eficaz toma de decisiones.

Sin embargo, esto conlleva a tener una dependencia en la Información y en los sistemas que la proporcionan. Este tipo de dependencia trae consigo una serie de riesgos inherentes que las organizaciones deben de enfrentar, a estas exposiciones se les conoce como riesgo tecnológico. Dicho riesgo es parte complementaria al riesgo operativo (definido dentro del Manual de Administración de Riesgo Operativo), el cual mientras exista este entorno, su gestión desempeñará un papel crítico y esencial dentro de las operaciones como factor de control estratégico.

El INPREMA no es la excepción, sus operaciones se realizan sobre una estructura tecnológica, con lo cual se hace más eficiente y oportuna la atención a los afiliados, sin embargo, está expuesto a modos de falla inherentes a dichas operaciones los cuales pueden materializarse al no contar con una adecuada administración del Riesgo Tecnológico.

Por tal razón, es importante desarrollar actividades para la administración del Riesgo Tecnológico como una práctica adicional a la administración integral de riesgos, que conlleve a minimizar los posibles impactos negativos por su uso y, desarrollar una estrategia basada en riesgos tecnológicos que permita fortalecer el proceso de toma de decisiones.

Para llegar a un estándar internacional en materia de Riesgo Tecnológico, se recomienda observar las mejores prácticas establecidas por el Comité de Basilea, así como COBIT (Control Objetives for Information and Related Technology) e ISO (Organización Internacional por la Normalización) /IEC 27001(International Electrotechnical Commission) para su mejor administración y gobierno.

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

Número Piloto: 2232-4036
2232-5613
Técnico Financiero: 2232-5269
Fax Secretaría: 2232-4651
Tesorería: 2239-0776
Apartado Postal No. 92
Comayagüela, M.D.C.

Asimismo, es interés del Instituto considerar y cumplir en lo posible, el marco regulatorio definido por la Comisión Nacional de Bancos y Seguros (CNBS).

2. OBJETIVOS

General

Concientizar a los dueños de los procesos y a los responsables de los sistemas de Información, de la existencia de riesgos y de la necesidad de mitigarlos a tiempo, ofreciendo un método sistemático de trabajo definido y repetible para el análisis y evaluación de tales riesgos; para ayudar a descubrir y planificar las medidas oportunas para mantener los riegos de TIC bajo control de acuerdo a las mejores prácticas.

Específicos

1. Preparar al Instituto para el proceso de administración de Riesgo Tecnológico basado en buenas prácticas, implementando un marco de trabajo para la gestión del Riesgo Tecnológico para una mejor gobernabilidad de las Tecnologías de la Información y Comunicaciones.
2. Contar con un método para poder identificar, evaluar, administrar, controlar y reportar los riesgos tecnológicos que enfrenta la institución, con el fin de mitigar o eliminar el posible impacto negativo de dichos riesgos en el Instituto.

3. ALCANCE

De aplicación general para todas las áreas del Instituto y los procesos que tengan implícito un riesgo tecnológico.

4. DEFINICIONES

Para los efectos de aplicación de la normativa vigente, de este manual y bajo la perspectiva de la tecnología de información y comunicaciones, deberán considerarse las siguientes definiciones:

Activo. Recursos del sistema de Información o relacionados con éste, necesarios para que el Instituto funcione correctamente

Administración Integral de Riesgos. Conjunto de objetivos, políticas, procedimientos y acciones que se llevan a cabo para identificar, medir, vigilar, limitar, controlar, informar y revelar los distintos riesgos a que se encuentra expuesto el Instituto.

Amenaza. Agente o circunstancia capaz de explotar una o más vulnerabilidades.

Ataques de Denegación de Servicio: Envío de solicitudes a servidores o equipos de comunicación que provoquen saturación en sus memorias para que de esta forma dejen de funcionar temporalmente y no presten los servicios que tengan configurados.

Ataques de Diccionario: Prueba de combinaciones de todos los usuarios y contraseñas posibles basados en un diccionario en español, inglés o cualquier otro idioma, para ingresar de manera ilegal a un sistema informático.

Ataques de Fuerza Bruta: Prueba de combinaciones de todos los usuarios y contraseñas posibles basados en todos los caracteres posibles, para ingresar ilegalmente a un sistema informático.

Canal de Comunicación: Métodos tecnológicos para la comunicación entre los usuarios de banca electrónica y las instituciones del sistema financiero entre otros Internet, Telefonía, etc.

La Comisión o CNBS: Comisión Nacional de Bancos y Seguros.

COBIT. (Control Objetives for Information and Related Technology) mejor práctica aplicada en materia de control y seguridad de TI emitido por ISACA (Information Systems Audit and Control Foundation)

Confidencialidad. Protección de datos personales o Información clasificada como confidencial en términos de las Políticas de Seguridad de la Información, por lo cual su divulgación no está autorizada.

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

Número Piloto: 2232-4036
2232-5613
Técnico Financiero: 2232-5269
Fax Secretaría: 2232-4651
Tesorería: 2239-0776
Apartado Postal No. 92
Comayagüela, M.D.C.

Control. Políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para procurar que los objetivos del negocio sean alcanzados y que los riesgos detectados sean prevenidos, detectados o corregidos.

Contraseña Segura o Fuerte: Contraseñas de uso informático que deben cumplir con las especificaciones de la política de contraseñas de la institución y que sean difíciles o casi imposibles de adivinar o hurtar.

Discontinuidad de Servicio Significativo: Incapacidad de continuar prestando los servicios definidos como críticos por la Alta Dirección, y sin los cuales se vería seriamente afectada la continuidad para los afiliados.

Disponibilidad. Acceso y utilización de la Información y los sistemas cuando se requieran.

Dueño de Proceso. Gerente responsable del diseño, aprobación e implementación de un proceso y subproceso específico en su área de responsabilidad.

Evento. Es algo que sucede en un lugar y tiempo particular.

Hardware. Componentes físicos de un sistema computacional.

Hash: Cadena de caracteres generada por un algoritmo de encriptación, el cual proporciona un valor estadísticamente único para un conjunto de datos de entrada. Bajo esta técnica se comprobará la validez de los datos recibidos o, como en el caso de las contraseñas, cifrar una información en un sólo sentido.

Indicador. Definición de datos que ayudan a medir objetivamente la evolución de una actividad o una tarea, así como la efectividad de un control para mitigar un riesgo.

Información. Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.

Integridad. Mantenimiento de la exactitud y completitud de la Información y sus métodos de proceso.

Instituto. Instituto Nacional de Previsión del Magisterio

ISO /IEC 27001. Estándar para la seguridad de la Información publicado como por International Organization for Standardization (ISO) y por la International Electrotechnical Commission (IEC).

Localizador Uniforme de Recursos (URL): Cadena de caracteres con la cual se asigna dirección única a cada uno de los recursos de información disponibles en Internet. Existe un URL único para cada página de cada uno de los documentos en Internet.

Memoria Caché: Memoria a la que una computadora puede acceder más rápidamente que a la memoria normal de la computadora (Memoria RAM), la computadora primero busca información en la memoria caché y luego en la RAM.

No Repudio: Cualidad o característica de una determinada comunicación, a través de la cual se protege a las partes de la comunicación frente a la negación de que dicha comunicación haya ocurrido. Existe no repudio cuando se produce el efecto legal o práctico de dicho atributo o característica.

Pared de Fuego (Firewall): Dispositivos de Seguridad (Hardware o software) utilizados para restringir el acceso en un ambiente de redes informáticas interconectadas, que permiten el acceso a ciertos servicios previamente definidos.

Penetración Significativa: Ataques a una red informática que alteren la disponibilidad, integridad y confidencialidad de la información sensitiva de la institución.

Procedimientos Almacenados (Stored Procedure): Conjunto de instrucciones u órdenes precompiladas, escritas en un lenguaje propietario como PL/SQL para Oracle database oPL/PgSQL para PostgreSQL, que pueden ser llamados usando el nombre que se les haya asignado. Son esencialmente cajas negras.

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

Número Piloto: 2232-4036
2232-5613
Técnico Financiero: 2232-5269
Fax Secretaría: 2232-4651
Tesorería: 2239-0776
Apartado Postal No. 92
Comayagüela, M.D.C.

