"Plan de Seguridad Física y Tecnológica"

Indice

1. INFORMACIÓN GENERAL

El Presente Plan de seguridad física y tecnológica sobre los activos de tecnología de información (**actualmente en revisión por el comité**) tiene la finalidad de mejorar los niveles de protección y de seguridad de las informaciones y equipos tecnológicos frente a emergencias naturales y/o antrópicas previsibles de probable o cercana ocurrencia, asegurando la respuesta oportuna y adecuada ante la eventualidad de emergencias y desastres que se puedan originar.

Para una mejor organización en el manejo de una emergencia las oficinas se han divido en 04 zonas:

ZONA 1	:	Áreas Administrativas, piso 4 Suite 401
ZONA 2	:	Oficinas técnicas, piso 3 Suite 305
ZONA 3	:	Áreas administrativas, piso 3 Suite 301
ZONA 4	:	Oficinas y salón de reuniones, piso 4 Suite 405

El Plan de contingencia deberá ser revisado y evaluado cada principio de año, y/o cuando se realicen modificaciones estructurales, nuevas instalaciones, o cuando exista alguna sugerencia u observación por parte del personal técnico.

2. INTRODUCCIÓN.

La seguridad es un factor importante y la evaluación de los riesgos en el medio laboral es necesario para poder enfrentar cualquier eventualidad.

3. TERMINOLOGÍA.

Accidente: Suceso extraño al normal desenvolvimiento de las actividades de una organización que produce una interrupción generando daños a las personas, patrimonio o al medio ambiente.

Accidente de trabajo: Lesión ocurrida durante el desempeño de las labores encomendadas a un trabajador.

Amenaza/Peligro: Factor extremo de riesgo, representado por la potencial ocurrencia de un suceso de origen natural o generado por la actividad humana, o la combinación de ambos, que puede manifestarse en un lugar específico, con una magnitud y duración determinadas.

Desastre: Una interrupción grave en el funcionamiento de una comunidad causando grandes pérdidas de nivel humano, material o ambiental, suficientes para que la comunidad afectada no pueda salir adelante por sus propios medios, necesitando apoyo externo.

Emergencia: Estado de daño sobre la vida, el patrimonio y el medio ambiente ocasionado por la ocurrencia de un fenómeno natural o tecnológico que altera el normal desenvolvimiento de las actividades de la zona afectada.

Clasificación de las emergencias: Cada emergencia requiere de una calidad de respuesta adecuada a la gravedad de la situación, para ello se definen tres niveles:

a) Emergencia de Grado 1: Comprende la afectación de un área de operación y puede ser controlada con los recursos humanos y equipos de dicha área.

b) Emergencia de Grado 2: Comprende a aquellas emergencias que por sus características requieren de recursos internos y externos, pero que, por sus implicancias no requieran en forma inmediata de la participación de la alta dirección del Instituto.

c) Emergencia de Grado 3: Comprende a aquellas emergencias que por sus características, magnitud e implicancias requieren de los recursos internos e externos, incluyendo a la alta dirección del Instituto y las organizaciones públicas y privadas del entorno, que correspondan.

Evento adverso: Alteración en la salud de las personas, servicios de salud, sistemas sociales, economía y medio ambiente causados por sucesos naturales, generados por la actividad del hombre o la combinación de ambos, que demanda una respuesta inmediata de la autoridad según sea el caso.

Plan de Evacuación: Plan cuyo objetivo es permitir la evacuación de las personas que se encuentran en determinado lugar de una manera segura y rápida (involucra personas).

Protección Pasiva: Comprende el tipo de edificación, diseño de áreas, vías de evacuación, materiales de construcción, barreras, distancias, diques, acabados, puertas, propagación de humos y gases, accesos, distribución de áreas.

Protección Activa: Comprende la detección, extintores portátiles, automáticos, manuales, redes hidráulicas, bombas, tanques de agua, rociadores, sistemas de espuma, gas carbónico, polvo químico seco. Asimismo, procedimientos de emergencias, brigadas, señalización, iluminación, comunicación.

