	Descripción	Fecha	Elaboró	Revisó	Aprobó
1	Plan Seguridad Privacidad y Riesgos de información	30 de julio de 2018	Irene garzon reyes Unidad de apoyo Informática	Irene garzon reyes Unidad de apoyo Informática	Carlos Mendoza Vélez. Subdirección Administrativa y Financiera

PLAN SEGURIDAD PRIVACIDAD Y RIESGOS DE LA INFORMACIÓN

El Instituto Sinchi con el fin de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de minimizar el riesgo de pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.

La seguridad de la información se entiende como la preservación de las siguientes características:

Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

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 relacionados con la misma, toda vez que lo requieran. Adicionalmente, debe considerarse los conceptos de:

Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

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 el Organismo.

ANTECEDENTES

1. La Subdirección Administrativa y Financiera a través de la unidad de Informática han establecido políticas, planes y guías, dentro de las cuales se tienen:
   1.1. Política para conexiones inalámbricas
   1.2. Política para Instalación y uso de antivirus Institucional
   1.3. Política para uso de red
   1.4. Política para acceso a servicios
   1.5. Política para copia de seguridad
   1.6. Plan de mantenimiento de equipos
   1.7. Guía para apagado de servidores Institucionales
   1.8. Guía para el establecimiento de grupos de usuarios a través de Mensajería instantánea - hangouts
   1.9. Guía para instalación Sistema Stone
   1.10. Guía para cambio de contraseña
   1.11. Guía para Subir VPN sedes Leticia y Guaviare
   1.12. Guía metodológica para atender el proceso de mesa de ayuda – Mantis
   1.13. Guía par análisis de riesgos – en revisión
   1.14. Guía para recibir aplicaciones – para aprobación
   1.15. Formato inclusión nuevos usuarios
   1.16. Guía para acceder a la intranet
   1.17. Guía para copia de seguridad y restablecimiento servidor Windows.

2. Con el propósito de proveer a los usuarios del Instituto Sinchi un punto único de contacto mediante el cual se resuelvan y/o canalicen sus necesidades relativas al uso de recursos y servicios de plataformas tecnológicas, se implantó la mesa de ayuda mantis a través de software libre cuyos objetivos principales son
   2.1. Tener el control de toso los requerimientos
   2.2. Resolver un alto porcentaje en línea
   2.3. Seguimiento en línea de los casos derivados
   2.4. Reducir llamados recurrentes en el tiempo

3. En el año En el año 2017, se realizó levantamiento de los activos de información los cuales se están en versión preliminar, para revisión. una vez se obtenga la aprobación se dará cumplimiento a lo establecido en la ley 1712 de 2014 respecto a la generación y publicación de los siguientes productos

3.1. Registro de activos
3.2. Índice de información clasificada o reservada
3.3. Esquema de publicación.

4. De acuerdo con el levantamiento de los activos de información se está adelantando el mapa de riesgos.

5. Se encuentra para revisión la versión preliminar de política para recibo de aplicativos o desarrollos, con la correspondiente lista de chequeo, para el recibo de los mismos. Versión preliminar.

6. A través de la resolución 003 de 2018 la directora general adopta para el Instituto Sinchi la política general de seguridad y privacidad de la información, la cual tiene como objetivo fundamental.

ALCANCE:

Este Plan de Seguridad y Privacidad de la Información y su política, son aplicables a todos los trabajadores del Instituto Sinchi, contratistas, proveedores y/o terceros, usuarios de la información impresa, digital y la soportada sobre las tecnologías de información y las comunicaciones del Instituto Sinchi.

OBJETIVO

Definir los mecanismos y todas las medidas necesarias por parte del Instituto Amazónico de Investigaciones Científicas Sinchi tanto técnica, lógica, física, legal y ambiental para la protección de los activos de información, los recursos y la tecnología de la entidad, con el propósito de evitar accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir de forma intencional o accidental, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Objetivos Específicos:

1. Minimizar el riesgo de los procesos misionales de la entidad.
2. Cumplir con los principios de seguridad de la información.
3. Cumplir con los principios de la función administrativa.
4. Mantener la confianza de los trabajadores, contratistas, terceros y demás partes involucradas.
5. Apoyar la innovación tecnológica.
6. Implementar el sistema de gestión de seguridad de la información.
7. Proteger los activos de información.
8. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
9. Fortalecer la cultura de seguridad de la información en los trabajadores, terceros, aprendices, practicantes y clientes del Instituto Amazónico de Investigaciones Científicas Sinchi
10. Garantizar y gestionar la continuidad del negocio frente a incidentes.
11. Dar cumplimiento a las obligaciones legales en relación con la protección de datos personales y de divulgación de la información catalogada como pública.