Red de Producción: Red que está compuesta por computadoras, servidores, archivos, bases de datos, equipos de comunicación, dispositivos de seguridad, etc., que contienen y transmiten datos reales y oficiales de una institución.

Riesgo. Es la exposición a la posibilidad de ocurrencia de eventos tales como pérdida o ganancia económica, daño físico, retrasos, etc., que surgen como consecuencia de seguir un curso particular de acción. El concepto de riesgo tiene dos elementos: la probabilidad de que algo ocurra y las consecuencias de si esto ocurre (impacto o severidad).

Riesgo Operativo. Es aquel que puede provocar pérdidas directas o indirectas como resultado de errores humanos, procesos internos inadecuados o defectuosos, controles internos inadecuados, fallas en los sistemas y a consecuencia de acontecimientos externos originados dentro de la propia operación del Instituto.

Riesgo residual. El riesgo asociado con un evento después de que un control se está llevando a cabo.

Riesgo Tecnológico. El Riesgo Tecnológico es la pérdida potencial por daños, interrupción, alteración o fallas derivadas del uso o dependencia en el hardware, software, sistemas, aplicaciones, redes y cualquier otro canal de distribución de Información que el Instituto dispone para prestar sus servicios.

Seguridad. Actividades encaminadas a preservar la confidencialidad, integridad y disponibilidad de la Información, así como los sistemas implicados en su tratamiento.

Software. Es un conjunto de programas, documentos, procedimientos y rutinas asociadas con la operación de un sistema computacional.

Servidor: Computadora que presta servicios de red a los usuarios de la misma. Estos servicios pueden ser bases de datos, impresión, antivirus, correo electrónico, aplicaciones, etc.

Sesión: Es el periodo de tiempo transcurrido desde que un usuario o un equipo informático inicia conexión, con otro equipo previa presentación de credenciales, hasta el momento que la conexión finaliza.

Sistema de Detección de Intrusos (IDS): Dispositivo o programa de cómputo que, de acuerdo a una base de datos, detecta patrones que son conocidos mundialmente como ataques o intentos de intrusión a redes y computadoras, enviando alertas y presentando reportes.

Tecnologías de Información y Comunicaciones (TIC): Recursos tecnológicos usados para crear, almacenar, intercambiar y usar información en sus diferentes formatos (datos, voz, imágenes, videos, presentaciones, etc.)

Tercerización (Outsourcing): Contrato mediante el cual una compañía provee servicios a otra. Estos servicios podrían ser provistos dentro de la misma institución.

Tercerización Significativa: Tercerización de servicios que son de carácter vital para una compañía, ya que si estos servicios fallan provocarían un impacto en la continuidad del negocio.

Valor SALT: Valor generado al azar, que es usado para modificar el hash de una contraseña, el cual previene las colisiones de contraseñas, es decir si más de un usuario selecciona la misma contraseña, la cadena de caracteres generada utilizando un valor SALT será diferente.

Vulnerabilidad. Debilidades o defectos en la infraestructura de seguridad de una organización

5. ASPECTOS NORMATIVOS

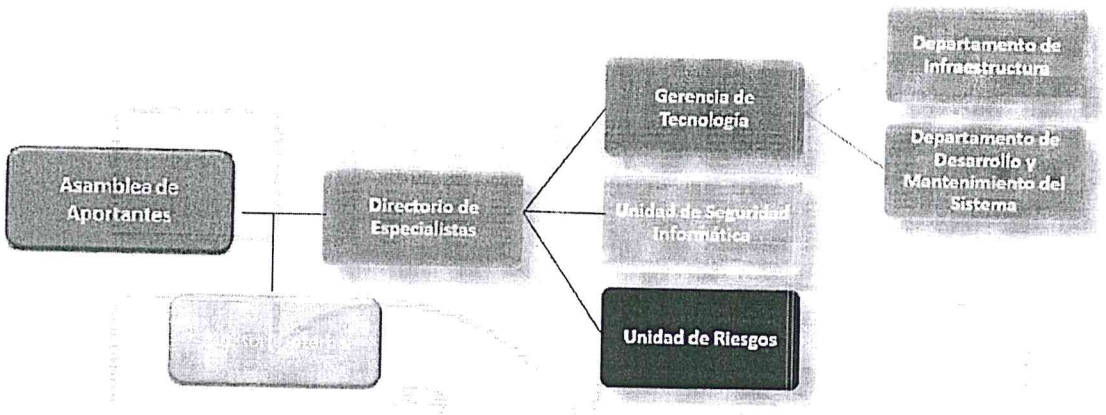
A. Ley del INPREMA
B. Resolución 1301/22-11-2005 "NORMAS PARA REGULAR LA ADMINISTRACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES EN LAS INSTITUCIONES DEL SISTEMA FINANCIERO",
C. Capítulo IV, Normas Generales Relativas a la Evaluación y Gestión de riesgos, Acuerdo Administrativo TSC No. 001/2009
D. Ley de Transparencia y Acceso a la Información Pública

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

Número Piloto: 2232-4036
2232-5613
Técnico Financiero: 2232-5269
Fax Secretaría: 2232-4651
Tesorería: 2239-0776
Apartado Postal No. 92
Comayagüela, M.D.C.

E. Normas contables, contraloras, nacionales e internacionales vigentes en lo que aplique a los sistemas de información, Ejemplo: NIIF, NICS, Resoluciones de la CNBS, BCH, SEFIN, ONADICI, TSC, etc.
F. Normas Generales de Control Interno emitidas por el TSC y ONADICI.
G. Manual de Administración Integral de Riesgos.

6.ORGANIZACIÓN DEL INSTITUTO



7. FUNCIONES Y RESPONSABILIDADES

Alta Administración

1. El Directorio deberá tener como mínimo una reunión anual para establecer o revisar las políticas y procedimientos sobre la administración tecnológica y seguridad de la información, que conlleven a la correcta toma de decisiones
2. El Directorio deberá nombrar a un Administrador de Seguridad Informática, el cual deberá estar subordinado a la máxima autoridad del Instituto.
3. Revisar y aprobar políticas y manuales desarrollados para administrar el riesgo tecnológico del instituto.
4. Conocer los reportes que le remita el Comité de Riesgos sobre el nivel de exposición al riesgo tecnológico, así como, medidas correctivas adoptadas.
5. Conocer sobre el nivel de cumplimiento de políticas y procedimientos aprobados.

Área de Tecnología

1. Identificar y evaluar los riesgos tecnológicos inherentes a sus procesos.
2. Determinar las causas y efectos derivados de los riesgos identificados.
3. Reportar la incidencia de eventos derivados de un riesgo tecnológico en cada área del Instituto.
4. Participar en las sesiones de medición y cuantificación del riesgo tecnológico.
5. Elaborar, establecer y dar mantenimiento a las políticas y procedimientos que afecten a su área.
6. Proporcionar Información relacionada con el seguimiento en las acciones referentes a las respuestas de riesgos tecnológicos.
7. Proporcionar la Información relacionada a cada uno de los indicadores de los riesgos tecnológicos identificados.

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

Número Piloto: 2232-4036
2232-5613
Técnico Financiero: 2232-5269
Fax Secretaría: 2232-4651
Tesorería: 2239-0776
Apartado Postal No. 92
Comayagüela, M.D.C.

8. Mantener una estrecha comunicación en su área, así como con la Unidad Riesgos de cualquier índole en relación al riesgo tecnológico que contribuya a una mejora continua.
9. Comunicar la necesidad de hacer un análisis de riesgos cuando se actualice, modifique o desarrolle un proceso.
10. Contar con un manual de puestos que deberá incluir los perfiles de puestos y la segregación de funciones y de autoridad.
11. Estructurar un programa de capacitación de acuerdo con las prioridades de la administración, que permita maximizar las contribuciones que brinde el personal del área. Esta capacitación debe incluirse en el presupuesto anual y ser consistente con los requerimientos mínimos de la organización.