Seguridad: Grado de aceptación de los riesgos.

Seguridad en Defensa Civil: Cualidad de mantener protegida una instalación, comunidad o área geográfica para evitar o disminuir los efectos adversos que producen los desastres naturales o tecnológicos y que afectan la vida, el patrimonio, el normal desenvolvimiento de las actividades o el entorno. Este mismo concepto comprende a los términos “seguridad” o “seguridad en materia de defensa civil” u otros similares utilizados en este documento.

Riesgo: Es la estimación o evaluación matemática de probables pérdidas de vidas, de daños a los bienes materiales, a la propiedad y la economía, para un periodo específico y área conocidos de un evento especifico de emergencia. Se evalúa en función del peligro y la vulnerabilidad.

Peligro: Probabilidad de ocurrencia de un fenómeno natural o tecnológico potencialmente dañino para un periodo especifico y una localidad o zona conocidas. Se identifica, en la mayoría de los casos, con el apoyo de la ciencia y tecnología.

Vulnerabilidad: Grado de resistencia y/o exposición de un elemento o conjunto de elementos frente a la ocurrencia de un peligro. Puede ser física, social, económica, cultural, institucional y otros.

4. BASE LEGAL

Ley General de Salud Ley No. 42-01
Plan Nacional de Gestión Integral del Riesgo de Desastres Ley No. 147-02 sobre Gestión de Riesgos.

5. EVALUACIÓN DE RIESGO

5.1. Identificación de Riesgos Potenciales

- Ubicación de cada oficina.
- Accesos: sólo poseen una salida, oficina principal.
- Características de construcción, no poseen escaleras de emergencia exterior.
- Área de emergencia, interna.
- Actividades que se desarrollen en cada área:
  - Áreas administrativas: oficinas, biblioteca y sala de reuniones.

- Medios de protección:

  Medios Técnicos:

  - No existen Señales de evacuación
  - No existe Señal de Zona de Seguridad colocada sobre las columnas de los laboratorios.
  - No se cuenta con Extintores.
    (En solicitud de 4 extintores).
  - No se cuentan con luces de emergencia en el nivel de oficinas.

- Medios Humanos:

ZONA 1: Presidente, Director Financiero, Enc. Contabilidad, Asist. Contabilidad, recepcionista, personal de mantenimiento, chofer.
ZONA 2: 4 técnicos, Asist. Informático, Asesor, 2 tecnología.
ZONA 3: Enc. Compras y Legal, Enc, Planificación y Enc, Recursos Humanos.
ZONA 4: No está ocupado.

- Personal a evacuar:

ZONA 1: Presidente, Director Financiero, Enc. Contabilidad, Asist. Contabilidad, recepcionista, personal de mantenimiento, chofer.
ZONA 2: 4 técnicos, Asist. Informático, Asesor, 2 tecnología.
ZONA 3: Enc. Compras y Legal, Enc, Planificación y Enc, Recursos Humanos.
ZONA 4: No está ocupado.

- Servicios Básicos:

  - Línea telefónica y con acceso a internet, pero este medio de comunicación es limitado en caso de emergencia, debido a la saturación y bloqueo.
  - Energía eléctrica, y en caso de corte se cuenta con un grupo electrógeno para las principales áreas de trabajo.

5.2. Evaluación

Se realizará una evaluación que pondere las condiciones del estado actual de cada uno de los riesgos considerados en cada área, así como su interrelación. Para este caso se usará el criterio del riesgo intrínseco en función al uso, de la ocupación, superficie de la actividad y altura de las edificaciones, instalaciones o recinto. Ello permite clasificar el nivel de riesgo alto, medio o bajo.