DEFINICIONES

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización.

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.
Control: Medida que modifica el riesgo.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Riesgo en la seguridad de la información. Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo. Aceptación de la pérdida o ganancia proveniente de un riesgo particular

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.

Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI: Sistema de Gestión de Seguridad de la Información.

Cronograma Plan de Seguridad Privacidad y Riesgos DE LA Información

Teniendo en cuenta la normatividad vigente del Estado Colombiano, que obliga el adecuado uso y tratamiento de la información gestionada por la Entidad en términos de confidencialidad, integridad y disponibilidad, el Instituto Sinchi presenta el cronograma a seguir por los próximos meses con el propósito de ponernos a la vanguardia.

El Plan se ejecutará de acuerdo con la disponibilidad presupuestal que facilite el desarrollo de los ítems propuestos relacionados con análisis, diseño, capacitación.

Cronograma

Ítem	Detalle	AÑO 2018				AÑO 2019	
		Enero a marzo	A bril a Junio	Octubre a Diiemb	Octubre a Diciem.	año 2019	año 2019
0	**DIAGNOSTICO DEL ESTADO DE IMPLEMENTACION DE ISO 27001**						
1	**CONTEXTO DE LA ORGANIZACIÓN**						
1.1	Comprensión De Las Necesidades Y Expectativas De Las Partes Interesadas						
1.2	Determinación del alcance del sistema de gestión de la seguridad de la información						
2	**POLÍTICAS DE SEGURIDAD**						
2.1	Directrices de la dirección en seguridad de información						
2.1.1	Conjunto de políticas para la seguridad de la información						
2.1.2	Revisión de la políticas para la seguridad de la información						
3	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN**						
3.1	**Organización Interna**						
3.1.1.	Compromisos de la Dirección con la seguridad en la información						
3.1.2	Coordinación de la seguridad de la información						
3.1.3	Asignación de responsabilidades relativas a la seguridad de la información						
3.1.4	Proceso de autorización de recursos para el tratamiento de la información						
3.1.5	Acuerdos de confidencialidad						

Ítem	Detalle	AÑO 2018				AÑO 2019	
		Enero a marzo	A bril a Junio	Octubre a Diiemb	Octubre a Diciem.	año 2019	año 2019
3.1.6	Contacto con las autoridades						
3.1.7	Contactos con grupos de especial interés						
3.1.8	Revisión independiente de la seguridad de la información						
3.2	**Terceros**						
3.2.1	Identificación de los riesgos derivados del acceso a terceros						
3.2.2.	Tratamiento de la seguridad en la relación con los clientes						
3.2.3	Tratamiento de la seguridad en contratos con terceros						
4	**GESTION DE ACTIVOS**						
4.1.	Responsabilidad sobre los activos						
4.1.1.	Inventario de activos						
4.1.2	Propiedad de los activos						
4.1.3	Uso aceptable de los activos						
4.1.4	Devolución de activos						
4.2	Clasificación de la información						
4.2.1	Directrices de la clasificación						
4.2.2.	Etiquetado y manipulado de la información						
4.2.3.	directrices de clasificación						
4.2.3.	Etiquetado y manipulación de la información						
4.2.4.	manipulación de activos						

Ítem	Detalle	AÑO 2018				AÑO 2019	
		Enero a marzo	A bril a Junio	Octubre a Diiemb	Octubre a Diciem.	año 2019	año 2019
4.2.5	Manejo de los soportes de almacenamiento						
4.2.6	Gestión de soportes extraíbles						
4.2.7	Eliminación de los soportes						
4.2.8	Soportes Físicos de transito						
5	**SEGURIDAD LIGADA A LOS RECUROS HUMANOS**						
5.1.	**Antes del empleo**						
5.1.1.	Funciones y responsabilidades						
5.1.2	Investigación y antecedentes						
5.1.3	Términos y condiciones de contratación						
5.2	**Durante el empleo**						
5.2.1	Responsabilidades de la dirección						
5.2.2.	Concientización formación, y capacitación en seguridad de la información						
5.2.3	Proceso disciplinario						
5.3	**Cese del empleo o cambio de puesto de trabajo**						
5.3.1	Responsabilidad del cese o cambio						
5.3.2	Devolución de activos						
5.3.3	Retirada de los derechos de acceso						
6	**CONTROL DE ACCESOS**						
6.1	Requisitos de negocio para el control de accesos						
6.1.1	Política de control de accesos						
6.1.2	Control de acceso a las redes y servicios asociados						