Área de Seguridad Informática

1. Proponer al Instituto las políticas, normas y procedimientos de seguridad informática.
2. Documentar e implementar las políticas, normas y procedimientos de seguridad informática aprobadas por la Junta o Consejo.
3. Verificar que los usuarios de los distintos sistemas y recursos tecnológicos cumplan con las políticas, normas y procedimientos aprobados.
4. Tomar las acciones correctivas que garanticen la seguridad informática requerida, una vez que se hayan identificado violaciones.
5. Identificar e implementar herramientas de seguridad informática que aseguren que la información y el equipamiento, no sean utilizados en perjuicio de la institución y los usuarios.
6. Controlar el uso indebido de programas (utilitarios) o herramientas que permiten la manipulación de los datos en los diferentes sistemas.
7. Desarrollar por lo menos una vez al año, evaluaciones de seguridad a las tecnologías de información y comunicaciones de la institución.
8. Identificar y evaluar los riesgos de seguridad de la información inherentes a sus procesos.
9. Determinar las causas y efectos derivados de los riesgos identificados.
10. Reportar la incidencia de eventos derivados de un riesgo de seguridad informática en cada área del instituto.
11. Participar en las sesiones de medición y cuantificación del riesgo de seguridad informática.
12. Elaborar, establecer y dar mantenimiento a las políticas y procedimientos que afecten a su área.
13. Proporcionar Información relacionada con el seguimiento en las acciones referentes a las respuestas de riesgos de seguridad informática.
14. Proporcionar la información relacionada a cada uno de los Indicadores de los riesgos identificados.
15. Mantener una estrecha comunicación en su área, así como con la Unidad Riesgos de cualquier índole en relación al riesgo, que contribuya a una mejora continua.
16. Comunicar la necesidad de hacer un análisis de riesgos cuando se actualice, modifique o desarrolle un proceso.
17. Contar con un manual de puestos que deberá incluir los perfiles de puestos y la segregación de funciones y de autoridad.
18. Estructurar un programa de capacitación de acuerdo con las prioridades de la administración, que permita maximizar las contribuciones que brinde el personal del área. Esta capacitación debe incluirse en el presupuesto anual y ser consistente con los requerimientos mínimos de la organización.

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

Número Piloto: 2232-4036
2232-5613
Técnico Financiero: 2232-5269
Fax Secretaría: 2232-4651
Tesorería: 2239-0776
Apartado Postal No. 92
Comayagüela, M.D.C.

Unidad de Auditoria

1. La Auditoría Interna de la institución deberá auditar la Tecnología de Información y Comunicación (TIC) a fin de verificar: la integridad, disponibilidad y confidencialidad de la información. La persona(s) encargada(s) de auditar las TIC deberá contar con experiencia y entrenamiento calificado para llevar a cabo este tipo de auditorías basadas en las mejores prácticas existentes en el mercado tales como COBIT e ISO-17799.
2. La institución deberá proveerle a la Auditoría Interna las herramientas necesarias para la realización y control del ambiente de la TIC y la SI.
3. El Auditor Interno será responsable de que, aun en el caso de que la Auditoría de Sistemas sea llevada a cabo por medio de la Tercerización (outsourcing) se cumplan las disposiciones contenidas en las Normas Mínimas para el Funcionamiento de las Unidades de Auditoría Interna de las Instituciones del Sistema Financiero y en las presentes normas.

Unidad de Procesos

1. Establecer y administrar la metodología para la documentación de procesos y subprocesos de acuerdo a las mejores prácticas, asegurando la consistencia operativa.
2. Asesorar y proporcionar las herramientas necesarias a todas las áreas del Instituto para la documentación de los procesos y subprocesos que describen el quehacer de cada área del Instituto, cuando se trate de una actualización, modificación o desarrollo de un nuevo proceso de acuerdo a la Metodología para la definición y documentación de los Modelos de Operación.

Unidad de Riesgos

1. Proponer el marco de gestión del Riesgo Tecnológico, así como, las políticas y procedimientos para la identificación, evaluación y control, así como, la implantación de métodos cualitativos y cuantitativos que permitan permear una cultura de riesgos en el Instituto.
2. Definir el alcance de la identificación y evaluación de riesgos.
3. Coordinar con los responsables de los procesos y/o subprocesos el cumplimiento del presente Manual, de forma que se complementen los lineamientos en materia de Control Interno.
4. Informar al menos de manera bimestral a través del reporte de riesgos, acerca de las exposiciones, incidencias y comportamiento de indicadores relativos al riesgo tecnológico al Comité de Riesgos y al Directorio.
5. Revisar y actualizar el Manual de Administración de Riesgo Tecnológico, cuando menos, una vez al año y/o cuando por cambios, el Instituto lo requiera.
6. Capacitar al Dueño de Proceso, cuando lo requiera, para identificar y evaluar los riesgos tecnológicos inherentes de acuerdo al presente manual.
7. Apoyar a los responsables facultados, del tratamiento de los riesgos a desarrollar (remediar, monitorear u optimizar el control).
8. Seguimiento y retroalimentación de las respuestas de riesgo.
9. Análisis de desviaciones en Riesgo Tecnológico.
10. Definir y monitorear los Indicadores por Riesgo Tecnológico.
11. Actualizar al menos una vez al mes la base de datos por riesgo tecnológico, a través del registro de incidencias que se tengan por conocimiento de las diferentes fuentes de Información y en su caso verificar que el monto de pérdida esté reflejado dentro de la contabilidad del Instituto.

8. POLÍTICAS

El área de **Tecnología** del Instituto cuenta con las siguientes políticas:

1. De la administración de redes y conexiones
2. Del monitoreo de servidores y equipos
3. Del monitoreo de servidores AS400
4. Del traslado de objetos al ambiente de producción del sistema
5. Del soporte técnico programado

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

Número Piloto: 2232-4036
2232-5613
Técnico Financiero: 2232-5269
Fax Secretaría: 2232-4651
Tesorería: 2239-0776
Apartado Postal No. 92
Comayagüela, M.D.C.

6. Del soporte técnico correctivo

El área de **Seguridad informática** cuenta con las siguientes políticas:

1. De los usuarios
2. Seguridad de información sensible
3. Uso de las estaciones de trabajo
4. Usuarios y contraseñas
5. Uso de antivirus
6. Administración y uso del correo electrónico
7. Uso del internet
8. Uso de dispositivos de almacenamiento externo
9. Adquisición de hardware y software
10. Dispositivos móviles
11. Contratación de consultores de servicios tecnológicos

9. METODOLOGÍA

La administración de riesgos del Instituto es el proceso en el que se identifican sistemáticamente, se evalúan y controlan los eventos no deseados que pueden ocasionar un cambio tecnológico considerando lo siguiente:

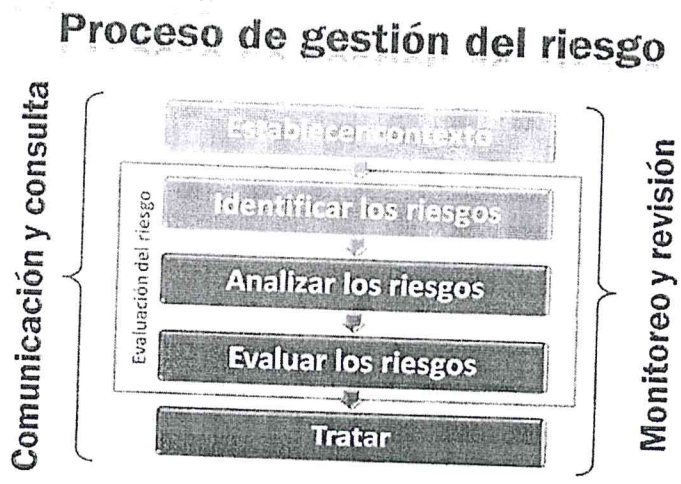
- Tiene que haber un cambio en el entendimiento de los procesos y sistematización del análisis de dependencias y riesgos de tecnología de Información.
- Continuamente se está en una nueva era de peligros, regulaciones y oportunidades.
- Se requiere detectar los riesgos actuales, permitiendo conocer las amenazas y debilidades y convertirlas en oportunidades y fortalezas.
- El no detectar el riesgo no implica que no exista.