Las condiciones de evacuación del Laboratorio de Biomedicina deberán ser evaluadas en función del cumplimiento o no de la normatividad vigente, definiéndose las condiciones de evacuación. Se debe establecer criterios de evaluación por el uso de la edificación, de la peligrosidad de los productos o instalaciones existentes, de su complejidad o de otros parámetros que deban ser considerados.

5.3. Valoración del Riesgo:

En esta etapa se evalúan y analizan los riesgos (AR) e impactos potenciales en base a una matriz de riesgo que toma en cuenta la probabilidad, frecuencia y la severidad de este.

Probabilidad (P): Es una estimación de la frecuencia con que ocurre un evento (riesgo) que está asociado a un aspecto e impacto ambiental.

Severidad (S): Es una estimación de la magnitud del daño actual o potencial asociado a un aspecto e impacto ambiental, físico y humano y que puede medirse mediante criterios tales como peligrosidad, toxicidad persistencia, extensión, valor y recuperabilidad del recurso afectado.

Frecuencia (F): Es una estimación de la frecuencia con que se repite un evento (riesgo) asociado a un Aspecto Ambiental o Impacto Ambiental, Accidentes e Incidentes ambientales.

Indicador de Riesgo (IR): Es el resultado de multiplicar el valor asignado a la probabilidad y frecuencia por la severidad del riesgo asociado a un daño en la salud, físico (equipos) y ambientales.

IR = PF x S

5.4. Matriz de Valoración de Riesgos

La Tabla de Valorización de Riesgos nos indicara el nivel de significancia del riesgo, previamente haciendo uso de la fórmula de Indicador de Riesgo (IR).

		SEVERIDAD				
PROBABILIDAD FRECUENCIA		MUY BAJA	BAJA	MEDIA	ALTA	MUY ALTA
	MUY BAJA	1	2	3	4	5
	BAJA	2	4	6	8	10
	MEDIA	3	6	9	12	15
	ALTA	4	8	12	16	20
	MUY ALTA	5	10	15	20	25

5.5. Identificación y Caracterización de la amenaza o Peligro

Nº	ÁREA	RIESGO	PF	S	IR	CONSECUENCIAS	MEDIDAS PREVENTIVAS Y CORRECTIVAS
1	ZONA 1	- Accidente en evacuación - Instalaciones eléctricas	B	B	4	- Afectar la salud del personal y visitantes, caídas, golpes. - Amago de incendio por corto circuito o recalentamiento de circuitos. - Generación de arco eléctrico en equipos de cómputo.	- Verificar que las rutas de evacuación estén libres de obstáculos. - Instalaciones eléctricas en buen estado - Medidas de prevención y contingencia contra incendios - Pasadizos con amplitud necesaria para facilitar la evacuación - Pozo a tierra y circuito de puesta a tierra. - Brigadas Defensa Civil o Bomberos.
2	ZONA 2	- Accidente en evacuación - Instalaciones eléctricas	M	M	9	- Afectar la salud del personal caídas, golpes. - Cortes menores. - Quemaduras químicas, intoxicaciones.	- Verificar que las rutas de evacuación estén libres de obstáculos. - Instalaciones eléctricas en buen estado - Medidas de prevención y contingencia contra incendios - Pasadizos con amplitud necesaria para facilitar la evacuación - Pozo a tierra y circuito de puesta a tierra. - Brigadas Defensa Civil o Bomberos.
3	ZONA 3	- Incidente por aglomeración - Rotura de material de vidrio - Accidente en evacuación - Instalaciones eléctricas	M	A	12	- Afecta la salud del personal caídas, golpes. - Cortes menores. - Quemaduras químicas, intoxicaciones. - Infecciones, enfermedades	- Verificar que las rutas de evacuación estén libres de obstáculos. - Instalaciones eléctricas en buen estado - Medidas de prevención y contingencia contra incendios - Pasadizos con amplitud necesaria para facilitar la evacuación - Pozo a tierra y circuito de puesta a tierra. - Brigadas Defensa Civil o Bomberos.
4	ZONA 4	- Lesiones por caída al resbalar	B	M	6	- Afectar la salud del personal, golpes, fracturas. - Pérdida de horas-hombre de trabajo	- Escalera provista de pasamanos y peldaños con cantoneras - Brigadas Defensa Civil o Bomberos.