Ítem	Detalle	AÑO 2018				AÑO 2019	
		Enero a marzo	A bril a Junio	Octubre a Diiemb	Octubre a Diciem.	año 2019	año 2019
6.2	Gestión de acceso de usuario						
6.2.1	Gestión de altas/bajas en el registro de usuarios						
6.2.2	Gestión de los derechos de acceso asignados a usuarios						
6.2.3	gestión de los derechos de acceso con privilegios especiales						
6.2.4	Gestión de información confidencial de autenticación de usuarios						
6.2.5	revisión de los derechos de acceso de los usuarios						
6.2.6	Retira o adaptación de los derechos de acceso						
6.3	responsabilidades del usuario						
6.3.1	uso de la información confidencial para la autenticación						
6.4	control de acceso a sistemas y aplicaciones						
6.4.1	restricción de acceso a la información						
6.4.2	procedimiento seguros de inicio de sesión						
6.4.3	Gestión de contraseñas de usuario						
6.4.4	uso de herramientas de administración de sistemas						
6.4.5	control de acceso al código fuente de los programas						
7	**CIFRADO**						

Ítem	Detalle	AÑO 2018				AÑO 2019	
		Enero a marzo	A bril a Junio	Octubre a Diiemb	Octubre a Diciem.	año 2019	año 2019
7.1	Controles criptográficos						
7.1.1	política de uso de los controles criptográficos						
7.1.2	gestión de claves						
8	**SEGURIDAD FISICA Y AMBIENTAL**						
8.1	Áreas seguras						
8.1.1	perímetro de seguridad física						
8.1.2	controles físicos de entrada						
8.1.3	seguridad de oficina, despachos y recursos						
8.1.4	protección contra las amenazas externas y ambientales						
8.1.5	el trabajo en áreas seguras						
8.1.6	áreas de acceso publico, carga y descarga.						
8.2	seguridad de los equipos						
8.2.1	emplazamiento y protección de equipos						
8.2.2	instalaciones de suministro						
8.2.3	seguridad del cableado						
8.2.4	mantenimiento de los equipos						
8.2.5	salida de activos fuera de las dependencias de la empresa						
8.2.6	seguridad de los equipos y activos fuera de las instalaciones						

Ítem	Detalle	AÑO 2018				AÑO 2019	
		Enero a marzo	A bril a Junio	Octubre a Diiemb	Octubre a Diciem.	año 2019	año 2019
8.2.7	reutilización o retirada segura de dispositivos de almacenamiento						
8.2.8	equipo informático de usuario desatendido						
8.2.9	política de puesto de trabajo despejado y bloqueo de pantalla						
9	**SEGURIDAD EN LA OPERATIVA**						
9.1	responsabilidades y procedimientos de operación						
9.1.1	documentación de procedimientos de operación						
9.1.2	gestión de cambios						
9.1.3	gestión de capacidades						
9.1.4	separación de entornos de desarrollo, prueba y producción						
9.2	protección contra código malicioso						
9.2.1	Controles contra código malicioso						
9.3	copias de seguridad						
9.3.1	copias de seguridad de la información						
9.4	registro de actividad y supervisión						
9.4.1	registro y gestión de eventos de actividad						
9.4.2	protección de los registros de la información						
9.4.3	registros de actividad del administrador y operador del sistema						
9.4.4	Sincronización de relojes						

Ítem	Detalle	AÑO 2018				AÑO 2019	
		Enero a marzo	A bril a Junio	Octubre a Diiemb	Octubre a Diciem.	año 2019	año 2019
9.5	control del software en explotación						
9.5.1	instalación del software en sistemas de producción						
9.6	gestión de la vulnerabilidad técnica						
9.6.1	gestión de las vulnerabilidades técnicas						
9.6.2	restricciones en la instalación de software						
9.7	consideración de las auditorias de los sistemas de información.						
9.7.1	Controles de auditorías de los sistemas de información.						
10	**SEGURIDAD EN LAS TELECOMUNICACIONES**						
10.1	gestión de la seguridad en la redes						
10.1.1	controles de red						
10.1.2	Mecanismos de seguridad asociada a los servicios en red						
10.1.3	segregación de redes						
10.2	intercambio de información en partes externas						
10.2.1	políticas y procedimientos de intercambio de información						
10.2.2	acuerdos de intercambio						
10.2.3	mensajería electrónica						