La metodología de gestión de riesgos del INPREMA estará basada en tres marcos de referencia como ser: Norma de la Comisión Nacional de Bancos y Seguros para las Tecnologías de la Información y el estándar AS/NZS 4360:1999 Estándar Australiano (hoy ISO 31000), que apoya la gestión de riesgo en general incluido el Operativo/Tecnológico.

ISO 31000 y el Proceso General de gestión de riesgos

El proceso de gestión integral del riesgo debe cumplir con una serie de características que lo fortalecen:

- Debe formar parte integral de la gestión.
- Debe estar acomodado en la cultura y prácticas de la organización.
- Debe estar adaptado a los procesos de negocio de la organización.



La metodología de administración de **Riesgo Tecnológico** del Instituto está basada principalmente en dos marcos de referencia generalmente aplicable y aceptado: el primero de ellos es COBIT

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

Número Piloto: 2232-4036
2232-5613
Técnico Financiero: 2232-5269
Fax Secretaría: 2232-4651
Tesorería: 2239-0776
Apartado Postal No. 92
Comayagüela, M.D.C.

(Control Objetives for Information and Related Technology – Objetivos de Control para la Información y las Tecnologías) mejor práctica aplicada en materia de control y gobernabilidad de TI emitido por ISACA (Information Systems Audit. and Control Foundation) y el segundo es ISO/IEC 27001que es el estándar para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información y es emitido conjuntamente por ISO (Organización Internacional por la Normalización y la IEC (International Electrotechnical Commission).

1º. COBIT

El uso del marco de trabajo COBIT para la administración de riesgos, se basa en el principio de proporcionar la Información que el Instituto requiere para lograr sus objetivos, su necesidad de administrar y controlar los recursos de TI y sus riesgos relacionados, usando un conjunto estructurado de procesos que ofrezcan los servicios requeridos de Información.

Es un conjunto de "mejores prácticas" que persiguen optimizar la alineación estratégica y operativa de las TI con el negocio de cada organización o empresa. Las TI deben maximizar el valor que los procesos de negocio aportan a la organización.

Dicho marco de trabajo debe documentar un nivel común y acordado de riesgos TI, estrategias para mitigarlos y riesgos que se acuerden aceptar como residuales. Cualquier riesgo potencial sobre las metas u objetivos de la organización, causado por algún evento no planificado, se tiene que identificar, analizar y evaluar.

El modelo de referencia COBIT se encuentra estructurado en:

1. **Requerimientos de Información**

Efectividad. Se refiere a que la Información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.

Eficiencia. Se refiere a la provisión de Información a través de la utilización óptima (más productiva y económica) de recursos.

Confidencialidad. Se refiere a la protección de Información sensible contra divulgación no autorizada.

Integridad. Se refiere a la precisión y suficiencia de la Información, así como a su validez de acuerdo con los valores y expectativas de la organización.

Disponibilidad. Se refiere a la disponibilidad de la Información cuando ésta es requerida. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

Cumplimiento. Se refiere al ejercicio de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocio está sujeto.

Confiabilidad. Se refiere a la provisión de Información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y cumplimiento.

2. **Recursos de TI**

Aplicaciones. Incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan Información.

Información. Son los datos en todas sus formas de entrada, procesados y generados por los sistemas de Información, en cualquier forma en que son utilizados por el negocio.

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

Número Piloto: 2232-4036
2232-5613
Técnico Financiero: 2232-5269
Fax Secretaría: 2232-4651
Tesorería: 2239-0776
Apartado Postal No. 92
Comayagüela, M.D.C.

Infraestructura. Es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.

Gente. Es el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de Información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.

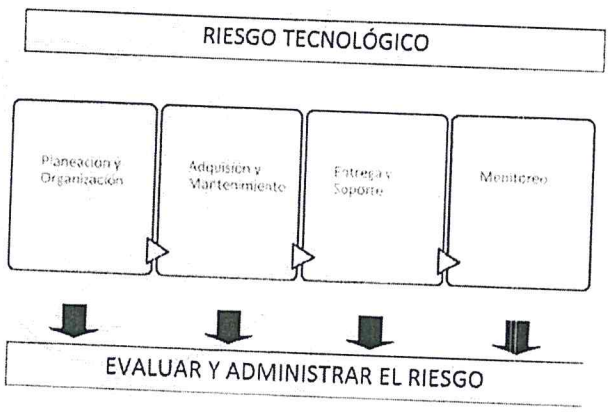
3. Procesos de TI

- Dominios
- Procesos
- Actividades

COBIT está formado por objetivos de control, los cuales se encuentran asociados a riesgos por el hecho de apoyarse de tecnología de Información para la operación del Instituto.

Las actividades que buscan mitigar los riesgos se encuentran divididas en 4 grandes dominios:

- Planeación y Organización (PO)
- Adquisición e Implementación (AI)
- Entrega y Soporte (DS)
- Monitoreo (ME)



Tratamiento de los riesgos en COBIT

En el proceso PO 9. **-Planificar y Organizar-. Evaluar y Administrar los riesgos de TI:**

Se establecen los principios que deben tenerse en cuenta para la gestión de los riesgos. Se establece que debe crearse y mantenerse un marco adecuado de trabajo para la gestión de riesgos.

Dicho marco de trabajo debe documentar un nivel común y acordado de riesgos TI, estrategias para mitigarlos y riesgos que se acuerden aceptar como residuales. Cualquier riesgo potencial sobre las metas u objetivos de la organización, causado por algún evento no planificado, se tiene que identificar, analizar y evaluar.

Objetivos de control detallados correspondientes al proceso PO 9

PO 9.1.- **Alineación de la administración o gestión de riesgos de TI con el negocio.** Se debe integrar el gobierno, la administración del riesgo y el marco del control de TI, al marco de trabajo de la administración de riesgos de la organización.

PO 9.2.- **Establecimiento del contexto del riesgo.** Se debe establecer el contexto en el cual el marco de trabajo de la evaluación de riesgo se aplica para garantizar los resultados apropiados.

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

Número Piloto: 2232-4036
2232-5613
Técnico Financiero: 2232-5269
Fax Secretaría: 2232-4651
Tesorería: 2239-0776
Apartado Postal No. 92
Comayagüela, M.D.C.

PO 9.3.- **Evaluación de eventos.** Identificar aquellos eventos (amenazas y vulnerabilidades) con un impacto potencial sobre objetivos, retos u operaciones de la empresa, aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operaciones.

PO 9.4.- **Evaluación de riesgos TI.** Se debe evaluar de forma recurrente la posibilidad de impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos.

PO 9.5.- **Respuesta a los riesgos.** Debemos identificar a los propietarios de los riesgos y a los dueños de los procesos afectados y elaborar y mantener respuestas a los riesgos que garanticen que los controles rentables y las medidas de seguridad mitigan y reducen la exposición a los riesgos de forma continua.

PO 9.6.- **Mantenimiento y monitoreo de un plan de acción de riesgos.** Debemos asignar prioridades y planear las actividades de control a todos los niveles para implantar las respuestas a los riesgos que sean necesarias, incluyendo costos y beneficios, así como la responsabilidad de la ejecución.

Es un principio generalmente aceptado que hoy en día ninguna organización puede sobrevivir (mucho menos triunfar) sin las TIC. Los sistemas de información deben:

1. Mantener la alineación con la estrategia de la organización.
2. Entregar valor.
3. Administrar o gestionar los riesgos.
4. Administrar los recursos.
5. Medir el rendimiento/desempeño.

Todos estos conceptos se encuentran en el gobierno de TI, según COBIT.

Otros procesos COBIT sobre gestión de los riesgos TI

En el DS5 - Asegurar la Seguridad de los Sistemas (dentro del área de procesos Entrega y Soporte (DS)), se incluyen:

1.- Gestión de la Seguridad TI.
2.- Plan de Seguridad TI.
3.- Gestión de la identidad.
4.- Gestión de la cuenta del usuario.
5.- Pruebas de seguridad, vigilancia y monitorización.
6.- Definición de Incidente de Seguridad.
7.- Protección de la Tecnología de Seguridad.
8.- Gestión de la clave criptográfica.

En el área de procesos de Mantener y Evaluar (ME) en el proceso ME4. - Suministrar Gobierno de TI existe el proceso Gestión del Riesgo.