Elaborado: Comité de emergencia.

6. OBJETIVO DEL PLAN DE CONTINGENCIA

El Plan de Contingencias tiene por objeto establecer las acciones que se deben de ejecutar frente a la ocurrencia de eventos de carácter técnico, accidental o humano, con el fin de proteger la vida humana, los bienes y patrimonio de los Laboratorios de Biomedicina y Microbiología, así como evitar retrasos y costos debido a accidentes.

Las actividades realizadas en los laboratorios son las más propensas a presentar riesgos, debido a la naturaleza de estas, así como la presencia de eventos naturales por encontrarnos en una zona sísmica, requiriéndose por tanto un Plan de Contingencia que evalúe los riesgos y que incluya las medidas para responder y controlar tales hechos.

En este Plan se esquematiza las acciones y se presenta un ordenamiento y descripción de los procesos y operaciones, indicando los factores generadores de riesgo de siniestros, de modo que permitan, primero identificar, enumerar y posteriormente recomendar las acciones de prevención, acción y mitigación a fin de reducir y prever los efectos destructivos de los fenómenos naturales o antrópicos que puedan ocurrir.

También se considera emergencias contraídas por eventos productos de errores involuntarios de operación como derrames, incendios y/o explosiones. Por lo que será necesario contar con personal encargado de emergencias a este nivel.

7. ORGANIZACIÓN PARA LA EMERGENCIA

La estructura del plan de contingencia se fundamenta en el planeamiento. Planear es identificar las posibles situaciones de emergencia, sus posibles variaciones, los procedimientos para hacerles frente y las alternativas disponibles. ***Es mejor estar preparados para algo que a lo mejor no va a suceder, a que nos suceda algo para lo cual no estemos preparados***.
El planeamiento se desarrolla a través de un proceso de seis etapas, cada una de las cuales se detalla a continuación:

Inventario de Peligros Específicos: Análisis completo de los peligros existentes en cada una de las áreas. Es importante en esta fase anticipar las situaciones extremas para cada uno de los peligros. En la evaluación de cada uno de los peligros se deberá especificarse su naturaleza, ubicación y magnitud relativa.

Inventario de Recursos: Una evaluación de los recursos disponibles en cada una de las áreas, indicando su clase, cantidad, ubicación, disponibilidad y tiempo de respuestas.
En esta fase es importante ser suficientemente realista para no crear falsas expectativas. También deberá incluirse los recursos externos, haciendo las mismas indicaciones.

Establecimiento de Objetivos: Para cada una de las situaciones esperadas se deberán definir objetivos específicos, para adelantar las acciones.

Procedimientos Operativos: Con base en los objetivos propuestos se deben establecer procedimientos operacionales claros, incluyendo las alternativas de acción a medida que el siniestro evoluciona. El conocimiento de este procedimiento nos permitirá definir las necesidades de recursos y programar su utilización.

Plan de Recuperación: La acción de atender una emergencia no termina con el control de esta, sino que se debe llevar hasta el restablecimiento de la normal operación de la organización. Para esto se debe contar con un plan de recuperación post-siniestro, que incluye mantenimiento interno y externo, proveedores y demás actividades, como relaciones con el agente de seguros y autoridades municipales.

Entrenamiento del Personal: La única manera de que cualquier plan funcione es que cada una de las personas involucradas en los mismos conozca y sea capaz de desarrollar las acciones previstas.

8. PLAN DE SEGURIDAD TECNOLÓGICA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

8.1. Objetivo general

Regular el uso adecuado de los sistemas de información y los recursos tecnológicos de la institución por parte de todos los colaboradores; preservando, protegiendo y administrando de forma eficiente la información y los medios utilizados para su manipulación y procesamiento, con el fin de asegurar el cumplimiento de integridad, confidencialidad y disponibilidad.