Ítem	Detalle	AÑO 2018				AÑO 2019	
		Enero a marzo	A bril a Junio	Octubre a Diiemb	Octubre a Diciem.	año 2019	año 2019
10.2.4	Acuerdos de confidencialidad y secreto						
11	**ADQUISICION, DESARRROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION.**						
11.1	Requisitos de seguridad de los sistemas de información						
11.1.1	Análisis y especificaciones de los requisitos de seguridad						
11.1.2	Seguridad de las comunicaciones en servicios accesibles por redes publicas						
11.1.3	protección de las transacciones por redes telemáticas						
11.2	seguridad en los procesos de desarrollo y soporte						
11.2.1	Política de desarrollo seguro de software						
11.2.2	Procedimientos de control de cambios en los sistemas						
11.2.3	revisión técnicas de las aplicaciones tras efectuar cambios en el sistema operativo						
11.2.4	restricción a los cambios a los paquetes de software						
11.2.5	Uso de principios de ingeniería en protección de sistemas						
11.2.6	Seguridad en entornos de desarrollo						

Ítem	Detalle	AÑO 2018				AÑO 2019	
		Enero a marzo	A bril a Junio	Octubre a Diiemb	Octubre a Diciem.	año 2019	año 2019
11.2.7	Externalización del desarrollo de software						
11.2.8	Pruebas de funcionabilidad durante el desarrollos de los sistemas						
11.2.9	Pruebas de aceptación.						
11.3	Datos de prueba						
11.3.1	Protección de los datos utilizados en pruebas						
12	**RELACIONES CON SUMINISTRADORES**						
12.1	Seguridad de la información en las relaciones con suministradores						
12.1.1	Política de seguridad de la información para suministradores						
12.1.2	Tratamiento del riesgos dentro de los acuerdos de suministradores						
12.1.3	Cadena de suministro en tecnologías de la información y comunicación.						
12.2	Gestión de la prestación del servicio por suministradores						
12.2.1	Supervisión y revisión de los servicios prestados por terceros						
12.2.2	Gestión de cambios en los servicios prestados por terceros						

Ítem	Detalle	AÑO 2018				AÑO 2019	
		Enero a marzo	A bril a Junio	Octubre a Diiemb	Octubre a Diciem.	año 2019	año 2019
13	**GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION**						
13.1	Gestión de incidentes de seguridad de la información y mejoras						
13.1.1	responsabilidades y procedimientos						
13.1.2	Notificaciones de eventos de seguridad de la información						
13.1.3	Notificación de puntos débiles de la seguridad						
13.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.						
13.1.5	Respuesta a los incidentes de seguridad						
13.1.6	Aprendizajes de los incidentes de seguridad de la información						
13.1.7	recopilación de evidencias						
14	**ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DEL NEGOCIO**						
14.1	Continuidad de la seguridad de la información						
14.1.1	Planificación de la continuidad de la seguridad de la información.						
14.1.2	Implantación de la continuidad de la seguridad de la información.						
14.1.3	Verificación, Revisión y evaluación de la continuidad de la seguridad de la información.						

Ítem	Detalle	AÑO 2018				AÑO 2019	
		Enero a marzo	A bril a Junio	Octubre a Diiemb	Octubre a Diciem.	año 2019	año 2019
14.2	redundancias						
14.2.1	Disponibilidad de instalaciones para el procesamiento de la información.						
15	**CUMPLIMIENTO**						
15.1	Cumplimiento de los requisitos legales y contractuales						
15.1.1	Identificación de la legislación aplicable.						
15.1.2	Derechos de propiedad intelectual (DPI).						
15.1.3	Protección de los registros de la organización.						
15.1.4	Protección de datos y privacidad de la información personal.						
15.1.5	Regulación de los controles criptográficos.						
15.2	Revisiones de la seguridad de la información.						
15.2.1	Revisión independiente de la seguridad de la información.						
15.2.2	Cumplimiento de las políticas y normas de seguridad.						
15.2.3	Comprobación y cumplimiento.						