Como vemos COBIT nos ofrece una enorme ayuda al implantar la gestión en general de las TI al servicio del negocio y en particular una excepcional ayuda al planificar y desplegar una adecuada gestión de los riesgos de TI.

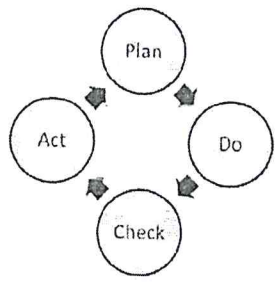
2º. ISO/IEC 27001

Es un estándar ISO (Organización Internacional por la Normalización) /IEC27001 (International Electrotechnical Commission) para la administración de los riesgos de seguridad de la información, reforzando la protección de los sistemas y redes de Información en base a políticas, procedimientos y acciones necesarias para afrontar tales riesgos y así garantizar la disponibilidad, confidencialidad e integridad de la Información.

La norma ISO/IEC 27001 se encuentra basada en el ciclo PDCA (Plan, Do, Check, Act):

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

Número Piloto: 2232-4036
2232-5613
Técnico Financiero: 2232-5269
Fax Secretaría: 2232-4651
Tesorería: 2239-0776
Apartado Postal No. 92
Comayagüela, M.D.C.



1.- Plan (Planear) - Establecer que hacer y cómo para satisfacer la política y objetivos de seguridad de la Información.

2.- Do (Hacer) – Poner en práctica lo planeado.

3.- Check (Checar) - Verificar si se ha hecho lo planificado y si lo que se ha hecho es eficiente.

4.- Act (Actuar) – Establecer las acciones de cómo y que mejorar.

Así mismo la norma indica los objetivos de control que se deben tener como mejor práctica en cuestión de seguridad de la información, divididos de la siguiente forma:

1- Política de Seguridad

- Organización de la Seguridad de la Información Administración de Activos.
- Seguridad de Recursos Humanos Seguridad física y ambiental.
- Administración de comunicaciones y operaciones. Control de acceso.
- Adquisición, mantenimiento y desarrollo de sistemas de Información.
  Administración de los incidentes de seguridad de la Información.
- Administración de la continuidad de negocio. Cumplimiento.

2- Definición del alcance

El primer paso es definir el alcance para determinar los límites de la evaluación, los recursos y la Información existente.

La definición del alcance del análisis de riesgos se realiza considerando:

- Los objetivos estratégicos del Instituto y sus políticas.
- Los procesos de negocio Institucionales.
- Las funciones y estructura organizacional.
- Requerimientos legales, contractuales y normativos.
- La política de seguridad institucional.
- El enfoque general institucional para la valoración del riesgo.
- Los activos de Información críticos.
- Recursos disponibles (financieros, humanos).

3- Criterios de evaluación, impacto y aceptación de riesgos

Previo a la Identificación es necesario establecer los criterios de evaluación, criterios de impacto y de aceptación del riesgo. Dichos criterios serán establecidos considerando lo siguiente:

a. **Criterios de evaluación**

- La criticidad del activo de Información involucrado.
- Requerimientos legales, regulatorios y contractuales.
- Importancia en la operación y en el negocio de la disponibilidad, confidencialidad y disponibilidad.
- Expectativas y percepciones de las partes interesadas y consecuencias negativas sobre la imagen y reputación.

b. **Criterios de impacto**

Niveles de clasificación de los activos de Información impactados. (magnitud del impacto)

Brechas en la seguridad de la Información (impacto a la confidencialidad, integridad y disponibilidad).

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

Número Piloto: 2232-4036
2232-5613
Técnico Financiero: 2232-5269
Fax Secretaría: 2232-4651
Tesorería: 2239-0776
Apartado Postal No. 92
Comayagüela, M.D.C.

- Problemas en la operación.
- Pérdida del valor del negocio o financieras.
- Alteración de planes o fechas de entrega.
- Brechas legales, regulatorias o requerimientos contractuales.

c. **Criterio de aceptación del riesgo**

- Criterios del negocio.
- Aspectos legales, regulatorios y legales.
- Operaciones.
- Tecnología.
- Finanzas.
- Factores Sociales.

4- Identificación de riesgos

El levantamiento de riesgos se basa en la aplicación de cuestionarios y entrevistas, revisión de documentos del Instituto, reportes de auditoría o análisis previos.

Así mismo es importante remarcar que al utilizar como marcos de referencia COBIT e ISO/IEC 27001 también se cubrirán los riesgos tecnológicos relacionados en sus objetivos de control que sean aplicables al Instituto.

Identificar dentro de la gestión de Riesgo Tecnológico, consiste en ubicar los activos a evaluar y determinar sus amenazas y vulnerabilidades.

Así al tener identificados los activos, amenazas y vulnerabilidades llegamos a lo que es un riesgo tecnológico el cual se define como el potencial de que, dada una amenaza, explote una vulnerabilidad en un activo o grupo de activos para causar pérdidas o daños a esos activos.

La identificación de riesgos se apoya del formato **"Identificación y valuación de Riesgos" (Ver Anexo A)** el cual se utilizará para documentar las exposiciones del Instituto.

1. Identificación de Activos

Se denominan activos, a los recursos de Tecnología de Información necesarios para que el Instituto funcione correctamente.

El activo esencial es la Información que maneja el sistema, y alrededor de estos datos se pueden identificar otros activos relevantes como:

- Los servicios que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
- Las aplicaciones informáticas (Software) que permiten manejar los datos.
- Los equipos informáticos (Hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Interfaces entre los sistemas.
- Dispositivos de almacenamiento de datos.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones donde residen los equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.

Los activos identificados deben ser documentados en un inventario, para lo cual el registro es apoyado por el **"Inventario de activos" (Ver Anexo B)**.

2. Identificación de Amenazas

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

Número Piloto: 2232-4036
2232-5613
Técnico Financiero: 2232-5269
Fax Secretaría: 2232-4651
Tesorería: 2239-0776
Apartado Postal No. 92
Comayagüela, M.D.C.

El siguiente paso, consiste en determinar las amenazas que pueden afectar a cada activo y obtener un extracto de las amenazas potenciales, las cuales son aplicables para la tecnología que estamos evaluando.

Una amenaza, es un agente o circunstancia capaz de explotar accidentalmente o intencionalmente una vulnerabilidad. No todas las amenazas afectan a todos los activos, sin embargo, existe cierta relación entre el tipo de activo y lo que le podría ocurrir.

Es importante considerar todas aquellas fuentes de amenaza que pueden causar daño tecnológico, como pueden ser:

- **Naturales**: Inundación, terremotos, tornados, huracanes, derrumbes, tormentas eléctricas, etc.

- **Humanas**: Acontecimientos causados por seres humanos sin intención (entrada incorrecta de datos) o acciones deliberadas (ataques contra la seguridad, infección de virus, acceso no autorizado a Información confidencial)

- **Ambientales:** Contaminación, apagones, entre otros.

La motivación y los recursos para realizar un ataque hacen a los seres humanos potencialmente peligrosos y existen diferentes tipos como son:

- Criminales computacionales
- Espionaje industrial
- Personas que pertenecen a la organización

3. Identificación de vulnerabilidades

Consiste en determinar las vulnerabilidades que pueden ser explotadas por las amenazas y recopilar la Información necesaria que permita la identificación de las vulnerabilidades que son aplicables para la tecnología que estamos evaluando.

Una vulnerabilidad es un defecto o una debilidad en procedimientos de seguridad, deficiencia en diseño o implementación de controles internos que podrían ser explotados y que resulte en una apertura de la seguridad.

La identificación de vulnerabilidades puede ser principalmente:

- Desarrollar una lista de requerimientos de seguridad
- Realizar pruebas de seguridad de los sistemas
- Preguntarse qué puede pasar si el evento ocurre

4. Evaluación de riesgos

La evaluación de riesgos se basa en la medición del impacto y la probabilidad que se determinan en función de escenarios o criterios de categorización; es decir, clasificar el riesgo según su grado de afectación y estimación de la periodicidad de ocurrencia dentro de un proceso para un área. Es una medición subjetiva dado a que se especifica con base a la experiencia y sensibilidad que tenga el responsable del proceso en su área por lo que no es un método totalmente acertado.