Objetivos específicos

- Informar y concientizar a todos los colaboradores de la institución sobre las políticas de seguridad y privacidad de la información, minimizando las amenazas que puedan afectar la entidad.
- Verificar la aplicación de las políticas de seguridad en los equipos de cómputo usuarios finales y en los sistemas de información.

8.2. Alcance

El plan de seguridad y privacidad de la información brinda las políticas, conceptos y campos de aplicación para todos los procesos institucionales, con el objetivo de cumplir con los lineamientos de las TIC en el proceso de una gestión responsable frente a la información.

8.3. Términos y Definiciones

Confidencialidad: garantizar que la información sea accesible sólo por las personas autorizadas.

Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos informáticos toda vez que lo requieran.

Adicionalmente, deberán considerarse los conceptos de:

Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución.

Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto la entidad.

Confiabilidad de la información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Para los efectos de una correcta interpretación del presente plan, se realizan las siguientes definiciones:

✓ **Spoofing:** uso de técnicas de suplantación que a través de las cuales un atacante, con fines maliciosos o de investigación se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.

✓ **Phishing:** técnica con base a la ingeniería social que trata de adquirir información de forma fraudulenta engañando e incitando al usuario que entregue información confidencial a través de páginas falsas, correos o hasta llamadas telefónicas.

✓ **Routers:** dispositivo de red de capa 3 diseñado para transportar el tráfico entre diferentes redes dependiendo de las reglas establecidas.

✓ **Switches:** dispositivo de red de capa 2 que se encarga de establecer la conexión física entre los diferentes equipos de red basado en sus direcciones físicas.

✓ **Access Point:** dispositivo de red que permite conexiones inalámbricas de diferentes tecnologías como son 802.11a, 802.11b, 802.11g entre otros.

✓ **RDSI:** sus siglas traducen Red Digital de servicios Integrados y es una tecnología de conectividad WAN digital y punto a punto que consta de canales BRI (de 64kbps cada uno) para el transporte de datos más un canal D (de 16 kbps) para fines de señalización.

✓ **Keylogger:** software que se puede utilizar para fines maliciosos el cual guarda un log local con todas las teclas que el usuario digite en el equipo donde está instalado.

✓ **Port Scanner:** software que realiza un escaneo de puertos contra una dirección IP específica. Revela muchas de las vulnerabilidades de los sistemas a nivel perimetral y de aplicación.

✓ **DoS:** traduce ataques de negación de servicio y es una técnica que busca que un recurso sea inaccesible para usuarios legítimos.

✓ **SMTP:** protocolo simple de transferencia de correo el cual está basado en texto utilizado para el intercambio de mensajes de correo electrónico entre dispositivos. Es el protocolo responsable de enviar los correos.

✓ **Programas Peer-to-Peer:** programas que utilizan a todos los otros usuarios de la red de internet para compartir información, por lo cual todos son clientes y servidores al tiempo.

Entre los más destacados actualmente se encuentran, limeWare, Emule, Azureus, BitTorrents y Kazza.

✓ **Proxys Piratas:** pueden ser páginas o software que enmascaran las URL (páginas de navegación) reales a las que el usuario está accediendo con el objetivo de tratar de violar los controles que se tienen de manera que no descubra a donde estaban accediendo realmente.

✓ **Incidente de seguridad:** evento que viole, o que intente violar la seguridad informática, se considera violación de la seguridad informática, el hecho que un individuo intente, ejecute o, encubra acciones o tenga acceso a información no autorizada para su uso o modificación.

✓ **Política de seguridad:** es una declaración formal de las reglas que deben seguir las personas con acceso a los activos de tecnología e información, dentro de la ANAMAR.

✓ **Procedimientos:** constituyen la descripción detallada de la manera como se implementa una política.