Para trabajar bajo este enfoque cualitativo, se toma como herramienta la autoevaluación que consiste en identificar los riesgos a través del mapeo de procesos, evaluación de control existente, determinación de puntos de mejora que se debe realizar y definición de Indicadores.

La finalidad del enfoque cualitativo, permite detectar fortalezas y debilidades del ambiente tecnológico y sus potenciales riesgos a los que el Instituto está expuesto.

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

Número Piloto: 2232-4036
2232-5613
Técnico Financiero: 2232-5269
Fax Secretaría: 2232-4651
Tesorería: 2239-0776
Apartado Postal No. 92
Comayagüela, M.D.C.

5. Clasificación de la Información

La gestión de la seguridad de la información con la norma ISO 27001 para algunas organizaciones es muy importante a la hora de realizar la clasificación de la información.

Es una de las principales tareas que se realizan en dicho ámbito desde que se tiene constancia de ello. Para clasificar la información según la norma ISO 27001, existen diferentes criterios en los que basarnos. El criterio más utilizado por las empresas es el basado en el carácter confidencial de la información.

Para una correcta gestión de la información podemos usar un proceso que consta de cuatro pasos y que nos ayudará a proteger este activo.

10. PROCESO DE CLASIFICACIÓN DE LA INFORMACIÓN ISO 27001

Para realizar una buena gestión de la información que se tiene que clasificar es necesario que se lleve a cabo el siguiente proceso. Cada empresa, en su política de clasificación de la información, describe cómo llevar a cabo cada una de las etapas de este proceso de cuatro pasos:

Paso 1 Incluir la información en el Inventario de Activos

Según esta etapa, es necesario conocer a la perfección de qué tipo de información disponemos, así como quién es el responsable de la misma.

La información clasificada podemos tenerla en distintos formatos y medios, por ejemplo:

- Los documentos de carácter electrónico.
- Bases de datos.
- Documentos en formato papel.
- Correos electrónicos.
- Medios de almacenamiento.
- Información verbal.

Paso 2 Proceder a la clasificación de la anterior información

La norma ISO 27001 no establece cuales son los niveles de clasificación concretos, sino que cada empresa, en base a sus criterios particulares y las generalidades de las características de su industria tiene que definir sus criterios de clasificación concretos.

Una empresa establece más niveles de clasificación a medida que la misma sea de mayor tamaño y presente una mayor complejidad.

El INPREMA utiliza diversidad de activos de información para la ejecución de sus operaciones, la clasificación de dichos activos se regirá bajo la siguiente clasificación:

- **Confidencial**: cuando el nivel de confidencialidad de la información se incremente.
- **Restringido**: para niveles medios de confidencialidad.
- **Uso interno**: información con un nivel bajo de confidencialidad.
- **Público**: cuando todas las personas pueden ver la información.

El propietario del activo, es la persona encargada de proceder a realizar la clasificación de la información, por lo que se realizará según los resultados obtenidos tras la evaluación del riesgo.

Paso 3 Asignar una etiqueta a la información, una vez haya sido clasificada

Realizada la anterior clasificación de la información, se tiene que etiquetar de forma adecuada.

Es necesario que se defina una serie de pautas a seguir para cada tipo de activo de información. Esto, igualmente es cuestión de cada empresa, la cual se hace responsable de definir sus propias reglas, dado que la norma ISO 27001 no es prescriptiva en este sentido.

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

Una empresa puede establecer las siguientes reglas para indicar el carácter confidencial en cada uno de los documentos en papel que posee: indicar en la esquina superior del lado derecho del documento concreto el nivel de confidencialidad atribuido al mismo y que aparezca en el frente de la portada y en la carpeta donde se archive tal documento.

11 PROCEDIMIENTO DE GESTIÓN DEL RIESGO TECNOLÓGICO

La administración de riesgos es un proceso definido y repetible, bajo el cual se desarrollan actividades en diferentes etapas, permitiendo establecer un análisis de riesgos para activos y procesos determinados bajo el enfoque tecnológico; para que se concreten las respuestas a éstos para su mitigación. Asimismo, se busca establecer o mejorar los controles, así como, la definición de indicadores para su monitoreo de acuerdo a las mejores prácticas de los marcos de referencia COBIT 4.1 e ISO/IEC 27001.

A continuación, se muestra el procedimiento cíclico de Administración de Riesgo Tecnológico:

1. La Unidad de Riesgos/Administrador de Seguridad Informática y Tecnología, determinan los procesos y activos a evaluar de acuerdo el manual normativo de riesgo tecnológico.

2. Una vez determinados los activos relacionados a los procesos a evaluar, La Unidad de Riesgos/Administrador de Seguridad Informática y Tecnología en conjunto con los dueños de los procesos a nivel medio (principalmente gerentes), realizan el levantamiento de los riesgos mediante cuestionarios o entrevistas identificando amenazas y vulnerabilidades tecnológicas estableciendo las causas, efectos y clasificación del riesgo.

3. Una vez detallada la matriz de riesgos, los dueños de los procesos evalúan los riesgos que afectan la operación de Tecnología de Información bajo un enfoque cualitativo de acuerdo a los parámetros establecidos de frecuencia e impacto.

4. La Unidad de Riesgos/Administrador de Seguridad Informática y Tecnología, con base a los resultados de la evaluación del riesgo inherente y el grado de implementación de los controles relacionados, obtiene los resultados del riesgo residual que sirve como base para poder priorizar los riesgos y de esta forma el Dueño de Proceso podrá desarrollar los planes de tratamiento del riesgo.

5. Los dueños del proceso implementan los planes de tratamiento del riesgo para establecer los controles necesarios para mitigar el riesgo, considerando las implicaciones en recursos y tiempo para poderlos efectuar.

6. La Unidad de Riesgos/Administrador de Seguridad Informática y Tecnología, define los indicadores relacionados con algunos riesgos que permitan monitorear la exposición que tiene el Instituto en dicha materia.

7. La Unidad de Riesgos/Administrador de Seguridad Informática y Tecnología registran en la base de datos las exposiciones e incidencias relacionadas con riesgo tecnológico.

8. La Unidad de Riesgos/Administrador de Seguridad Informática y Tecnología documentan los resultados obtenidos de la evaluación del riesgo tecnológico incorporando las incidencias ocurridas, así como el comportamiento de los Indicadores establecidos para comunicarlo al Comité de Riesgos y a las diferentes dependencias.

12. MATRIZ DE IDENTIFICACIÓN Y EVALUACIÓN

El riesgo es la posibilidad de que se produzca un hecho generador de pérdidas que afecten el valor económico de las instituciones. Es la probabilidad de sufrir una pérdida de valor económico o de obtener un resultado distinto (negativo) al objetivo esperado por una decisión o inversión. Los factores de riegos tienen dos tipos de fuentes:

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

Número Piloto: 2232-4036
2232-5613
Técnico Financiero: 2232-5269
Fax Secretaría: 2232-4651
Tesorería: 2239-0776
Apartado Postal No. 92
Comayagüela, M.D.C.

- **Exógenas**: son situaciones que se encuentran por fuera de la Institución y que pueden afectar los resultados organizacionales.
- **Endógenas**: son situaciones internas que ocurren en cualquier organización y que afectan los resultados planeados.

Para su evaluación se utilizará una matriz de evaluación y valoración de los riegos del proceso que se encuentra documentado, su estructura es:

1 MACROPROCESO	2 PROCESOS	3 FACTORES DE RIESGO	4 ORIGEN DEL RIESGO	5 POTENCIAL CONSECUENCIA	6 IMPACTO

7 PROBABILIDAD DE OCURRENCIA	8 NIVEL DE RIESGO INHERENTE	9 TIPO DE RIESGO	10 CONTROL DE RIESGO	11 EFECTIVIDAD	12 PROMEDIO	13 RIESGO NETO O RESIDUAL

Macroproceso: Identifica el nombre del macroproceso al que pertenece el proceso analizado.
Proceso: Contiene el nombre del Proceso analizado.

Factores de Riesgo: En esta columna se deben señalar todos los factores de riesgo identificados para cada proceso. Estos factores de riesgo pueden ser de naturaleza endógena o exógena.

Origen del Riesgo: En esta columna se deberá señalar el origen del factor de riesgo; señalando si es endógeno (todos aquellos factores que se generan dentro del INPREMA) o exógeno (todos aquellos factores que se generan por fuera del INPREMA pero que lo pueden afectar).

Potencial consecuencia: Definir las potenciales consecuencias que los factores de riesgo señalados podrían causar en los objetivos estratégicos de la institución o en el negocio en general.

Impacto: Categorizar el nivel de afectación que podría ocasionar el factor de riesgo en el proceso o en el negocio. La categorización podrá ser: ALTO, MEDIO, BAJO, con la siguiente escala:

3	Ato Impacto Pérdidas de gran magnitud que puede afectar la continuidad del negocio.
2	Impacto Medio Pérdidas que afectan la posición financiera de la institución pero que no ponen en riesgo la continuidad del negocio.
1	Bajo Impacto Pequeña pérdidas que se presentan por la presencia del factor de riesgo y que no afectan ni la posición financiera ni la continuidad.

Probabilidad de ocurrencia: Valorar la probabilidad de que se presente el factor de riesgo definido. La valorización de la probabilidad de ocurrencia podrá ser: ALTA, MEDIA, BAJA. Su escala de calificación es:

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

Número Piloto: 2232-4036
2232-5613
Técnico Financiero: 2232-5269
Fax Secretaría: 2232-4651
Tesorería: 2239-0776
Apartado Postal No. 92
Comayagüela, M.D.C.

3	**Alta probabilidad** Evento de riesgo que se puede presentar continuamente en un período de tiempo.
2	**Probabilidad Media** Evento de riesgo que se puede presentar eventualmente en un período de tiempo.
1	**Baja probabilidad** Evento de riesgo que se podría presentar en un intervalo largo de tiempo.

Nivel de Riego Inherente: Obtiene una puntuación del riesgo inherente en una escala de 5 puntos, que cuantifica el riesgo propio de la actividad sin tomar en cuenta la efectividad de las actividades realizadas para su minimización.

5	**Riesgo Crítico** Riesgo que tiene alta probabilidad de ocurrencia y su impacto financiero puede poner en riesgo la continuidad del negocio.
4	**Riesgo Alto** Riesgo que tiene alta probabilidad de ocurrencia y su impacto financiero no pone en riesgo la continuidad del negocio; o, Riego con probabilidad de ocurrencia media y que su impacto financiero puede poner en riesgo la continuidad del negocio.
3	**Riesgo Moderado** Riego que tiene probabilidad media de ocurrencia y su impacto financiero no pone en riesgo la continuidad del negocio
2	**Riesgo Bajo** Riego con probabilidad de ocurrencia baja y que su impacto financiero no puede poner en riesgo la continuidad del negocio.
1	**Riesgo Muy bajo** Riesgo que tiene baja probabilidad de ocurrencia y su afectación financiera es mínima

13. PLAN DE CONTINUIDAD DE TECNOLOGÍA

El área de Tecnología tiene un plan de continuidad a efectos de poder levantar los servicios requeridos de su parte, para mitigar el riesgo de no poder brindar los servicios que los afiliados esperan del Instituto.

El Instituto deberá examinar y revisar su plan de contingencias atendiendo los cambios que han ocurrido desde la revisión anterior. Dicha revisión deberá realizarse como mínimo cada dos (2) años, así como cada vez que ocurran cambios significativos.

14. VIGENCIA

El presente manual entrará en vigencia una vez sea aprobado en Comité de Riesgos así como en Directorio, las modificaciones o actualizaciones futuras deberán contar con los mismos niveles de aprobación y deberán constar en Actas así como en Resoluciones.

ANEXO 1. MATRIZ DE IDENTIFICACIÓN Y EVALUCIÓN – INPREMA

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

Número Piloto: 2232-4036
2232-5613
Técnico Financiero: 2232-5269
Fax Secretaría: 2232-4651
Tesorería: 2239-0776
Apartado Postal No. 92
Comayagüela, M.D.C.

FACTORES DE RIESGO	ORIGEN DEL RIESGO	POTENCIAL CONSECUENCIA	IMPACTO	PROBABILIDAD DE OCURRENCIA	NIVEL DE RIESGO INHERENTE	TIPO DE RIESGO	CONTROL DE RIESGO	EFECTIVIDAD	PROMEDIO	RIESGO NETO O RESIDUAL
					0			#¡N/A	0.00	
					0			#¡N/A	0.00	
					0			#¡N/A	0.00	
					0			#¡N/A	0.00	
					0			#¡N/A	0.00	
					0			#¡N/A	0.00	

ANEXO No. 2 INVENTARIO DE ACTIVOS

No.	Activo de Información	Clasificación de la Información	Tipo de Archivo	Tipo de amenaza	Disponibilidad	Ubicación	Usuario	Gerencia

ANEXO C. MATRIZ DE IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

FACTORES DE RIESGO	ORIGEN DEL RIESGO	POTENCIAL CONSECUENCIA	IMPACTO	PROBABILIDAD DE OCURRENCIA	NIVEL DE RIESGO INHERENTE	TIPO DE RIESGO	CONTROL DE RIESGO	EFECTIVIDAD	PROMEDIO	RIESGO NETO O RESIDUAL
Que no se otorgue una contraseña de acceso de manera directa al responsable del usuario	Endógeno	Que se brinde acceso a usuarios no autorizados, modificaciones se realicen modificaciones a la información sin registro de la misma.	Alto	Bajo	2	Operacional	Comunicación directa con el responsable del usuario.	4 Alta efectividad. El nivel de control implementado reduce el impacto del riesgo pero no por completo	4.00	0.38
Que no se verifique la autorización de la Jefatura solicitante o la autorización del responsable directo de la cuenta de usuario.	Endógeno	Manipulación no autorizada de la información o aplicativos del sistema.	Alto	Bajo	2	Legal	Contacto directo de manera obligatoria con el responsable de un usuario que se preterita activar.	4 Alta efectividad. El nivel de control implementado reduce el impacto del riesgo pero no por completo	4.00	0.38
El Departamento o Unidad solicitante no tenga bien definidos los accesos necesarios para determinado cargo en una solicitud.	Endógeno	Brindar acceso a programas o aplicativos que no corresponden para las funciones del puesto así como también brinad acceso a cierta información restringida.	Medio	Bajo	1	Operacional	Revisión prévia del catálogo de menús.	4 Alta efectividad. El nivel de control implementado reduce el impacto del riesgo pero no por completo	4.00	0.25
Que se brinden los accesos al personal sin la previa notificación de parte de Talento Humanno.	Endógeno	Manipulación no autorizada de la información o aplicativos del sistema.	Medio	Bajo	1	Operacional	Revisión diaria de notificaciones de Depto. Talento Humano.	4 Alta efectividad. El nivel de control implementado reduce el impacto del riesgo pero no por completo	4.00	0.25
El Departamento o Unidad solicitante no tenga bien definidos los accesos necesarios para determinado cargo en una solicitud.	Exógeno	Acceso a opciones que no corresponden a las funciones del puesto y dar acceso a cierta información restringida.	Alto	Bajo	2	Operacional	Revisión previa del catalogo de menus.	4 Alta efectividad. El nivel de control implementado reduce el impacto del riesgo pero no por completo	4.00	0.38
Que se brinden los accesos al personal sin la previa notificación de parte de Talento Humanno.	Endógeno	Falta de control de usuarios creados y asignados a empleados.	Medio	Bajo	1	Operacional	Revisión diaria de notificaciones de Depto. Talento Humano.	4 Alta efectividad. El nivel de control implementado reduce el impacto del riesgo pero no por completo	4.00	0.25
Brindar accesos a modulos sin previa autorización de la Unidad aministradora del mismo.	Endógeno	Acceso a opciones que no corresponden a las funciones del puesto y dar acceso a cierta información restringida.	Alto	Bajo	2	Operacional	Revisión de Catálogo de menús y memorandum de solicitud	4 Alta efectividad. El nivel de control implementado reduce el impacto del riesgo pero no por completo	4.00	0.38
Niveles de seguridad de accesos inadecuados.	Endógeno	Posibles ataques a la integridad de los datos	Alto	Bajo	2	Operacional	Fortalecimiento de la seguridad en perfiles y acceso a aplicaciones	4 Alta efectividad. El nivel de control implementado reduce el impacto del riesgo pero no por completo	4.00	0.38
Insuficiencia en el aseguriamiento de los datos.	Endógeno	Pérdida de la información	Alto	Medio	3	Operacional	Procesos de mantenimiento mensual de las Bases de Datos y monitoreo de posibles intrusiones.	4 Alta efectividad. El nivel de control implementado reduce el impacto del riesgo pero no por completo	4.00	0.75