✓ **Virus informático:** programa ejecutable o segmento de código con habilidad de ejecutarse y reproducirse, regularmente escondido en documentos electrónicos, que causan problemas al ocupar espacio de almacenamiento, así como destrucción de datos (información) y reducción del desempeño de un equipo de cómputo.

✓ **GPO:** es un conjunto de políticas del sistema, desplegadas mediante el directorio activo de la ACI y se aplican apenas el usuario inicia sección en alguno de los equipos de cómputo de la agencia.

8.4. Roles y Responsabilidades

División de Tecnología de la Información y Comunicación: es responsable de la elaboración, actualización y divulgación del Plan de Seguridad. Aprueba las Políticas de Seguridad y Privacidad Informática y es responsable de fortalecer e incentivar las políticas allí definidas dando cumplimiento a la gestión responsable frente a la información.

Usuarios Finales (colaboradores, contratistas, terceros): cumplir a cabalidad con las políticas de Seguridad y Privacidad Informática, procedimientos y buenas prácticas que se tenga definido en la institución para el buen uso de los recursos tecnológicos. Informar cualquier anomalía, vulnerabilidad o incidente de seguridad que se detecte en el que hacer de sus labores

Administrador de Red, Sistemas y Servidores: identificar vulnerabilidades en los sistemas de información e infraestructura, hacer ajustes necesarios para corregir y disminuir los riesgos informáticos. Auditar el cumplimiento de las políticas y notificar a través de informes formales a la división de recursos humanos los casos de no cumplimiento.

Elaborar planes, campañas de divulgación de las políticas a todos los usuarios y otras estrategias de tipo preventivas. Proveer los recursos necesarios para el buen cumplimiento de estas políticas. Sensibilizar a todos los colaboradores la importancia de estas políticas de seguridad para el éxito de estas.

8.5. Descripción de las Políticas de Seguridad y Privacidad de la Información

Acceso a la información

- La información es un recurso que, como el resto de los activos, tiene valor para la institución siendo este el activo más importante, su manejo influye en el objetivo de alcanzar la misión institucional y está expuesta a problemas de seguridad, por consiguiente, debe ser debidamente protegida.
- Todos los colaboradores de la institución deben tener acceso sólo a la información necesaria para el desarrollo de sus funciones. Es responsabilidad de cada encargado de área solicitar el acceso de acuerdo con el trabajo realizado por el personal a su cargo.
- Las prerrogativas otorgadas para el uso de los sistemas de la institución, servicios de red y correo deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la entidad.
- Toda la información contenida, procesada o generada en los equipos de cómputo es propiedad de la ANAMAR.

8.6. Seguridad de la Información

- Los colaboradores que laboran en la ANAMAR son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la institución y por la normativa que la proteja, pendientes a evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma. entre esta información tenemos la siguiente: hojas de Excel, documentos tipo Word, documentos tipo PowerPoint, correo electrónico, documentos tipo pdf, entre otros.
- Todos los colaboradores que utilice los recursos informáticos tienen la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y crítica.
- No debe dejar visible sus contraseñas de correo, red y archivos, porque pueden ser utilizadas por otras personas alterando o dañando su información, ni tampoco comparta sus contraseñas pueden ser utilizadas con otros objetivos.
- No debe permitir que personal externo opere su información.
- Al desplazarse de su puesto de trabajo, bloquee la sección en el equipo, esto evita posibles ingresos no autorizados a su información.

8.7. Seguridad Sistemas de Información

- La plataforma office 365, herramientas gubernamentales, CRM institucional, unidades de red, softwares de índoles contable y legal son utilidades asociadas de la institución que debe ser usado únicamente para el ejercicio de las funciones y actividades de competencia de cada usuario.
- El uso de la red Internet debe ser solo para fines laborales, no está permitido el ingreso a páginas del siguiente tipo: pornografía, radio y tv, juegos, armas, sitios maliciosos, software free, entre otros.
- Contraseñas
  La contraseña debe de cumplir con una longitud mínima de 8 caracteres, y al menos con tres tipos entre los caracteres siguientes:
  - Letras Mayúsculas
  - Letras Minúsculas
  - Números en sustitución de letras (1 por I, 0 por o, 3 por la E, etcétera)
  - Caracteres especiales no alfanuméricos, como signos de puntuación
  - Cada 90 días el sistema le exige que cambie su contraseña de red.