ANEXO D. MATRIZ DE IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS DE TECNOLOGÍA

FACTORES DE RIESGO	ORIGEN DEL RIESGO	POTENCIAL CONSECUENCIA	IMPACTO	PROBABILIDAD DE OCURRENCIA	NIVEL DE RIESGO INHERENTE	TIPO DE RIESGO	CONTROL DE RIESGO	EFECTIVIDAD	PROMEDIO	RIESGO NETO O RESIDUAL
Pérdida o corrupcion de los datos en Sistema	Endógeno	Pérdida de la información	Alto	Medio	3	Operacional	Copias de seguridad, para tener respaldos y evitar daños, redundancia ciclica. Inclusión en el plan de Backus de todo el servidor	4 Alta efectividad. El nivel de control implementado reduce el impacto del riesgo pero no por completo	4.00	0.75
Ataques informáticos frente a la seguridad de la información	Exogeno	Pérdida, robo o mala utilización de la información.	Alto	Medio	3	Legal	Monitoreo preventivo con el uso de aplicaciones especializadas para determinar anormalidades fortaleciendo la seguridad activa de la red.	4 Alta efectividad. El nivel de control implementado reduce el impacto del riesgo pero no por completo	4.00	0.75
Ataques de malware	Exógeno	Daño, pérdida o corrupcion de la información y equipos.	Alto	Medio	3	Operacional	Utilización de Herramientas de antivirus con bases de firmas actualizadas para la detección y desinfección de malware	4 Alta efectividad. El nivel de control implementado reduce el impacto del riesgo pero no por completo	4.00	0.75
Utilización de dispositivos magnéticos	Endógeno	Robo o sustracción de información sensible	Alto	Bajo	2	Legal	Aplicación de política de uso de dispositivos magnéticos la cual restringe el uso de los mismos.	4 Alta efectividad. El nivel de control implementado reduce el impacto del riesgo pero no por completo	4.00	0.38
Difusión de software dañino	Endógeno	Corrupción de la información	Alto	Bajo	2	Operacional	Aplicacion de Políticas de Uso de Software que limite al personal de TI la instalación de software oficial.	4 Alta efectividad. El nivel de control implementado reduce el impacto del riesgo pero no por completo	4.00	0.38
Negligencia de los usuarios en el uso de la información	Endógeno	Pérdida de la integridad de la información	Medio	Bajo	1	Operacional	Socialización y concientización al personal sobre el correcto uso de los aplicativos.	3 Moderada efectividad. El desempeño del control implementado es medianamente suficiente	3.00	0.33
Uso inadecuado de la Navegación en Internet	Endógeno	Acceso a páginas con contenido malicioso	Medio	Bajo	1	Operacional	Aplicación de Política de Uso de Internet y Herramienta de Filtro de Contenido Web para limitar las categorías de navegación permitidas.	5 Máxima efectividad En relación con el control de riesgo implementado	5.00	0.20
Robo o extravío de equipo portatil fuera del Instituto	Exógeno	Pérdida de información sensible.	Alto	Medio	3	Legal	Utilización de Herramienta de Encriptación de Discos que bloqueara toda la información del mismo.	5 Máxima efectividad En relación con el control de riesgo implementado	5.00	0.60

Tels.: 2231-0914,16,17
18, 19, 20, 21, 33
37, 39, 42, 45, 46
48, 50, 51, 52, 53
2232-5053
2232-5269
2232-5454
2232-4046
Boulevard Centroamérica, Frente
a las Colinas, Tegucigalpa, M.D.C.

Número Piloto: 2232-4036
2232-5613
Técnico Financiero: 2232-5269
Fax Secretaría: 2232-4651
Tesorería: 2239-0776
Apartado Postal No. 92
Comayagüela, M.D.C.

ANEXO D. MATRIZ DE IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS DE TECNOLOGÍA

FACTORES DE RIESGO	ORIGEN DEL RIESGO	POTENCIAL CONSECUENCIA	IMPACTO	PROBABILIDAD DE OCURRENCIA	NIVEL DE RIESGO INHERENTE	TIPO DE RIESGO	CONTROL DE RIESGO	EFECTIVIDAD	PROMEDIO	RIESGO NETO O RESIDUAL
Fallos de Hardware	Endógeno	Falla del computador principal, errores de procesamiento de los servicios.	Alto	Bajo	2	Operacional	Se adquiere si es necesario el soporte del proveedor	4 Alta efectividad: El nivel de control implementado reduce el impacto del riesgo pero no por completo	4.00	0.38
Fluctuación de Energía	Exógeno	Daño en los equipos en general	Alto	Bajo	2	Operacional	Se cuenta con 1 UPS en el Data Center de Tegucigalpa	4 Alta efectividad: El nivel de control implementado reduce el impacto del riesgo pero no por completo	4.00	0.38
Incendio	Endógeno/exógeno	Daño a los equipos en general	Alto	Medio	3	Operacional	Se adquirirá una Remodelación del Data Center de Tegucigalpa que incluya control para incendio	1 Ninguna / Mínima efectividad: No se ha implementado ningún control, o el diseñado no es efectivo	1.00	3.00
Inundaciones	Endógeno	Daño a los equipos en general	Alto	Medio	3	Operacional	Se adquirirá una Remodelación del Data Center de Tegucigalpa que incluya control para inundaciones	1 Ninguna / Mínima efectividad: No se ha implementado ningún control, o el diseñado no es efectivo	1.00	3.00
Paro de Labores/Huelga	Endógeno/exógeno	No halla acceso al datacenter	Alto	Bajo	2	Operacional	Se cuenta con un Data Center de Contingencia en San Pedro Sula	5 Máxima efectividad: En relación con el control de reisgo implementado	5.00	0.30
Robo	Endógeno	Interrupción de los servicios debido al robo de switch y router (equipo de comunicaciones) en oficinas regionales	Alto	Medio	3	Operacional	Se implementará un sistema de camarás con detección de robo para todo el equipo de infraestructura Tecnológica	1 Ninguna / Mínima efectividad: No se ha implementado ningún control, o el diseñado no es efectivo	1.00	3.00
Sabotaje	Endógeno	Daño a la información almacenada en los diferentes aplicativos del sistema ó a los equipos de red.	Alto	Bajo	2	Operacional	Se cuenta con un Data Center de Contingencia en San Pedro Sula	5 Máxima efectividad: En relación con el control de reisgo implementado	5.00	0.30

SEGUNDO: Comunicar la presente Resolución a la Secretaría General del **INSTITUTO** que a su vez lo comunicará a la Gerencia de Tecnología, Unidad de Seguridad Informática, Unidad de Auditoria, Unidad de Procesos, Unidad de Riesgos y Comité de Riesgos -**TERCERO:** La presente Resolución es de ejecución inmediata. F) LIC. ERNESTO EMILIO CARÍAS CORRALES, Director Especialista Presidente, Lic. CÉSAR GUIOVANY GUIFARRO RIVERA, Director Especialista, Lic. NESSY E. MARTÍNEZ HERNÁNDEZ, Directora Especialista y Abogada. ALEJANDRA ISABEL MEDINA, Secretaria General. **COMUNÌQUESE.**

Atentamente,

INSTITUTO DE PREVISION DEL MAGISTERIO
DIRECTOR PRESIDENTE
TEGUCIGALPA, HONDURAS C.A.

LIC. ERNESTO EMILIO CARIAS CORRALES
DIRECTOR PRESIDENTE
Cc: Lic. Nessy E. Martínez Hernández
Lic. Cesar Guiovany Guifarro
Cc: Arch.
ecc/SP