8.8. Seguridad en recursos informáticos

Todos los recursos informáticos deben cumplir con lo siguiente:

- **Administración de usuarios:** establece como deben ser utilizadas las claves de ingreso a los recursos informáticos y da parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiarlas y los períodos de vigencia de estas, entre otras. Lo anterior se encuentra configurado en los controladores del dominio de la ANAMAR con GPO (Group Policy Object).
- **Rol de usuario:** los sistemas de información, bases de datos y aplicativos deberán contar con roles predefinidos, definiendo las acciones permitidas por cada uno de estos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles. También deben permitir que un rol de usuario desarrolle la administración de usuarios.

- El control de acceso a todos los sistemas de información de la institución debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario. Las palabras claves o contraseñas de acceso a los recursos informáticos, que designen los usuarios de la ANAMAR son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.
- Todo sistema de información debe tener definidos los perfiles de usuario de acuerdo con la función y cargo que puedan acceder a dicho sistema.
- Toda la información que sea sensible, crítica o valiosa debe tener controles de acceso para garantizar que no sea inapropiadamente descubierta, modificada, borrada o no recuperable.

8.9. Seguridad en comunicaciones

- Las direcciones IP internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la entidad, deberán ser considerados y tratados como información confidencial.
- Todas las conexiones a redes externas de tiempo real que accedan a la red interna de la institución deben pasar a través de los sistemas de defensa electrónica que incluyen servicios de inscripción y verificación de datos, detección de ataques e intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.

8.10. Software utilizado

- Todo software que utilice la institución será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos o reglamentos internos.
- Todo el software de manejo de datos que utilice la institución dentro de su infraestructura informática deberá contar con las técnicas más avanzadas para garantizar la integridad de los datos.
- Debe existir una cultura informática dentro de la institución que garantice el conocimiento por parte de los colaboradores, contratistas y personal externo de las implicaciones que tiene el instalar software ilegal en los computadores de la ANAMAR.
- La instalación de software en los equipos estará controlada mediante configuración especial en dichos computadores y administrada desde los servidores, la cual solicitará usuario y contraseña del administrador al momento de realizar una instalación, esto asegura que ningún programa o software podrá ser instalado en los computadores; a su vez el personal de sistemas deberá intervenir en dicha instalación ya que son los autorizados para esta labor.

8.11. Actualización de hardware

Cualquier cambio que se requiera realizar en los equipos de cómputo de la entidad (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización del personal de sistemas.
La reparación técnica de los equipos, que implique la apertura de estos, únicamente puede ser realizada por el personal de TIC y se documentará cuando no exista garantía vigente de las partes a reemplazar.

Los computadores e impresoras no deben reubicarse sin la aprobación previa del personal de Sistemas.

8.12. Violaciones a las Políticas de Seguridad

Las siguientes actividades son consideradas como violaciones a las políticas de seguridad:

- Enviar correo electrónico no solicitado o Spam.
- Envío de correo con contenidos pornográficos.
- Instalación o ejecución de software no autorizado.
- Utilización del internet indebidamente, esto incluye, navegación a páginas con contenidos pornográficos, sitios de música en línea, juegos en línea, sistemas de mensajería instantánea (no autorizados), casinos, proxys piratas, programas de carga de archivos, o cualquier otro sitio con fines diferentes a los laborales.
- Traslado o instalación de nuevos equipos a la red sin la autorización ni el procedimiento establecido por el proceso de recursos tecnológicos.
- Dañar física o lógicamente los equipos o la infraestructura informática.
- Instalar dispositivos o tarjetas de acceso remoto, módems. RDSI, routers o cualquier otro dispositivo de comunicaciones en los clientes de la red.
- Utilizar cualquiera de los recursos informáticos de la institución para fines diferentes a las funciones contractuales.
- Utilizar cualquier tipo de software para fines malicioso o intrusos tales como sniffers, port scanner, keyloggers, entre otros.
- Utilizar cualquier técnica de hacking hacia cualquiera de los recursos tecnológicos de la institución entre los que se incluye, ataques DoS, phising, spoofing y broadcast storm.
- Violación o cambio de contraseñas diferentes a las personales.
- Usar cuentas de equipos sin autorización.
- Conseguir acceso no autorizado a cualquier equipo o información.
- Conseguir acceso no autorizado a los recursos compartidos, almacenados en los equipos y servidores de la infraestructura informática.
- Acceso sin autorización a equipos de red tales como servidores, routers, Switches, Access Point, Firewalls, u otros appliance de red de la institución o que estén en sus instalaciones.
- Ejecución intencionada de scripts que comprometan la seguridad y buena utilización de los recursos.
- Ejecutar una base de datos con el propósito de colectar datos contenidos en ella.
- Acceso no autorizado a sistemas críticos y delicados como bases de datos, CRM institucional, sistema backup, unidad de red no autorizada.
- Ejecución de comandos SNMP a servidores de correo.
- Utilizar cualquiera de los recursos informáticos de la institución para fines lucrativos diferentes a los contratos.
- Las violaciones de las políticas de seguridad y privacidad por parte de colaboradores y contratistas o personal externo de los recursos tecnológicos darán lugar a la respectiva investigación de carácter disciplinario, penal, civil y fiscal a que haya lugar.

8.13. Propiedad Intelectual

La ANAMAR podrá tener acceso en el momento que sea necesario a cualquier información alojada en alguno de los equipos que son propiedad de esta tales como PC, servidores, unidades lógicas de la SAN entre otros, así mismo podrá tener acceso a cualquier información generada y transmitida por la red.

Todos los computadores y servidores de la institución deberán pertenecer al dominio y sujetarse a las políticas de seguridad que estén establecidas actualmente, por lo tanto, cualquier software

que se esté instalando en las maquinas deberá tener su respectiva licencia y previa autorización por parte de la División de TIC para su correcto funcionamiento.

Se debe tener en cuenta que cualquier acción dentro del dominio se registra con el nombre de usuario individual, por lo cual los usuarios y claves del dominio son personales e intransferibles y cada uno es responsable de la utilización y del buen uso que les dé a los elementos informáticos, tales como uso del internet, correo, almacenamiento y transferencia de archivos, carpetas compartidas, y utilización de las aplicaciones.

Para una mejor organización oficinas se han divido en 04 zonas:

- **ZONA 1:** Áreas Administrativas, piso 4 Suite 401
- **ZONA 2:** Oficinas Técnicas, piso 3 Suite 305
- **ZONA 3:** Áreas Administrativas, piso 3 Suite 301
- **ZONA 4:** Área Financiera, Tecnológica y Salón de Eventos, piso 4 Suite 405

La zona 1 dispone de un gabinete de distribución (switch, patch panel, cableado), así como un UPS central el cual alimenta esta zona y la zona 3.
La zona 2 dispone de un gabinete de distribución (switch, patch panel, cableado, fibra óptica ADSL, troncal SIP)
La zona 3 dispone de un gabinete de distribución (switch, patch panel, cableado)
La zona 4 dispone de un gabinete de distribución (switch, patch panel, cableado), así como un UPS central el cual alimenta esta zona y la zona 2).

8.14. Plan de Mejora

Para finales del 2019, en la zona 4 se estará concentrando el centro de datos de la institución, el cual constará de Servidor, Dominio, Central Telefónica, Servidor Wi-Fi, Firewall, etc).

APROBACIÓN

Elaborado por:

Revisado por:		

Aprobado por: