RESOLUCIÓN N° 589 /2021-

"POR LA CUAL SE APRUEBA LA MATRIZ DE IDENTIFICACIÒN Y EVALUACIÒN DE RIESGOS POR OBJETIVOS ESTRÀTEGICOS, DEFINICIÒN DE CONTROLES EXISTENTES Y POLITICAS OPERACIONALES, FORMATOS MECIP N°42 NORMOGRAMA, FORMATO 45 MAPA DE PROCESOS, MANUAL DE COMUNICACIÒN VERSIÒN 3, MANUAL DE CIBERSEGURIDAD VERSIÒN 2, DEL INSTITUTO PARAGUAYO DE TECNOLOGIA AGRARIA (IPTA)"

Asunción, 29 de Diciembre de 2021.-

VISTO: El memorando MECIP N°94/21 presentado por la Coordinación del MECIP, a través del cual, a efectos de consolidar el sistema de control interno de la Institución, solicita la aprobación **LA MATRIZ DE IDENTIFICACIÒN Y EVALUACIÒN DE RIESGOS POR OBJETIVOS ESTRÀTEGICOS, DEFINICIÒN DE CONTROLES EXISTENTES Y POLITICAS OPERACIONALES, FORMATO 42 NORMOGRAMA, FORMATO 45 MAPA DE PROCESOS, MANUAL DE COMUNICACIÒN VERSIÒN 3, MANUAL DE CIBERSEGURIDAD VERSIÒN 2 INSTITUTO PARAGUAYO DE TECNOLOGIA AGRARIA (IPTA)**, y;

CONSIDERANDO: ***Que***, la Resolución CGR N° 425/08 , se establece y adopta el Modelo Estándar de Control Interno para las Entidades Públicas del Paraguay- MECIP como marco para el control, fiscalización y evaluación de los sistemas de control interno de los Sisternas de Control Interno de entidades sujetas a la supervisión de la Contraloría General de la República.

Que, la Resolución CGR N° 377, de fecha 13 de mayo de 2016, adopta como marco para el control, fiscalización y evaluación de los sistemas de control interno de las instituciones, la Norma de Requisitos Mínimos para un Sistema de Control Interno del Modelo Estándar de Control Interno para las Entidades Públicas del Paraguay- MECIP 2015.

Que la Dirección de Asesoría Jurídica, por Memorándum N°212/2.021, de fecha 29/12/2021, con el Exp. MEI N° 107-800-2021, expresa que el mismo se ajusta a derecho, por lo que no encuentra objeciones legales para la emisión de la resolución respectiva y proseguir los trámites administrativos pertinentes, salvo mejor parecer de la Presidencia.

POR TANTO: En uso de las atribuciones y facultades, que le confiere la Ley N° 3.788/10;

...///

RESOLUCIÓN N° 589 /2021-

"POR LA CUAL SE APRUEBA LA MATRIZ DE IDENTIFICACIÒN Y EVALUACIÒN DE RIESGOS POR OBJETIVOS ESTRÀTEGICOS, DEFINICIÒN DE CONTROLES EXISTENTES Y POLITICAS OPERACIONALES, FORMATOS MECIP N°42 NORMOGRAMA, FORMATO 45 MAPA DE PROCESOS, MANUAL DE COMUNICACIÒN VERSIÒN 3, MANUAL DE CIBERSEGURIDAD VERSIÒN 2, DEL INSTITUTO PARAGUAYO DE TECNOLOGIA AGRARIA (IPTA)"

...///

EL PRESIDENTE
DEL INSTITUTO PARAGUAYO DE TECNOLOGÍA AGRARIA (IPTA)
R E S U E L V E:

Artículo 1°.- ***APROBAR,*** **el Anexo que forma parte de la presente resolución que comprende lo siguiente:**

LA MATRIZ DE IDENTIFICACIÒN Y EVALUACIÒN DE RIESGOS POR OBJETIVOS ESTRÀTEGICOS, DEFINICIÒN DE CONTROLES EXISTENTES Y POLITICAS OPERACIONALES, FORMATO 42 NORMOGRAMA, FORMATO 45 MAPA DE PROCESOS, MANUAL DE COMUNICACIÒN VERSIÒN 3, MANUAL DE CIBERSEGURIDAD VERSIÒN 2, DEL INSTITUTO PARAGUAYO DE TECNOLOGIA AGRARIA (IPTA), ajustado a las Normas de Requisitos Mínimos para un Sistema de Control Interno MECIP 2015.

Artículo 2º.- ***DEJAR SIN EFECTO,*** cualquier otro Acto Administrativo anterior a la presente disposición, que se contraponga a lo establecido en ésta.

Artículo 3º.- ***COMUNICAR,*** a quienes corresponda y cumplida archivar.

ES COPIA

Ing. Agr. ***LORENZO MEZA***
Encargado de Despacho - IPTA

IPTA — Instituto Paraguayo de Tecnología Agraria — GOBIERNO NACIONAL — Paraguay de la gente

MODELO ESTÁNDAR DE CONTROL INTERNO - MECIP -

COMPONENTE CORPORATIVO DE CONTROL ESTRATÉGICO

COMPONENTE: DIRECCIONAMIENTO ESTRATÉGICO
ESTÁNDAR: MODELO DE GESTIÓN POR PROCESOS
FORMATO: Mapa de Procesos
Nº: 45 - MP-01 - REV. 02

JERARQUÍA DEL MACRO PROCESO	1) NOMBRE MACROPROCESOS	2) NOMBRE PROCESOS	3) NOMBRE SUBPROCESOS
ESTRATÉGICO	1. Direccionamiento y Organización Institucional *(DO-00-00-00-01)*	1.1. Planificación Estratégica *(DO-PL-00-00-01)*	1.1.1. Planificación Estrátegica *(DO-PL-PEI-00-01)*
			1.1.2. Estructura Organizacional y funciones *(DO-PL-EO-00-01)*
		1.2. Planificación Operativa *(DO-PO-00-00-01)*	1.2.1. Planificación Operativa *(DO-PO-POI-00-01)*
			1.2.2. Seguimiento y Evaluación a Planes Institucionales *(DO-PO-SE-OO-01)*
			1.2.3. Elaboración y seguimiento de Proyectos de Investigación *(DO-PO-EP-00-01)*
MISIONAL	2. Generación de Conocimiento y tecnología para la innovación agraria *(CO-00-00-00-01)*	2.1. Investigacion y Desarrollo de Conocimientos y Tecnologias innovadoras *(CO-TL-00-00-01)*	2.1.1. Gestion de Transferencia y Tecnologia *(CO-TL-TT-00-01)*
	3. Transferencia y Difusión de Tecnologia *(TD-00-00-00-01)*	3.1. Transferencia y y difusion de resultados de investigación agraria *(TD-DR-00-00-01)*	3.1.1. Gestión de Transferencia y difusión *(TH-DR-TT-00-01)*
	4. Servicios Tecnologicos *(ST-00-00-00-01)*	4.1. Gestión de Negocios y Servicios Tecnologicos *(ST-NS-00-00-01)*	4.1.1. Negocios y Servicios Tecnológicos *(ST-NS-NG-00-01)*
	5. Género y Juventud Rural *(RU-00-00-00-01)*	5.1. Gestión de Genero y Juventud Rural *(RU-JV-00-00-01)*	5.1.1. Gestión de la Investigación e Innovación para el Desarrollo Rural (RU-JV-DR-00-01)
ESTRATÉGICO	6. Gestión de Comunicación e Información *(CGI-00-00-00-01)*	6.1. Establecimiento de la Politica de Comunicación de la Institución *(GCI-EP-00-00-01)*	6.1.1. Diseño de la Imagen Institucional *(GCI-EP-DI-00-01)*
			6.1.2. Gestión de Monitoreo y Evaluación General *(GCI-EP-ME-00-01)*
			6.1.3. Gestión de la Planifiación para la Implementación *(GCI-EP-PM-00-01)*
			6.1.4. Implementación de Control Estrátegico *(GCI-EP-CE-00-01)*
			6.1.5. Implementación de Control de Gestión *(GCI-EP-CG-00-01)*
			6.1.5. Implementación de Control de Evaluación *(GCI-EP-EV-00-01)*
		6.2. Diseño e Instalacion del Plan de Comunicación Institucional *(GCI-DE-00-00-01)*	6.2.1. Elaboración de Información Interna y Externa *(GCI-DE-IE-00-01)*
			6.2.2. Produccion de Materiales de Comunicación *(GCI-DE-MC-00-01)*

INSTITUTO PARAGUAYO DE TECNOLOGIA AGRARIA

MANUAL DE COMUNICACIÓN INSTITUCIONAL VERSION 3

Año 2021

1. POLÍTICA DE COMUNICACIÓN INSTITUCIONAL

En el INSTITUTO PARAGUAYO DE TECNOLOGIA AGRARIA (IPTA), la comunicación está orientada a fortalecer las gestiones institucionales mediante acciones estratégicas, dirigidas a los usuarios internos y externos atendiendo la Misión, Visión y Objetivos Estratégicos institucionales.

1.1 POLITICA DE ALINEAMIENTO ESTRATEGICO

La Política de Comunicación del IPTA, se encuentra acorde con la Misión, Visión y Objetivos Estratégicos de la institución, y la difusión interna y externa se realizará a través de un **Plan de Comunicación.**

LINEAMIENTO 1: PLANEACIÓN DE LA COMUNICACIÓN

Se elaborará un Plan de Comunicación para coordinar, ejecutar, verificar y evaluar las acciones comunicativas.

Orientaciones

1) Para la obtención del Plan de Comunicación, la Dirección de Comunicación Institucional ejecutará un "diagnóstico" del estado de la Comunicación Institucional que le servirá como línea de base para orientar su elaboración.
2) El diagnóstico se realizará por medio de encuestas, entrevistas y observación.
3) El Plan de Comunicación establecerá las distintas estrategias a ejecutar con el fin de alcanzar los objetivos comunicacionales propuestos, además de las acciones para la correcta aplicación de la comunicación interna y externa.
4) El Plan de Comunicación será aprobado por Resolución Institucional para su implementación.
5) La Dirección de Comunicación Institucional, será la encargada de socializar el Plan de Comunicación con todas las dependencias del IPTA.

Lic. Zarmina Martínez
Directora
Dirección de Comunicación
IPTA

LINEAMIENTO 2: INDUCCION DE LOS SERVIDORES PUBLICOS

El IPTA desarrollará procesos dinámicos de inducción, se buscará lograr la integración, la adhesión de la cultura y las normas institucionales y el logro de la estrategia de la Institucion del nuevo servidor público. El proceso de Inducción estará a cargo de la Dirección de Gestión y Desarrollo de las Personas con apoyo de la Dirección de Comunicación Institucional.

Orientaciones

La Dirección de Gestión y Desarrollo de las Personas con apoyo de la Dirección de Comunicación Institucional prepararán los materiales a ser distribuidos en el momento de la inducción.

La Dirección de Gestión de y Desarrollo de las Personas y la Dirección de Comunicación Institucional designarán funcionarios/as que realizarán el debido proceso de inducción.

1) Los servidores públicos que ingresan a la institución recibirán la inducción, que incluirá la socialización de la estructura organizacional, el reglamento interno de la institución y los beneficios que le corresponden, además de la visión, los objetivos y valores éticos de la institución.
2) Concluido el proceso de inducción, el funcionario/a designado por la Dirección de Gestión y Desarrollo de las Personas acompañará al nuevo servidor público a conocer la Sede Institucional y lo presentará a la dependencia en donde prestará servicios.

LINEAMIENTO 3: REINDUCCIÓN DE LOS SERVIDORES PÚBLICOS

La reinducción estará dirigida a reorientar la integración de todos los funcionarios públicos a la cultura organizacional en virtud a los cambios producidos dentro de la institución, se realizará en forma anual o de acuerdo a la necesidad que se presente.

Orientaciones

1) La Dirección de Gestión y Desarrollo de las Personas con apoyo de la Dirección de Comunicación Institucional prepararán los materiales a ser distribuidos en el momento de la reinducción.
2) La Dirección de Gestión y Desarrollo de las Personas y la Dirección de Comunicación Institucional designarán funcionarios/as que realizarán el debido proceso de reinducción.
3) Se buscará la motivación, sensibilización, actualización y reorientación a la cultura institucional del servidor público, informándole anualmente o cuando la situación lo requiera, sobre las estrategias (visión, misión, valores éticos, políticas y objetivos institucionales) y los resultados de la gestión institucional.

LINEAMIENTO 4: DIFUSIÓN DE LA INFORMACIÓN

Se dará prioridad a la difusión de la información institucional de interés a servidores públicos y ciudadanía en general, a través de recursos tecnológicos disponibles.

Orientaciones

Directora
Dirección de Comunicación
IPTA

1) La Dirección de Comunicación Institucional, difundirá a través de la Página Web y otros medios , las Leyes, Decretos, Resoluciones y otras Normativas de carácter general.
2) La institución, por medio de las dependencias responsables, darán cumplimiento en tiempo y forma, de la elaboración y remisión de informes a los organismos competentes y de control de conformidad a las leyes y reglamentaciones vigentes.
3) Las dependencias deberán remitir a la Dirección de Comunicación Institucional periódicamente informaciones de las actividades y avances que consideren deban ser difundidos, para que ésta determine su forma de difusión atendiendo a los objetivos estratégicos institucionales.
4) La Dirección de Comunicación Institucional difundirá constantemente las informaciones de interés, a los servidores públicos de la Institución.

1.2 POLITICA DE LA PROMOCIÓN DE BUEN SERVICIO E IMAGEN CORPORATIVA

Se promoverá la capacitación y entrenamiento de los servidores públicos, para que brinden atención con calidad y calidez a los usuarios (internos y externos), contribuyendo al cumplimiento de la misión institucional y proyectando una imagen favorable basada en la calidad de los servicios.

LINEAMIENTO 1: CAPACITACION PARA EL BUEN SERVICIO

Se promoverá la capacitación y entrenamiento de los servidores públicos en las buenas prácticas para una atención eficaz y eficiente y proyectando así una imagen positiva.

Orientaciones

1) La Dirección de Gestión y Desarrollo de las Personas incluirá en su plan anual de capacitación Programas de capacitación y entrenamiento para el óptimo desempeño de los Servidores Públicos, acorde a la Política de Comunicación de la Institución.
2) La Dirección de Comunicación Institucional, promocionará el Programa de capacitación elaborado por la Dirección de Gestión y Desarrollo de las Personas.
3) La elaboración de los procedimientos para la correcta ejecución, evaluación y control de la capacitación, será responsabilidad de la Dirección de Gestión y Desarrollo de las Personas.
4) La Dirección de Gestión y Desarrollo de las Personas, será responsable de la consolidación y elaboración de un informe de las capacitaciones realizadas, y remitirá a la Dirección de Comunicación Institucional.

LINEAMIENTO 2: RECONOCIMIENTO Y DESEMPEÑO DE LOS SERVIDORES PÚBLICOS

Se reconocerá el buen desempeño de los servidores públicos que demuestren, la ética profesional, el sentido de pertenencia y el compromiso con la Institución.

Lic. Carmiña Martínez
Directora
Dirección de Comunicación
IPTA

Orientaciones

1) La Dirección de Gestión y Desarrollo de las Personas elaborará un Programa de Reconocimiento para Servidores Públicos.
2) La Dirección de Comunicación Institucional apoyará en la difusión del proceso e implementación del Programa de Reconocimiento para Servidores Públicos.

LINEAMIENTO 3: PROYECCIÒN DE LA IMAGEN CORPORATIVA

La Dirección de Comunicación Institucional implementará acciones que promuevan el fortalecimiento de la imagen institucional, con base a su Misión y sus Objetivos Estratégicos.

Orientaciones

1) La Dirección de Comunicación Institucional, actualizará y evaluará constantemente los materiales de la institución que se difundirán.
2) El IPTA establecerá el Manual de Imagen en una herramienta para el manejo de las directrices de presentación de los mensajes institucionales, como medio para garantizar el respeto y la promoción de la identidad de la institución , en cada uno de los programas de información.
3) El IPTA utilizara el Manual de Imagen ,para facilitar a nivel global todo lo concerniente a la institución ,reseña histórica, objetivos del programa, vocabulario, signos de identidad, emblema, símbolo, logotipo ,gama cromática, Normas Básicas: Disposición formal de los colores, Control de un solo color, Control de diapositivas, Negro y Escalas de grises, Control de proporción, Normas tipográficas, Normas complementarias: Control de sombras, Control de rotación, Control de deformación, Aplicaciones, Papelería, Papelería administrativa, Indumentaria, Fachada,etc.
4) Tanto el logo símbolo, como el eslogan del IPTA, primarán sobre toda identificación particular de las dependencias, programas, proyectos, campañas y de otras instituciones.
5) La Dirección de Comunicación Institucional establecerá el Manual de Imagen y marca en una herramienta para el manejo de las directrices de presentación de los mensajes institucionales, como medio para garantizar el respeto y la promoción de la identidad de la institución, en cada uno de los programas de información
6) Los Directores/as Generales y demás Directores/as serán responsables de la correcta utilización del logos, símbolos y el slogan del Instituto.
7) Los Directores/as serán responsables de la señalización adecuada de todas las áreas de sus dependencias, para facilitar el acceso de los usuarios a los servicios que ofrece la institución.

1.3 POLITICA DE RECEPTIVIDAD INSTITUCIONAL

Habrá un Responsable designado por la Dirección de Comunicación Institucional, encargado de promover la recepción de sugerencias, comentarios, quejas, reclamos y

Lic. Carmina Martin
Directora
Dirección de Comunicac
IPTA

propuestas del servidor público y del ciudadano. La Dirección de Comunicación Institucional será la encargada de canalizar y dar providencia a lo recibido.

LINEAMIENTO 1: RECEPTIVIDAD INTERNA

Orientado hacia los propios servidores públicos, a fin de garantizar la canalización efectiva de las inquietudes presentadas.

Orientaciones

1) Para recibir sugerencias se habilitará buzones, en Mesa de Entrada del IPTA (Recepción – Asunción), en la Dirección Nacional (San Lorenzo), cada sede del interior del país; se habilitará una línea telefónica y una dirección de correo electrónico.
   Se habilitará en Mesa de entrada y en la Página web del IPTA un buzón de sugerencias, quejas y reclamos, se pondrá a disposición de los interesados, público interno o externo un formulario en el cual podrán expresar sus inquietudes. Los documentos depositados en el buzón de sugerencias serán retirados periódicamente por la Dirección de Comunicaciones, direccionados al cómite de rendición de cuenta y a las instancias correspondientes.
2) En el caso de las quejas y denuncias contra algún servidor público en particular el proceso de las mismas se describe en los Artículos 24° al 40° del Código de Buen Gobierno y la misma hace referencia en el Código de Ética de nuestra institución como guía del comportamiento ético de los servidores públicos de ésta institución . Las decisiones finales tomadas por el Comité de Ética con respecto al servidor público, serán enviadas a la Dirección de Gestión y Desarrollo de las Personas para el archivo en su legajo y a la Dirección de Comunicación Institucional para su difusión.
3) Los Jefes/as y Directores/as tendrán la responsabilidad de reportar por escrito al Responsable designado por la Dirección de Comunicación Institucional o al Comité de Rendición de Cuentas, las sugerencias que reciban de sus colaboradores en sus reuniones de trabajo, en los buzones instalados en mesa de entrada y en la página web del IPTA, y/o cualquier otro tipo de situación que consideren pertinente al caso.
   La Dirección de Comunicaciones hará un monitoreo periódico de los medios escritos, identificando y compilando informaciones relevantes para la institución. Asimismo mantendrá informada a la Máxima Autoridad y a los funcionarios del IPTA
4) Cada mes el Responsable designado, presentará a la Dirección de Comunicación Institucional un reporte consolidado de la información recibida, a fin de canalizarlas, para la toma de decisiones y brindar soluciones para el mejoramiento institucional.
5) Las respuestas ante las inquietudes y las decisiones que se tomen, serán difundidas por la Dirección de Comunicación Institucional destacando las soluciones brindadas.

Lic. Carmina Martin
Directora
Dirección de Comunicaci
IPTA

LINEAMIENTO 2: RECEPTIVIDAD EXTERNA

Estará orientada al Sector Externo, con apertura hacia la sociedad, a través de la recepción de inquietudes y requerimientos de los ciudadanos.

Orientaciones

1) Para recibir sugerencias se habilitará buzones, en Mesa de Entrada del IPTA (Recepción – Asunción), en la Dirección Nacional (San Lorenzo), cada sede del interior del país, se habilitará una línea telefónica y una dirección de correo electrónico, para recibir las sugerencias, comentarios, quejas y reclamos de los ciudadanos.
2) Cada mes el Responsable designado, presentará a la Dirección de Comunicación Institucional un reporte consolidado de la información recibida, a fin de canalizarlas, para la toma de decisiones y brindar soluciones para el mejoramiento institucional.
3) Las respuestas ante las inquietudes y las decisiones que se tomen, serán difundidas por la Dirección de Comunicación Institucional destacando las soluciones brindadas.

2. COMUNICACIÓN PÚBLICA

La Comunicación Pública de la Institución estará orientada a la interacción, el fortalecimiento, la credibilidad y la confianza hacía los diferentes grupos de interés, a través del manejo fluido y responsable de la información, como elemento indispensable para la trasparencia de sus acciones, para que estos a su vez faciliten el cumplimiento de los objetivos del IPTA.

2.1 INTEGRACION Y SISTEMATIZACION DE LA INFORMACION

La integración de la información será responsabilidad de la Dirección de Comunicación Institucional, quien dará directrices claras para la recolección, sistematización, clasificación de la información provenientes de las diferentes áreas del IPTA, buscando unificación en el manejo y una adecuada administración.

LINEAMIENTO 1: MANEJO INTEGRADO DE LA INFORMACION

La información es claramente identificada, recolectada y registrada según datos dados por las dependencias del IPTA, en función a los lineamientos dictados por la Dirección de Comunicación Institucional.

Orientaciones

1) El Director/a de Comunicación Institucional designará un representante, quien será el responsable de solicitar y recepcionar las informaciones de las diferentes áreas y establecerá mecanismos de recolección de información y los plazos a ser presentados.
2) Cada dependencia designará a un representante para la integración de la información y será el nexo con el representante de la Dirección de Comunicación Institucional.

Lic. Carolina [illegible]
Directora
Dirección de Comunic.
IPTA

3) La información a ser publicada por los medios de prensa, deberán ser comunicadas a la Dirección de Comunicación Institucional, por lo menos con dos días de anticipación, teniendo en cuenta la fecha, hora, lugar del evento, responsables, programas, salvo en caso de casos de urgencia.
4) Cualquier información a ser publicada deberá ser revisado y aprobado por el Director/a de la Comunicación Institucional antes del envío a los medios masivos de comunicación.

LINEAMIENTO 2: SISTEMATIZACION DE LA INFORMACION

Utilizar los recursos informáticos para la sistematización de la información institucional, a fin de simplificar los procesos de obtención y publicación de la información.

Orientaciones

1) Implementación de un Programa Informático para una adecuada sistematización y consolidación de información de todas las dependencias del IPTA. (ZIMBRA)
2) Implementación de un sistema informático para el seguimiento de documentaciones, tanto interno como externo (Intranet).
3) Sistematización de todas las disposiciones internas y externas relacionadas a la institución.
4) Capacitación para la implementación de los sistemas.
5) Sistematización de todas las disposiciones internas y externas relacionadas a la institución.
6) Facilitar acceso a internet, intranet, otros.
7) Actualización permanente del sistema informático.

2.2 MANEJO DE LA INFORMACIÓN

Entendida como soporte indispensable para el mejoramiento de la comunicación institucional, una vez clasificada, sistematizada y establecida como pública, se dará a conocer en forma oportuna y servirá como base para elaborar materiales informativos y educativos para los diversos grupos de interés, que a la vez dará trasparencia a la gestión.

LINEAMIENTO 1: RELACIONAMIENTO CON LOS GRUPOS DE INTERES

El IPTA en su política de apertura a los grupos de interés, se basará en la imparcialidad y equidad en el manejo de la difusión de la información, excepto aquellos casos que se considere de carácter reservado, atendiendo a las características específicas de cada grupo en un marco de confianza y colaboración.

Orientaciones

1) La Dirección de Comunicación Institucional será el canal de difusión a los diferentes grupos de interés.

Lic. Carmina Martínez
Directora
Dirección de Comunicación
IPTA

2) Todas las actividades donde tenga participación el IPTA, ya sean nacionales, internacionales, internas, deberán ser canalizadas a través de la Dirección de Comunicación Institucional.
3) Todas las dependencias, del IPTA proveerán a la Dirección de Comunicación Institucional, la información que deba comunicarse, según los lineamientos de este manual.
4) La Dirección de Comunicación Institucional, tendrá la responsabilidad de hacer los ajustes necesarios de la información recepcionada, de acuerdo al estándar establecido
5) La Dirección de Comunicación Institucional será la asesora a las diversas instancias sobre estrategias a ser utilizados en la elaboración de materiales informativos.
6) La Dirección de Comunicación Institucional en coordinación con la Dirección de TICS, actualizará diariamente la página web del IPTA, considerando el interés colectivo y respetando la confidencialidad.
7) La Dirección de Comunicación Institucional remitirá al Presidente del IPTA, un informe consolidado diariamente o según requerimiento del mismo.

LINEAMIENTO 2: RELACIONAMIENTO CON LOS MEDIOS DE COMUNICACIÓN

La Dirección de Comunicación Institucional fomentará una política de apertura y de buen relacionamiento con los medios de comunicación masivos, tanto a nivel nacional e internacional para satisfacer las demandas y la difusión estratégica de la información institucional.
Las demandas de los medios de comunicación y los requerimientos institucionales exigen una adecuada coordinación para dar satisfacción a las partes, ya sea para entrevistas con periodistas, convocatorias de prensa, preparación de eventos con los medios, así como la distribución de informes.

Orientaciones

1) La Dirección de Comunicación Institucional es el responsable de la coordinación y convocatorias de los medios de comunicación para la realización de entrevistas, ruedas de prensa, etc., con autoridades de la institución.
2) Las ruedas de prensa y reuniones informales serán realizadas dentro de la institución, cuando las autoridades del mismo consideren necesario comunicar e informar a la ciudadanía sobre algún acontecimiento de interés general, postura sobre un tema determinado, responder a denuncias, entre otros aspectos.
3) Las entrevistas y reportajes concedidos a medios de comunicación, se enfocará siempre hacía el logro de un mejor posicionamiento de la entidad.
4) Todos los servidores públicos del IPTA que necesiten comunicar algo a la ciudadanía, necesariamente deberán recurrir a la Dirección de Comunicación Institucional para recibir una orientación profesional antes de hacerlo. El objetivo es mantener la coherencia en los mensajes que se emiten institucionalmente.

ES COPIA

Lic. Carmiña Martínez
Directora
Dirección de Comunicación
IPTA

LINEAMIENTO 3: PROVISIÓN DE LA INFORMACIÓN

Los materiales de información, elaborados y producidos para publicaciones de todas las dependencias, serán remitidas previamente a la Dirección de Comunicación Institucional para su verificación, adecuación correspondiente.

Orientaciones

1) Se emitirán Boletines de Prensa precisas cuando la situación así lo requiera sobre las acciones y actividades de la institución, de manera a que la información esté disponible para la ciudadanía en general y los diferentes grupos de interés. Estas deberán ajustarse a los criterios de responsabilidad en el manejo de la información.
2) Los boletines de prensa también serán difundidos a través de correos institucionales, correos privados, notas, memos, circulares, etc., para la comunicación.

LINEAMIENTO 4: VOCERO INSTITUCIONAL

El IPTA contará con servidores públicos de buen nivel que actuarán de voceros para dirigirse a la sociedad ya sea en forma directa o a través de medios de comunicación, tanto en encuentros nacionales e internacionales.

Orientaciones

1) El Presidente del IPTA será en todo momento el portavoz oficial y principal de la institución, dentro y fuera del país.
2) La Dirección de Comunicación Institucional podrá actuar de vocero institucional para la difusión ordinaria de información, de serle asignada esta función por la máxima autoridad.
3) Los Directores/as Generales son funcionarios del alto rango autorizados para dirigirse a la opinión pública cuando lo consideren oportuno, salvo mejor criterio de la alta autoridad institucional.
4) Ningún servidor público está autorizado a dar a conocer a la ciudadanía información que pueda perjudicar la imagen de la institución.

LINEAMIENTO 5: CLASIFICACION DE LA INFORMACION

La información será consolidada y sistematizada previa clasificación. La confidencialidad de cierta información tendrá como fin asegurar el cumplimiento de los objetivos de la institución y en ningún caso servirá para obstaculizar la transparencia de la gestión del IPTA.

Orientaciones

Lic. Carmina Martínez
Directora
Dirección de Comunicación
IPTA

1) El interés general prevalecerá siempre sobre el interés particular para la difusión pública de una información.
2) Ningún servidor público podrá utilizar ni retener información de la institución para la consecución de fines personales, de grupos o sectores.
3) Todos los servidores públicos respetarán los criterios establecidos para el manejo de información del IPTA, en especial la de carácter confidencial, incluso fuera de sus actividades laborales.

2.3 RELACIONAMIENTO CON LOS MEDIOS DE COMUNICACIÓN

El IPTA establecerá un buen relacionamiento con los medios de Comunicación, para posicionar a la institución y fortalecer el conocimiento de los procesos de la entidad y a la apropiación de los mismos por parte de los servidores públicos y el público en general. La finalidad es conseguir una mayor cobertura y repercusión mediática de las actividades desarrolladas.

LINEAMIENTO 1: ESTRATEGIA Y CLASIFICACION DE LOS MEDIOS DE COMUNICACIÓN

La Dirección de Comunicación Institucional actuará de enlace formal entre las autoridades del IPTA y los medios de Comunicación y será definida de acuerdo con las estrategias de la proyección de imagen corporativa, de difusión de gestiones de la institución y de los resultados.

Orientaciones

1) La Dirección de Comunicación Institucional definirá las estrategias comunicacionales y solicitará a la máxima autoridad el nombramiento de voceros/os institucionales para la difusión de la información.
2) La Dirección de Comunicación Institucional, al principio de cada año definirá un Plan Anual de Medios y acciones comunicativas, para mejor direccionamiento de la información.
3) Los contenidos comunicacionales tendrán uniformidad de criterios para la producción de las publicaciones de la entidad, así como la utilización de mensajes y lenguajes adecuados al objetivo de la comunicación.
4) La Dirección de Comunicación Institucional clasificará y calificará la información a ser publicada en función a estándares establecidos en el Plan de Comunicación, el Plan de Medios y directrices del Presidente.

LINEAMIENTO 2: RELACIONAMIENTO CON LOS MEDIOS DE COMUNICACIÓN

Lic. Carolina Mar...
Directora
Dirección de Comunica...
IPTA

La Dirección de Comunicación Institucional actuará de enlace formal entre autoridades ministeriales, medios de comunicación y definirá los canales correspondientes para la entrega de la información.

Orientaciones

1) El Presidente es el principal vocero institucional. El carácter de Directivo dependiente de los Direcciones Generales implicará la responsabilidad de oficiar como vocero técnico en temas que competen a su área, salvo mejor criterio de la máxima autoridad.
2) El Encargado de Despacho del IPTA es quien reemplazará al Presidente como vocero principal en casos de urgencia o ausencia temporal del país.
3) El Director/a de Comunicación Institucional podrá actuar de vocero institucional para la difusión ordinaria de la información, de serle asignada esta función por la máxima autoridad institucional.
4) Los Directores/as Generales son funcionarios del alto rango autorizados para dirigirse a la opinión pública cuando lo consideren oportuno, salvo mejor criterio de la alta autoridad institucional.
5) Los voceros autorizados será los responsables de defender la posición institucional sobre un tema determinado y sencillamente hacer una aclaración.
6) Ningún servidor público está autorizado a dar a conocer, tanto a medios de comunicación y ciudadanía en general, información que pueda dañar la imagen de la entidad o de los intereses institucionales.

LINEAMIENTO 3: INTERACCION CON LA CIUDADANIA

La comunicación con la ciudadanía y usuarios de los servicios que presta el IPTA, estará centrada en construir una relación cercana con los mismos, pues constituye uno de los pilares básicos de la Administración. La atención a la ciudadanía pone en marcha una serie de actuaciones:

- Web/Internet.
- Buzones de sugerencias, quejas y reclamos
- Teléfonos de Información.
- Otros.

Orientaciones

1) Mantener actualizada la página web institucional www.ipta.gov.py puesta a disposición de la ciudadanía, en la misma se orientará acerca de trámites y procesos administrativos, se dispondrá de informaciones básicas referente a las dependencias del IPTA.
2) La Ventana de Acceso a la Información, se actualizara y ajustará en cuanto a su eficiencia y funcionamiento.

LINEAMIENTO 4: MONITOREO DE MEDIOS DE COMUNICACIÓN

Lic. Martínez
Directora
Dirección de Comunicación
IPTA

Se realizará un seguimiento de la información emitidas por los medios de comunicación, sean estos, impresos, radiales, televisivos y electrónicos para su análisis.

Orientaciones

1) La Dirección de Comunicación Institucional será responsable del monitoreo diario de medios de Comunicación, sobre temas que conciernen a la institución.
2) Monitorear la información que manejan las Redes Sociales del IPTA.
3) Analizar la tendencia de la información de acuerdo al medio informativo.
4) Emitir informes sobre el monitoreo diario para que pueda ser utilizado en toma de decisiones.
5) Realizar una medición de la información de los medios impresos –diarios- para su posterior análisis.
6) Elaborar un reporte de medios electrónicos para su análisis.
7) La Dirección de Comunicación Institucional contará con un sistema de monitoreo de las emisiones radiales y televisivas, de forma diaria y permanente.
8) La Dirección de Comunicación Institucional copilará las publicaciones de medios en general sobre la Institución y áreas que le competen.
9) La Dirección de Comunicación Institucional, archivará en forma impresa y digital si fuere necesario, todas las publicaciones de prensa escrita, radial y televisiva.
10) Todas las informaciones copiladas referentes a la institución serán remitidas diariamente al Presidente, Directores/as Generales, otros.

3. POLITICA DE RENDICION DE CUENTAS

La Rendición de Cuentas se realiza a fin de brindar transparencia a la sociedad, propiciar condiciones de confianza entre autoridades y la ciudadanía, y garantizar transparencia en la gestión.

3.1 POLITICA DE ADECUACION INSTITUCIONAL PARA LA RENDICION DE CUENTAS

En el marco de la Rendición de Cuentas como deber del Estado y derecho del ciudadano, y en cumplimiento de los principios de la función pública y la participación social, se deberá adoptar un **Programa de Rendición de Cuentas** buscando dar transparencia a la gestión y generar confianza y credibilidad en la ciudadanía. Ello implica una adecuación institucional para la realización de la Audiencia Pública de Rendición de Cuentas y se deberá evaluar los resultados de la presentación realizada.

LINEAMIENTO 1: CONFORMACION DEL COMITÉ TECNICO DE RENDICION DE CUENTAS

El Comité de Rendición de Cuentas estará conformado por: la Dirección de Transparencia y Anticorrupción (Unidad Impulsora),Dirección de Gabinete, Dirección de Planificación, Dirección de Administración y Finanzas, Dirección de Comunicación, Dirección de

Directora
Dirección de Comunicación
IPTA

Tecnología de la Información y Comunicación , Auditoría Interna Institucional, Direcciones con funciones misionales.

Orientaciones

1) Se conformará mediante una resolución, el equipo de Comité Técnico de Rendición de Cuentas, este Comité será el encargado de la planificación, evaluación y control de la Rendición de Cuentas a la Ciudadanía. La Dirección de Transparencia y Anticorrupción deberá liderar la elaboración del informe de Rendición de Cuentas.
2) En la Resolución de conformación del comité se deberá incluir la fecha tope de presentación de las conclusiones de la elaboración del informe de Rendición de Cuentas y el probable mes de realización de la Audiencia Pública para poner a conocimiento de la ciudadanía los resultados de la gestión.
3) El Comité Técnico de Rendición de Cuentas planificará las actividades y elevará a la Máxima Autoridad institucional, la propuesta de la Rendición de Cuentas del año deberá ser aprobado antes de la finalización del mes de febrero, de modo tal que se encuentre vigente operativamente en el mes de marzo, mes en que se elaborará el informe trimestral donde se comunicará a la ciudadanía sobre la conformación del CRCC, el plan de metas para el año en curso y las actividades ya realizadas hasta la fecha.
4) El Comité Técnico de Rendición de Cuentas valiéndose de todos los informes recogidos (informes parciales) y acciones realizadas en el marco del Plan de Rendición de Cuentas, iniciará el proceso de elaboración del informe final de rendición de cuentas, en el mes de diciembre de documento generado con las informaciones recepcionadas de las diferentes áreas de la Institución para el análisis e interpretación de la información.-

LINEAMIENTO 2: ELABORACION DEL INFORME DE RENDICION DE CUENTAS

En base a las informaciones recibidas de las áreas involucradas se elaborará el **Informe de Rendición de Cuentas**, dirigido a los servidores públicos, a los grupos de interés y a la ciudadanía.

Orientaciones

1) Una vez conformado el Comité Técnico de Rendición de Cuentas, los integrantes deben tomar conocimiento de la resolución y su alcance.
2) La Máxima Autoridad institucional designará a la Dirección de Transparencia y Anticorrupción, como responsable de Impulsar el inicio del proceso de rendición de cuentas al ciudadano, y la internalización del modelo y los lineamientos estandarizados.
3) El Comité deberá identificar etapas e hitos en el marco del desarrollo del año y preparar las capacidades institucionales del año para los actos y actividades de rendición de cuentas anuales.
4) El Comité, con el apoyo de y liderazgo específicos de la Dirección de Planificación y la Dirección de Gabinete, deberá identificar las áreas de acción institucional que por

Lic. Carmina Martínez
Directora
Dirección de Comunicación
IPTA

diversos motivos, constituyen prioridades para la rendición de cuentas del año respectivo.

5) El Comité Técnico solicitará y recibirá todas las informaciones que serán utilizadas para la elaboración del Informe de Rendición de Cuentas, cada dependencia institucional deberá reportar informe trimestralmente conforme al plan elaborado por el comité en los periódos comprendidos del primer, segundo y tercer trimestre del año que contemplen los informes seleccionados del área (misionales, administrativas y de apoyo) en informes parciales que serán publicados conforme al siguiente listado:
   Primer Informe Parcial : Marzo
   Segundo Informe parcial: Junio
   Tercer Informe Parcial:Setiembre
6) El Comité Técnico analizará, clasificará e interpretará la información conforme a indicadores de evaluación y a temas prioritarios a incluir en el Informe de Rendición de Cuentas.
7) El Comité elaborará informes de Rendición de Cuentas que podrán ser utilizados en el procedimiento de reinducción a los servidores públicos. Además deberá presentar un Informe Anual que se presentará en las audiencias públicas de Rendición de Cuentas a la ciudadanía y a grupos de interés.
8) El Informe de Rendición de Cuentas deberá ser elaborado en un lenguaje accesible al ciudadano en formatos que faciliten su comprensión y visualización (gráficos, afiches, vídeos, revistas, etc.),deberán prever mecanismos para que sean inclusivo, teniendo en consideración especial al bilingüismo (castellano y guaraní)
9) Una vez elaborado el Informe de Rendición de Cuentas, y con la aprobación del Presidente, el Comité lo entregará a la Dirección de Comunicación Institucional, para que disponga la impresión e implemente mecanismos de difusión.
10) CRCC designará un funcionario/a quien será responsable de la recepción y guarda de los Informes de Rendición de Cuentas impresas, tales reportes al igual que los informes parciales trimestrales serán acompañadas de las evidencias respectivas y serán publicadas por los conductos que serán habilitados para tal efecto, en base a las indicaciones de la SENAC
11) El funcionario/a designado será responsable de entregar copias de Informes de Rendición de Cuentas, a los participantes de la Audiencia Pública de Rendición de Cuentas y a los servidores públicos en el procedimiento de re inducción.
12) El CRCC deberá evaluar, durante cada trimestre, la información compilada de los canales habilitados para la ciudadanía (encuestas, buzones de sugerencias, redes sociales, entrevistas, etc)

3.2 POLITICA DE AUDIENCIAS PÚBLICAS PARA LA RENDICION DE CUENTAS

A fin de intercambiar información, brindar explicaciones, evaluaciones y propuestas con los diferentes grupos de interés, organizaciones de la sociedad civil y los ciudadanos acerca del manejo de los recursos públicos utilizados para cumplir con la ejecución de los programas y

Lic. Carmiña Martínez
Directora
Dirección de Comunicación
IPTA

el logro de los objetivos tratados, se requerirá de estrategias de comunicación, campañas de promoción y convocatoria para la realización de las Audiencias Públicas de Rendición de Cuentas a la Ciudadanía. Además se deberá elaborar el Reglamento de la Audiencia Pública.

LINEAMIENTO 1: DISEÑO Y ELABORACION DEL REGLAMENTO DE RENDICION DE CUENTAS

Se deberá convenir las bases y condiciones, estrategias comunicacionales, campañas de promoción y convocatoria necesarias para la realización de la Audiencia Pública de Rendición de Cuentas.

Orientaciones

1) El Comité deberá elaborar el Reglamento de Rendición de Cuentas
2) El Reglamento deberá contener las Bases y Condiciones para asistir y participar de la Audiencia Pública, diseñar los formularios y documentos que se requiera para el evento
3) La Dirección de Comunicación Institucional será la encargada de diseñar los dispositivos de comunicación (imagen, logos, materiales de apoyo, espacios en los medios de prensa, plan de medios, diseños de gráficos, demos, etc.) en formatos de fácil comprensión para el ciudadano.

LINEAMIENTO 2: ORGANIZACIÓN LOGISTICA DE LA AUDIENCIA PÚBLICA DE RENDICION DE CUENTAS

La organización y logística para la realización de la Audiencia de Rendición de cuentas a la Ciudadanía será responsabilidad del Comité Técnico en conjunto con la Dirección de Comunicación Institucional

Orientaciones

1) El Comité Técnico de Rendición de Cuentas en conjunto con la Dirección de Comunicación Institucional serán los responsables de la logística, definir el lugar, la fecha y hora así como la duración de la audiencia de rendición de cuentas.
2) El Comité Técnico de Rendición de Cuentas deberá prever el número aproximado de participantes y dentro de lo posible confirmar la asistencia de los invitados.
3) El Comité Técnico de Rendición de Cuentas en conjunto con la Dirección de Comunicación Institucional deberán prever las necesidades de suministros (refrigerio, equipos informáticos, de comunicación micrófonos, etc.) para el adecuado desarrollo de la Audiencia.

LINEAMIENTO 3: INVITACIONES PARA LA PARTICIPACION EN LA AUDIENCIA PÚBLICA DE RENDICION DE CUENTAS

Lic. Carmiña Mari...
Directora
Dirección de Comunicaci...
IPTA

Para asegurar la participación de las partes interesadas, se confeccionará, entregará y socializará invitaciones a las autoridades nacionales, representantes de entidades, personas naturales y jurídicas en general.

Orientación

1) La Dirección de Comunicación Institucional será la encargada de promocionar por lo menos con 30 días de anticipación la realización de la Audiencia Pública de Rendición de cuentas.
2) El Comité Técnico de Rendición y la Dirección de Comunicación Institucional serán los encargados de diseñar las invitaciones para la Audiencia Pública de Rendición de Cuentas.
3) La convocatoria a la ciudadanía en general podrá realizarse a través de la WEB institucional, medios de prensa, etc., mencionando que la información sobre la institución figura en la página web para las consultas
4) Se deberán confeccionar formularios de evaluación de satisfacción y sugerencias a ser distribuidos a los destinatarios de la rendición, a fin de medir la efectividad y la mejorar la planificación de otras actividades.

LINEAMIENTO 4: REALIZACION DE LA AUDIENCIA PÚBLICA DE RENDICION DE CUENTAS

La realización de la Audiencia Pública implica desde la exposición del informe por parte de la autoridad, las preguntas del pleno hasta la evaluación y cierre del evento.

Orientaciones

1) El Comité Técnico de Rendición y la Dirección de Comunicación Institucional designarán funcionarios/as encargados de entregar a los participantes los documentos de interés (Informes de Rendición de Cuentas Anuales, cuestionario de evaluación, etc.).
2) El Comité Técnico de Rendición de Cuentas designará un moderador para organizar los tiempos y moderar las intervenciones.
3) El Presidente realizará la apertura y presentará el Informe de Rendición de Cuentas.
4) Los participantes podrán realizar consultas, emitir comentarios, presentar objeciones en relación al Informe de Rendición de Cuentas, de acuerdo al Reglamento de Audiencia Pública.
5) El Presidente podrá responder durante el acto a las consultas efectuadas por los interesados.
6) Habrá funcionarios/as designados encargados de recibir de los participantes las Evaluaciones completadas, así como las propuestas y consultas hechas sobre la Audiencia de Rendición de cuentas.
7) El Comité Técnico presentará las conclusiones de la Audiencia Pública y brindará las gracias por la participación.

Lic. Carmiña Martínez
Directora
Dirección de Comunicación
IPTA

COLABORACIÓN

- Dirección de Gestión y Desarrollo de las Personas
- Dirección de TIC´s

ÁREAS INVOLUCRADAS EN EL PROCESO

- Presidencia
- Dirección de Gabinete
- Dirección Nacional
- Dirección de Gestión y Desarrollo de las Personas
- Dirección de Comunicación Institucional
- Direcciones de Centros de Investigación
- Jefaturas de Campos Experimentales
- Dirección de TIC´S
- Servidores Públicos en general

Lic. Carmiña Martínez
Directora
Dirección de Comunicación
IPTA

ES COPIA

Instituto PARAGUAYO DE TECNOLOGÍA AGRARIA

GOBIERNO NACIONAL

Paraguay de la gente

INSTITUTO PARAGUAYO DE TECNOLOGIA AGRARIA

DIRECCIÓN DE TECNOLOGIA DE LA INFORMACIÓN Y COMUNICACIÓN

MANUAL DE CIBERSEGURIDAD DE LA DIRECCIÓN DE TIC´S

VERSION 2.0

ES COPIA

Ing. Agr. César Espínola
Director Secretaría General

Instituto Paraguayo de Tecnología Agraria
Dirección de Tecnologías de la Información y Comunicación

Ing. Agr. Hugo H. Carrillo G.
Director
Dirección de TIC's

AÑO 2021

Contenido

1. OBJETIVOS 1
2. ALCANCE 1
3. RESPONSABILIDADES 1
3.1 Principios Generales 1
3.2 Oficina de Tecnología y Sistemas de la Información 2
3.3 Los Funcionarios 4
3.4 Dirección de Gestión de Desarrollo de las Personas y Dirección de Contratación 4
3.5 Departamento de Patrimonio 4
3.6 Dirección Administrativa 5
3.7 De la prestación de servicios por terceros 5
3.8 Implementación 5
4. LINEAMIENTOS DEL MANUAL DE SEGURIDAD INFORMATICA 5
3.9 Del buen uso 6
3.9.1 De los activos tecnológicos 6
3.9.2 Del Internet 7
3.9.3 Del Correo electrónico ZIMBRA 7
3.9.4 Derechos de Autor 8
3.10 Control de Accesos 8
3.10.1 Gestión de Acceso de Usuarios de Correos, Bases de datos Sistemas de Información. ... 8
3.10.1.1 Creación de usuarios de Correo e INTRANET. 8
3.10.1.2 Creación de usuarios en Bases de Datos 9
3.10.1.3 Creación de usuarios de Red. 9
3.10.1.4 Sistemas de Administración de Contraseñas 9
3.10.1.5 Uso y creación de Contraseñas de usuarios de Correo, Bases de Datos, y Redes. 10
3.10.1.6 Uso y creación de Contraseñas de usuarios de Sistemas de Información. 10

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

3.10.1.7 Alta y baja de contraseñas de usuarios de Correo, Bases de Datos, Sistemas de Información y Redes. 10

3.10.1.8 Sustitución de contraseñas de usuarios de Correo, Bases de Datos, Sistemas de Información y Redes. 11

3.10.1.9 Control de Identificación y Autenticación de Usuarios de Correo, Bases de Datos, Sistemas de Información y Redes 11

3.10.1.10 Responsabilidades de los usuarios de Correo, Bases de Datos, Sistemas de Información y Redes. 11

3.10.2 Acceso a las Bases de Datos y Sistemas de Información. 12

3.10.3 Acceso a las Redes 13

3.10.4 Roles y perfiles de usuarios 13

3.10.4.1 Acceso a Servidores. 13

3.10.4.2 Control de acceso de los usuarios para uso de la red del IPTA. 14

3.10.4.3 Autenticación de Usuarios en la red para Conexiones Externas 15

3.10.4.3.1 Responsabilidades del uso de las redes de IPTA. 15

3.10.5 Acceso a los sistemas de Información 15

3.10.5.1 Gestión de privilegios. 15

3.10.5.2 Revisión de privilegios. 16

3.10.5.3 Cancelación de Privilegios. 16

3.10.5.4 Desarrolladores (INTERNOS Y EXTERNOS) 17

3.10.6 Acceso Computacional Móvil y Trabajo Remoto 18

3.10.6.1 Uso de equipos Móviles y dispositivos de almacenamiento móvil. 18

3.10.6.2 Trabajo Remoto 19

3.10.6.3 Conexiones remotas. 19

3.10.6.4 Responsabilidades de los usuarios: 19

3.10.7 Monitoreo de los Accesos. 19

3.10.7.1 Registro de eventos: 20

3.10.7.2 Registro de uso de los sistemas 20

Instituto Paraguayo de Tecnología Agraria

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

3.11 Uso y creación de contraseñas seguras 20
3.12 Seguridad 22
3.12.1 Antivirus 22
3.12.1.1 Funcionarios del IPTA deben: 22
3.12.2 Red 23
3.12.3 Servidores 24
3.12.3.1 Configuración e instalación 24
3.12.4 Seguridad Perimetral 25
3.12.5 Sistemas de Detección de Intrusos (IDS) 25
3.12.6 Redes Privadas Virtuales (VPN) 26
3.12.7 Seguridad física y Ambiental en centros información y de cableado 27
3.13 Vulnerabilidades 28
3.13.1 Objetivos Específicos 28
3.13.2 Gestión de Vulnerabilidades 28
3.13.2.1 Pre requisito para la evaluación de vulnerabilidades 28
3.13.3 Caracterización de Gestión de Vulnerabilidades: 28
3.13.3.1 Fases de Gestión de Vulnerabilidades: 28
3.13.3.1.1 Fase de Identificación de la Vulnerabilidad 28
3.13.3.2 Administ ración de las Vulnerabilidades. 30
3.13.3.2.1 Asignación de Vulnerabilidades. 30
3.13.3.3 Remediación. 31
3.13.3.3.1 Priorización atención de Vulnerabilidad. 31
3.13.3.3.2 Tratamiento de la Vulnerabilidad 31
3.13.3.3.3 Priorización atención de la Remediación de la Vulnerabilidad 32
3.13.3.4 32
3.13.3.5 Actividades de Gestión de Vulnerabilidades. 32
3.14 Gestión de LOGs 33

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

3.14.1 Almacenamiento y Retencion 34
3.14.2 Frecuencia de Auditoria de LOGS. 35
3.15 Conectividad 35
3.15.1 Red Inalámbrica (WIFI) 35
3.15.1.1 Acceso a funcionarios: 35
3.16 Evaluación de los Riesgos de Seguridad Informática 36
3.17 Gestión de Borrado Seguro. 37
3.17.1 Generalidades. 37
3.17.2 Método de Borrado seguro de la Información. 37
3.17.2.1 . Formateo abajo nivel. 37
3.17.3 Herramienta para el Formateo abajo nivel. 37
3.17.4 Tratamiento de eliminación de las licencias de Software. 38
3.17.5 Paso a Paso para el Borrado Seguro. 38
b) RESPONSABLES 38
c) DEFINICIONES 38
Funcionarios: (funcionarios, contratistas y/o terceros) de todas las áreas y procesos del IPTA 38

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

1. OBJETIVOS

Garantizar la calidad en los servicios tecnológicos y de comunicaciones del Instituto Paraguayo de Tecnología Agraria - IPTA ofreciendo confiabilidad, integridad, disponibilidad y eficiencia, optimizando y asegurando su correcta funcionalidad, brindando un nivel de seguridad óptimo y que permitan:

- Disminuir las amenazas de los sistemas de información institucional.
- Evitar el mal uso e indiscriminado de los recursos.
- Cuidar y proteger los recursos tecnológicos del IPTA.
- Concientizar a los funcionarios del IPTA sobre la importancia del uso racional y seguro de la infraestructura informática, sistemas de información, servicios de red y canales de comunicación.

2. ALCANCE

Los Lineamientos del presente documento de seguridad informática de la Dirección de TIC´s del Instituto Paraguayo de Tecnología Agraria (IPTA), aplica para todos los funcionarios, contratistas, personal de apoyo y terceros no vinculados directamente al IPTA, pero que presten su servicio y utilicen tecnología de información, equipos propios del IPTA o arrendados y a los equipos de personas externas que sean conectados a la red del IPTA.

La revisión de estos lineamientos, así como de los objetivos del Manual de Seguridad Informática, debe realizarse con una periodicidad mínima de una vez al año, o cuando se originen cambios en la entidad que puedan afectar la operación de los servicios Tics, o durante las revisiones periódicas que desde la dirección se ejecutan para asegurar la continuidad del sistema.

3. RESPONSABILIDADES

3.1 Principios Generales

Todos los directivos y los funcionarios del IPTA tienen la responsabilidad de proteger la seguridad de los activos y de los recursos de TI bajo su control, de acuerdo con las instrucciones y las capacitaciones recibidas. Deben definirse responsabilidades expresas para la implementación, operación y administración de los controles de seguridad informática y deben discriminarse dichas responsabilidades de aquéllas que sean incompatibles cuando esto pudiera debilitar el nivel del control interno en forma inaceptable.

Ing. Hugo H. Carrillo G.
Director
IPTA Dirección de TIC's

3.2 Oficina de Tecnología y Sistemas de la Información

El Responsable de la Seguridad Informática del IPTA, será la Dirección de TIC´s a través del Departamento de Redes y Comunicaciones cual se encargará de:

a) Desarrollar, revisar, actualizar e implementar las políticas y lineamientos del IPTA.
b) Proporcionar una dirección funcional en el ámbito de seguridad informática en el IPTA;
c) Acordar las prioridades de seguridad informática en el IPTA;
d) Monitorear e informar sobre el trabajo de seguridad informática a la Dirección;
e) Dar asesoramiento sobre la seguridad física de todas las instalaciones del IPTA;
f) Garantizar que la seguridad de todos los activos de TI esté debidamente protegida; que se le dé la prioridad correspondiente al trabajo de seguridad informática, de manera oportuna, en todos los proyectos de TI;
g) Definir lineamientos de gestión de acceso que permitirá únicamente el ingreso a los usuarios autorizados por la dependencia correspondiente, y en el nivel asignado, sobre los datos, la red y sistemas de información necesarios para desempeñar sus tareas habituales.
h) Definir los lineamientos de contraseñas robustas para los usuarios de las Bases de Datos, Red y Sistemas de Información.
i) Definir las herramientas, procedimientos, formatos entre otros, para la implementación de un sistema de autenticación de acceso a los usuarios internos y externos en las diferentes plataformas tecnológicas.
j) Definir las herramientas, procedimientos de monitorización de los sistemas con el fin de detectar accesos no autorizados y desviaciones, registrando eventos que suministren evidencias en caso de producirse incidentes relativos a la seguridad.
k) Garantizar la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica del IPTA.
l) Proveer las herramientas que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica del IPTA y los servicios que se ejecutan en la misma.

ES COPIA

Ing. Hugo R. Carrillo G.
Director
Dirección de TIC's

m) Establecer responsabilidades y procedimientos para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios existente en el IPTA. Conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones en caso que los haya.

n) Validar los riesgos que genera la migración hacia nuevas versiones del software operativo.

o) Establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo del IPTA.

p) Realizar el borrado seguro del contenido de medios reutilizables que contengan información reservada del IPTA que se van a retirar de las instalaciones.

q) Realizar respaldo a través del proceso de gestión de copias de respaldo de la información reservada del IPTA cuya duración es mayor al tiempo de vida del medio en donde se encuentra almacenada.

r) Realizar pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, a través de un tercero, que cumplan con estándares internacionales.

s) Proponer políticas y especificaciones técnicas de bienes y servicios, procedimientos, acciones y medidas específicas en materia de Seguridad Informática; que sean aplicables a cualquiera de los elementos tecnológicos que integren la plataforma de Seguridad Informática de la entidad;

t) Del sistema de gestión de incidentes de seguridad de la información, analizar aquellos que involucren los servicios informáticos a fin de establecer controles para detectar, corregir y prevenir incidentes posteriores.

u) Revisar y mantener actualizado el inventario de Activos Informáticos relacionados con la Plataforma de Seguridad Informática del IPTA como complemento del inventario de activos de Información infraestructura con que esta cuenta;

v) Publicar en el Sistema de Gestión Documental los documentos técnicos (lineamientos, políticas, guias, procesos, procedimientos) en materia de Seguridad Informática emitidos por la DTIC´s

w) Promover el cumplimiento de la Política de Seguridad de la Información del IPTA;

Instituto Paraguayo de Tecnología Agraria
Ing. Hugo H. Carrillo G.
Director
IPTA
Dirección de TIC's

x) Revocar y/o recuperar las contraseñas, cuando las claves estén comprometidas según sea el caso.

y) Administrar y registrar todos los nombres de equipos que son accesibles a la red del IPTA;

z) Controlar y registrar todos los certificados de seguridad de los sitios de la entidad;

aa) Coordinar con las instancias y especialistas de seguridad del operador para manejar los reportes de incidentes y anomalías de Seguridad Informática;

bb) Las demás que determine la Dirección de TIC´s.

3.3 Los Funcionarios

Todos los Funcionarios del IPTA son responsables de:

a) Cumplir con las instrucciones y los procedimientos de seguridad aprobados y aquellas responsabilidades de seguridad específicas documentadas en los objetivos personales y la descripción de tareas;

b) Mantener la confidencialidad de las contraseñas personales y evitar que terceros utilicen los derechos de acceso de los usuarios autorizados;

c) Proteger la seguridad de los equipos informáticos, así como de la información bajo su control directo;

d) Informarle a la directiva inmediata o de seguridad cualquier sospecha de violaciones de la seguridad y de cualquier debilidad detectada en los controles de esta, incluyendo sospechas de divulgación de contraseñas.

e) Acatar con los lineamientos establecidos dentro de este documento

3.4 Dirección de Gestión de Desarrollo de las Personas y Dirección de Contratación

a) Debe informar a la Dirección de TIC´s todo movimiento del personal o contratos (altas, bajas prorrogas de contratos) a fin de realizar los procedimientos pertinentes.

3.5 Departamento de Patrimonio

a) Responsable del inventario de equipos y su actualización, según se establezca en las normas vigentes;

Instituto Paraguayo de Tecnología Agraria
Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

3.6 Dirección Administrativa

a) proporcionar los suministros de los equipos que permitan la operación adecuada de los procesos de la entidad.

3.7 De la prestación de servicios por terceros

a) Todo proveedor que proporcione servicios informáticos al IPTA que tenga acceso a información reservada y/o confidencial, deberá apegarse a las disposiciones de las leyes, reglamentos y demás instrumentos normativos relacionados con acceso a la información pública y protección de datos personales y contar con acuerdos de no divulgación ni uso que perjudique al IPTA.

b) Todo servicio informático otorgado por terceros debe ser monitoreado y revisado por la persona responsable de su contratación, para asegurar que se cumplan con los términos estipulados en los acuerdos o contratos del IPTA.

3.8 Implementación

A fin de implementar controles de seguridad informática que sean efectivos y eficaces, el manual de seguridad informática es:

a) implementar un conjunto coherente y equilibrado de controles de prevención, detección y recuperación de datos;

b) implementar controles complementarios, y que se refuercen mutuamente, en todos los sistemas y actividades interrelacionadas. Debe evitarse el depender en un solo nivel de controles;

c) automatizar los controles, cuando sea posible y se justifique el costo;

d) simplificar los controles y reducir la variedad y complejidad de las herramientas de seguridad cuando sea posible y se justifique el costo. Políticas y Lineamientos de Seguridad Informática

4. LINEAMIENTOS DEL MANUAL DE SEGURIDAD INFORMATICA

Los presentes lineamientos se dictan con el objeto de gestionar adecuadamente la Tecnología, los sistemas informáticos y el ambiente tecnológico del IPTA.

ES COPIA
Ing. Agr. César Espinola
Director General

Instituto Paraguayo de Tecnología Agraria

Ing. Hugo H. Carrillo G.
Director

3.9 Del buen uso

3.9.1 De los activos tecnológicos

a) Los activos tecnológicos definidos y entregados por la Dirección de TIC´s son:
   - PCs. de escritorio, portátiles y tablets.
   - Impresoras y/o fotocopiadoras multifunción.
   - Router, Switch, Access Point
   - Equipo de Videoconferencia

   Toda esta propiedad del IPTA.

b) La Dirección de TIC´s asignara a los Funcionarios y a las áreas de acuerdo con la necesidad los activos informáticos necesarios para uso de sus funciones y estos serán los únicos responsables de su utilización, así como también de la información contenida en los mismos, por lo que debe evitar compartirlos. En caso de requerir compartirlo o prestar el activo informático, será solamente para cuestiones laborales y sin liberarlo de su responsabilidad.

c) Los PCs de escritorio y portátiles se encuentran configurados con el Hardware y Software básico necesario para su funcionamiento y cumplimiento de las funciones.

d) Toda movilización del activo informático dentro o fuera de las instalaciones de la entidad es responsabilidad del funcionario asignado a este.

e) Cuando exista algún incidente (robo, extravió, daño físico, etc.) que afecte de manera directa a un activo informativo del IPTA, deberá ser notificado al Dpto. de Patrimonio y la Dirección de TIC´s, donde esta informara las acciones a tomar.

f) Solo funcionarios de la DTIC está autorizada a realizar reparaciones, cambios, desarme de los activos informáticos del IPTA.

g) La DTIC realizara periódicamente actualizaciones a los sistemas operativos, parches de seguridad, antivirus y de las aplicaciones instaladas en los PCs de escritorio y portátiles de los funcionarios del IPTA, los cuales deben garantizar el reinicio de estos para la aplicación de estas.

h) Los Funcionarios con activos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por DTIC.

Ing. Agr. César Espínola
Director Secretaría General

Ing. Hugo H. Carrillo G.
Dirección de TIC's

3.9.2 Del Internet

a) La DTIC provee el servicio de internet a todos los funcionarios del IPTA para adelantar exclusivamente las funciones asignadas a su cargo utilizándose de forma eficiente y responsable para fines institucionales.

b) Abstenerse de publicar Información relevante al IPTA independiente de su formato (word, excel, Power Point, PDF, avi, mp3,mp4 o cualquier otro formato actual o futuro) o su nivel de clasificación de confidencialidad en sitios de internet no licenciados por el IPTA en los denominados discos, nubes, carpetas virtuales o cualquier sistema de publicación de documentos actual o futura dentro o fuera de la entidad.

c) Abstenerse de utilizar aplicaciones que permitan evadir los controles implementados por el IPTA.

d) El acceso a páginas Web con contenido inapropiado se encuentra restringido. Sin embargo y si por la naturaleza del cargo se requiere el acceso a páginas de acceso contralado, se debe solicitar a la Dirección de TIC´s su acceso adjuntando y el formulario la aprobación y justificación por parte del jefe inmediato.

e) Abstenerse de descargar imágenes, sonidos, música y videos, a su vez descargar archivos o instalar programas de sitios web desconocidos o gratuitos. debido a que puede saturar el canal.

f) La DTIC se reserva el derecho de bloquear sitios que se detecten como peligrosos (con contenidos no autorizados) para la seguridad de los activos informáticos.

g) Cada funcionario es responsable del adecuado manejo de los usuarios de autenticación y contraseña a la hora de ingresar a los diferentes sistemas de información que consulte en internet.

3.9.3 Del Correo electrónico ZIMBRA

a) El único servicio de correo de uso obligatorio y de carácter oficial aprobado según Resolución IPTA N° 606/2016 es la herramienta ZIMBRA.

b) El correo electrónico institucional es para uso exclusivo de los funcionarios activos, dependencias del IPTA, sistemas de información, etc., por lo cual deberá ser utilizado sólo para realizar actividades relacionadas con sus funciones.

Instituto Paraguayo de Tecnología Agraria
Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

3.9.4 Derechos de Autor

a) Queda estrictamente prohibido inspeccionar, copiar y almacenar programas informáticos, software y demás fuentes que violen la ley de derechos de autor, para tal efecto todos los funcionarios se comprometan, bajo su responsabilidad, a no usar programas de software que violen la ley de derechos de autor y que se encuentren licenciados por parte del IPTA.

b) Para asegurarse de no violar los derechos de autor, no está permitido a los funcionarios copiar ningún programa instalado en los activos informáticos de la entidad en ninguna circunstancia sin la autorización escrita de la DTIC. No está permitido instalar ningún programa en el activo informático sin dicha autorización o la clara verificación de que la entidad posee una licencia que cubre dicha instalación.

c) No está autorizada la descarga de Internet de programas informáticos no autorizados por DTIC. De ser necesario por cualquier área del IPTA se debe solicitar por medio de la DTIC.

d) No está permitido que los funcionarios realicen copias no autorizadas de programas informáticos, cualquier tipo de información, sistemas de información, base de datos, etc.

e) Si se evidencia que algún funcionario ha realizado copia de programas informáticos música en forma ilegal, la DTIC comunicara al jefe inmediato para que este tome las medidas necesarias.

f) Los funcionarios que realicen, adquieran o utilicen copias no autorizadas de programas informáticos estarán sujetos a sanciones disciplinarias internas de acuerdo al Comité de Ética Institucional.

3.10 Control de Accesos

3.10.1 Gestión de Acceso de Usuarios de Correos, Bases de datos Sistemas de Información.

3.10.1.1 Creación de usuarios de Correo e INTRANET.

La DTIC establece como mecanismos para la creación de usuarios de correos a través de un formulario disponible en la Página web institucional, generada por el funcionario solicitante y todos aquellos que requieran realizar la creación, modificación y eliminación de usuarios, el mismo deberá obtener el visto bueno del Superior inmediato y de la

3.10.1.2 Creación de usuarios en Bases de Datos

La creación de usuarios de base de datos se solicita a través de un formulario disponible en la Página web institucional, generada por el funcionario solicitante con el visto bueno del superior inmediato.

La solicitud para creación de usuarios en bases de datos debe ser aprobada por el jefe de Desarrollo de Software.

3.10.1.3 Creación de usuarios de Red.

La DTIC establece como mecanismos para la creación de usuarios de red y/o instalación de puntos de red a través de un formulario disponible en la Página web institucional, con el visto bueno del superior inmediato, en donde se realizará la creación, modificación y eliminación de usuarios en el IPTA y la autorización para el ingreso de páginas restringidas por la Dirección de TIC´s debidamente justificadas.

3.10.1.4Sistemas de Administración de Contraseñas.

El sistema de administración de contraseñas para usuarios de correo, Bases de Datos, sistemas de información y redes del IPTA deben cumplir como mínimo con las siguientes especificaciones:

a) Obligar el uso de los usuarios y contraseñas individuales para determinar responsabilidades.
b) Permitir que los usuarios seleccionen y cambien sus propias contraseñas luego de cumplido el plazo mínimo de mantenimiento de estas o cuando consideren que la misma ha sido comprometida e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
c) Obligar a los usuarios a cambiar las contraseñas provisionales o que han sido asignadas por el administrador del sistema de información.
d) No permitir mostrar las contraseñas en texto claro cuando son ingresadas.

ES COPIA
Ing. Agr. César Espínola
Director Secretaría General

Instituto Paraguayo de Tecnología Agraria
Ing. Hugo D. Carrillo C.
Director
Dirección de TIC's

e) La longitud mínima de la contraseña sea ocho (8) caracteres combinadas aleatoriamente entre números, letras minúsculas, letras mayúsculas y símbolos.

3.10.1.5 Uso y creación de Contraseñas de usuarios de Correo, Bases de Datos, y Redes.

El uso y creación de contraseñas para usuarios de correos, Bases de datos, Sistemas de Información y Redes deben estar alineados con el numeral del buen uso y creación de contraseñas seguras dentro de este manual.

3.10.1.6 Uso y creación de Contraseñas de usuarios de Sistemas de Información.

La DTIC es la única encargada de realizar la creación de las cuentas de usuarios de los sistemas de Información y velar por el buen uso de ellas.
La administración de usuarios en los sistemas de información del IPTA, debe estar alineada a la Guía de Gestión de Usuarios que tiene por objetivo la creación, actualización e inactivación de usuarios en los diferentes sistemas de información.

3.10.1.7 Alta y baja de contraseñas de usuarios de Correo, Bases de Datos, Sistemas de Información y Redes.

La DTIC es la encargada de realizar las gestiones asociadas a la creación, edición o eliminación de contraseñas.

La administración y buen uso de contraseñas es responsabilidad de cada usuario de correo, Bases de Datos, Sistemas de Información, redes y deben estar alineadas con la política de uso y creación de contraseñas seguras.

Las contraseñas deben estar almacenadas en un sistema informático protegido mediante tecnologías diferentes a las utilizadas para la identificación y autenticación de usuarios.

3.10.1.8 Sustitución de contraseñas de usuarios de Correo, Bases de Datos, Sistemas de Información y Redes.

Para la sustitución de las contraseñas para usuarios de correo, Bases de Datos, Sistemas de Información y Redes se debe realizar bajo las siguientes premisas:

a) Cumplimiento del periodo de rotación establecido para la contraseña.
b) Cambio de contraseña decidido por el usuario.
c) Cambio de contraseña por olvido, pérdida o sospecha de haber sido comprometida la seguridad de la anterior.
d) Cambio de una contraseña por defecto.
e) El responsable de iniciar un procedimiento de cambio de contraseña podrá ser el dueño de la cuenta cuya contraseña ha de cambiarse, o DTIC (Responsable del Sistema) del IPTA.

3.10.1.9 Control de Identificación y Autenticación de Usuarios de Correo, Bases de Datos, Sistemas de Información y Redes.

La DTIC define que todos los usuarios tendrán un identificador único (ID de Usuario) solamente para su uso personal exclusivo, de manera que las actividades tengan trazabilidad.

3.10.1.10 Responsabilidades de los usuarios de Correo, Bases de Datos, Sistemas de Información y Redes.

La DTIC considera las siguientes responsabilidades de los usuarios de correo, Bases de Datos, Sistemas de Información y Redes:

a) Los usuarios de correo, Bases de Datos, Sistemas de Información y Redes son responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.

b) Los funcionarios no deben compartir sus cuentas de usuario y contraseñas con otros puestos que son personales e intransferibles.

Ing. Hugo H. Carrillo G.
Director

c) A los funcionarios que les fuesen asignada una cuenta y contraseña de otras entidades deberán cumplir con las políticas del IPTA, así como las políticas de seguridad de la entidad que asigna dicha cuenta.

d) Los funcionarios y personal provisto por terceras partes que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información del IPTA deben acogerse a lineamientos y políticas para la configuración de cuentas de usuario y contraseñas implantados por el IPTA, con el fin de garantizar una gestión y administración adecuada de las cuentas de usuario y contraseñas.

3.10.2 Acceso a las Bases de Datos y Sistemas de Información.

Toda la información del IPTA deberá únicamente ser operada a través de un mismo tipo de sistema manejador de base de datos y sistemas de información para beneficiarse de los mecanismos de integridad, seguridad y recuperación de información en caso de presentarse alguna falla.

a) El acceso a los sistemas de información deberá contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información del IPTA. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser manipulado por software.

b) Se deben delimitar las responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes.

c) Los datos de los sistemas de información deben ser respaldados de acuerdo con la frecuencia de actualización de sus datos, guardando respaldos históricos periódicamente. Es indispensable llevar una bitácora oficial de los respaldos realizados.

d) Todos los sistemas de información que se tengan en operación deben contar con el protocolo de paso a producción.

e) Los sistemas de información deben contemplar el registro histórico de las transacciones sobre datos relevantes, así como la clave del usuario y fecha en que se realizó (Normas Básicas de Auditoria y Control).

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

f) Se deben implantar rutinas periódicas de auditoria a la integridad de los datos y de los programas, para garantizar su confiabilidad.

3.10.3 Acceso a las Redes

El acceso de los funcionarios a las redes y a los servicios de red no debería comprometer la seguridad de los servicios de red garantizando que:

a) Se exige control de acceso de los usuarios a los servicios de información.
b) Mantener instalados y habilitados sólo aquellos servicios y puertos que sean utilizados por los sistemas de información y software de la institución.
c) Controlar el acceso lógico a los servicios, tanto a su uso como a su administración mediante bloqueo de puertos en el firewall de la institución.
d) El acceso de las redes del IPTA es de uso exclusivo y único para la infraestructura provista.

3.10.4 Roles y perfiles de usuarios

Los roles y perfiles de usuarios de Redes, se encuentra contenida en la matriz de roles.

3.10.4.1 Acceso a Servidores.

La DTIC, define que los servidores físicos y virtuales, deben estar bajo un solo administrador.

Se deberá acceder a los servidores Físicos y Virtuales por Consola o por escritorio remoto conservando las reglas definidas en el siguiente:

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

Ambiente	Consola y escritorio remoto	Reglas tráfico entrante
Desarrollo	Compartido (IPTA-Operador de red)	1. Todo cerrado excepto. a. Puertos documentados para su respectivo servicio y buen funcionamiento de aplicación. b. Permisos de acceso hacia los servidores. 2. Las reglas se depuran cada tres meses. 3. Evitar reglas provenientes de 'any'. Es preferible especificar IP o rango de IP.
Producción	Operador del Servicio	1. Todo cerrado excepto. a. Puertos documentados para su respectivo servicio y buen funcionamiento de aplicación. 2. Las reglas se depuran cada tres meses. 3. Evitar reglas provenientes de 'any'. Es preferible especificar IP o rango de IP.

Los accesos de los diferentes ambientes están limitados solo al tipo de ambiente requerido ya que no se debe mezclar los ambientes.

3.10.4.2 Control de acceso de los usuarios para uso de la red del IPTA.

La DTIC define como control de acceso de los usuarios a las redes los siguientes lineamientos:

a) Los usuarios del IPTA únicamente deben tener permiso de acceso directo a las aplicaciones y bases de datos, para cuyo uso están específicamente autorizados.

b) Todos los accesos de los usuarios remotos a sistemas y aplicaciones de información del IPTA deben estar controlados por medio de autenticación.

c) Todas las conexiones remotas que se realicen a sistemas de información del IPTA deben ser autenticadas.

d) Los puertos empleados para diagnóstico remoto y configuración deben estar controlados de forma segura, deben estar protegidos a través de un mecanismo de seguridad

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

adecuado y un procedimiento para asegurar que los accesos lógicos y físicos a estos son autorizados.

3.10.4.3 Autenticación de Usuarios en la red para Conexiones Externas

La autenticación de usuarios remotos deberá ser aprobada por el jefe inmediato del funcionario y bajo una solicitud con su respectivo formato.

3.10.4.3.1 Responsabilidades del uso de las redes de IPTA.

Cada uno de los funcionarios del IPTA, es responsable de usar de forma adecuada los recursos de red y de seguir los procedimientos definidos para el acceso a las redes.

3.10.5 Acceso a los sistemas de Información

Todos los funcionarios deben acceder a los recursos de servicios de información a través de la cuenta de usuario asignada.

El acceso lógico al software de aplicación se restringe a usuarios no autorizados.

El acceso a las aplicaciones y bases de datos debe ser independiente del acceso al sistema operativo.

3.10.5.1 Gestión de privilegios.

La asignación, modificación o revocación de privilegios en los Sistemas de Información del IPTA será solicitada por los responsables del departamento o área a la que pertenezca el destinatario de dichos privilegios.

Existirán privilegios asociados a:

a) Cada usuario.
b) Cada perfil, tales como: Administrador, Operador, Usuario Externo, Usuario Interno, Usuario Temporal o Etc.
c) Cada recurso, tales como: Bases de datos, Aplicaciones. o Etc.
d) Cada permiso, tales como: Lectura, Escritura o Control total.
e) Los sistemas deben estar diseñados o configurados de tal forma que sólo se acceda a las funciones permitidas.

Ing. Hugo H. Carrillo G.
Director
de TIC's

f) La información se creará al dar de alta a un usuario por primera vez en alguno de los sistemas afectados, y deberá mantenerse actualizada, registrándose todas aquellas modificaciones que se produzcan en los privilegios de acceso hasta el momento en que el usuario haya causado baja en todos los sistemas incluidos en el alcance.

3.10.5.2 Revisión de privilegios.

Al menos, cada año, se realizará una revisión de los privilegios de acceso de todos los usuarios.

Cuando se trate de privilegios especiales (administrador, root, etc.), tal revisión de privilegios se deberá realizar, al menos, cada 1 año, y, en cualquier caso, siempre que existan:

a) Alta de nuevos usuarios.
b) Baja de usuarios.
c) Además, los privilegios de acceso de usuarios, tanto internos como externos, deben ser revisados siempre que existan cambios en las funciones o responsabilidades. Para ambos tipos de usuarios se tendrán en cuenta, al menos, las siguientes cuestiones:
    - Necesidad de nuevos permisos.
    - Cancelación de antiguos permisos.
    - Segregación de funciones.
    - Devolución de activos y modificación o cancelación de permisos de accesos físicos.
    - Modificación de contraseñas de acceso.
    - Notificación al personal implicado de su baja o cambio.
    - Necesidad de retención de registros.

3.10.5.3 Cancelación de Privilegios.

Todos los privilegios de accesos de usuarios de correo, Bases de Datos, Sistemas de Información y Redes tanto internos como externos deben ser cancelados en el momento de la finalización de su contrato o prestación de sus servicios en el IPTA.

Los accesos lógicos a los activos de información deben ser removidos por los administradores de sistemas de forma inmediata.

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

Las cuentas de acceso de correo, bases de datos, sistemas de Información y redes se deben colocar en modo inactiva.

3.10.5.4 Desarrolladores (INTERNOS Y EXTERNOS)

Los desarrollares deben cumplir y acatar las políticas de seguridad de la información.

Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.

Los desarrolladores deben garantizar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.

Los desarrolladores deben garantizar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.

Los desarrolladores deben garantizar que los controles de autenticación cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.

Los desarrolladores deben asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.

Los desarrolladores deben garantizar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.

Los desarrolladores deben asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deben tener un periodo de validez establecido; se deben forzar el cambio de las contraseñas temporales después de su utilización.

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

Los desarrolladores deben garantizar que el último acceso (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso a los sistemas de información.

Los desarrolladores deben asegurar la re-autenticación de los usuarios antes de la realización de operaciones críticas en los aplicativos.

Los desarrolladores deben, a nivel de los aplicativos, restringir acceso a archivos u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas por los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados.

Los desarrolladores deben garantizar que periódicamente se re-valida la autorización de los usuarios en los aplicativos y se asegura que sus privilegios no han sido modificados.

3.10.6 Acceso Computacional Móvil y Trabajo Remoto.

Se entiende como dispositivos informáticos y comunicación móviles, todos aquellos que permitan tener acceso y almacenar información institucional, desde lugares diferentes a las instalaciones del IPTA.

3.10.6.1 Uso de equipos Móviles y dispositivos de almacenamiento móvil.

El uso de equipos informáticos y dispositivos de almacenamiento móviles está restringido únicamente a los provistos por la institución y contemplan las siguientes directrices:

a) Uso de usuario y contraseña para acceso al mismo.
b) Cifrado de la información.
c) Restricción de privilegios administrativos para los usuarios.
d) Uso de software licenciado y provisto por el IPTA.
e) Realización de copias de seguridad periódicas.
f) Uso de mecanismos de seguridad que protejan la información en caso de pérdida o hurto de los dispositivos.
g) Mantener apagado el Bluetooth o cualquier otra tecnología inalámbrica que exista o llegara a existir.

Hugo R. Carrillo G.
Director
Dirección de TIC's

3.10.6.2 Trabajo Remoto

El trabajo remoto solo es autorizado por el responsable de la unidad organizativa de la cual dependa el funcionario que solicite el permiso. Dicha autorización solo se otorgará por la DTIC, una vez se verifique las condiciones de seguridad del ambiente de trabajo.

3.10.6.3 Conexiones remotas.

Utilizar la conexión de acceso remoto solo para acceder a servicios (File server, diferentes aplicativos, infraestructura entre otros) exclusivos del IPTA los cuales sean inalcanzables desde redes externas.

La DTIC permitirá las conexiones remotas a los recursos de la plataforma tecnológica; únicamente a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

La DTIC suministrará las herramientas y controles necesarios para realizar conexiones de manera segura.
La DTIC debe monitorear las conexiones remotas a los recursos de la plataforma tecnológica de la institución de manera permanente.

3.10.6.4 Responsabilidades de los usuarios:

Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de la institución y deben acatar las condiciones de uso establecidas para dichas conexiones.
Los usuarios únicamente deben establecer conexiones remotas a través de las VPN seguras y utilizar computadores previamente identificados y, en ninguna circunstancia, en computadores públicos, de hoteles o cafés internet, entre otros.

3.10.7 Monitoreo de los Accesos.

Se deben realizar labores periódicas de monitorización de los sistemas con el fin de detectar accesos no autorizados y desviaciones, registrando eventos que suministren evidencias en caso de producirse incidentes relativos a la seguridad.

Instituto de Tecnología Agraria
Dirección de Información y Comunicación
Ing. Hugo R. Carrillo G.
Director
Dirección de TIC's

Un técnico asignado del Dpto. de Redes y Comunicaciones realizará las revisiones periódicas para la verificación del cumplimiento de los lineamientos.

A tal efecto, se tendrán en cuenta los registros de eventos y de uso de los sistemas descritos a continuación.

3.10.7.1 Registro de eventos:

La DTIC contempla que el sistema de monitoreo debe suministrar como mínimo:

a) Intentos de acceso fallidos.
b) Bloqueos de cuenta.
c) Debilidad de contraseñas.
d) Cuentas inactivas y deshabilitadas.
e) Últimos accesos a cuentas. entre otros.

3.10.7.2 Registro de uso de los sistemas

a) Accesos no autorizados.
b) Uso de Privilegios.
c) Alertas de sistema. Entre otros

3.11 Uso y creación de contraseñas seguras

Los Funcionarios del IPTA deben proteger sus contraseñas siguiendo las siguientes recomendaciones

a) No escribir ni reflejar la contraseña en papel o documento donde quede constancia de esta.
b) No enviar nunca la contraseña por correo electrónico, redes sociales o en un SMS.
c) Las contraseñas que se generen en las diferentes aplicaciones deben viajar cifrada por la red.
d) No se debe facilitar ni mencionar la contraseña en conversaciones o comunicaciones de cualquier tipo.
e) No utilizar en ningún caso contraseñas que se ofrezcan en los ejemplos explicativos de construcción de contraseñas robustas.
f) No escribir las contraseñas en equipos informáticos de los que se desconozca su nivel de seguridad y puedan estar monitorizados, o en ordenadores de uso público (bibliotecas, cibercafés, telecentros, etc.).

g) No compartir su contraseña con terceros. El uso de la contraseña es personal e intransferible.
h) No revelar su contraseña vía telefónica.
i) No utilizar la función "Recordar Contraseña " de programas de aplicación, como Internet Explorer, Correo Electrónico, o cualquier otro programa.
j) Informar cualquier incidente de seguridad que ponga en riesgo su contraseña a la DTIC por medio de formulario de mesa de ayuda y/o correo electrónico.
k) Informar a la DTIC por medio del formulario de mesa de ayuda y/o correo electrónico sialguien dentro ofuera de la entidad le solicita su contraseña.
l) No permita que le observen al escribir su contraseña.
m) Cambiar las contraseñas por defecto proporcionadas por la DTIC.
n) Luego de 5 intentos de ingreso de contraseña fallidos, se bloqueará la cuenta de usuario y este deberá solicitar por medio de la Mesa de Ayuda de Tecnología el desbloqueo de esta.
o) Cuando un usuario inicie sesión por primera vez o cuando se realice una activación del usuario, el sistema exigirá cambio de contraseña. Las contraseñas generadas por primera vez deben estar alineadas a los requisitos y recomendaciones que a continuación se contemplan.

La DTIC ha definido una serie requisitos y recomendaciones en la creación y uso de las contraseñas:

a) No utilizar información personal en la contraseña: nombre del servidor o de sus familiares, ni sus apellidos, ni su fecha de nacimiento, ni cuentas bancarias, ni tarjetas de crédito, etc.
b) Se deben utilizar al mínimo 8 caracteres para crear la clave.
c) Las contraseñas deben utilizar la combinación aleatoria de los siguientes tipos de caracteres (Minúsculas, Mayúsculas, Números, Caracteres especiales como +*! @ # $ & % ^ -/)
d) Evitar utilizar secuencias básicas de teclado (por ejemplo: "qwerty", "asdf" o las típicas en numeracion: "1234" y "98765").
e) No repetir los mismos caracteres en la misma contraseña. (ej.: "111222").
f) No se debe utilizar como contraseña, ni contener, el nombre de usuario asociado a la contraseña.

g) Las contraseñas no deben ser FECHAS.
h) La contraseña no debe basarse en dos palabras separadas por un espacio ( ), guion (-) o guion bajo (_).
i) No se deberían asignar contraseñas en blanco. No utilizar datos relacionados con el usuario que sean fácilmente deducibles, o derivados de estos
j) Cuando el sistema le solicite cambio de contraseña esta no debe haber sido utilizada en los históricos del sistema.
k) Realizar cambio de contraseña como mínimo cada 45 días.
l) Las contraseñas deberán tener histórico de 10 claves para que puedan ser repetidas.

3.12 Seguridad

3.12.1 Antivirus

3.12.1.1 Funcionarios del IPTA deben:

a) Garantizar que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.
b) Notificar a la DTIC en caso de sospecha de alguna infección por software malicioso deben para que tome las medidas de control correspondientes.
c) Realizar copias de la información reservada del IPTA, mediante el uso de los puertos de los computadores, a cualquier dispositivo de almacenamiento externo (CD's, DVD's, discos duros externos, memorias USB, etc.).
d) Generar contraseñas robustas para las Bases de Datos, Red y Sistemas de Información.
e) Utilizar las herramientas, procedimientos, formatos entre otros, para la implementación de un sistema de autenticación de acceso a los usuarios internos y externos en las diferentes plataformas tecnológicas
f) Utilizar los formularios disponibles en la página web para el restablecimiento de privilegios para el control de acceso lógico de

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información del IPTA.

g) Velar porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y garantizará que la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

h) Utilizar las herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica del IPTA y los servicios que se ejecutan en la misma.

i) A permitir las actualizaciones de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica del IPTA.

j) A realizar copias periódicas de la información correspondiente a sus funciones dentro del IPTA, que contengan sus equipos informáticos.

k) Comunicar a la DTIC por los medios correspondientes cualquier caso de vulnerabilidad dentro de los sistemas de información del IPTA.

3.12.2 Red

a) Las redes tienen como propósito principal servir en la transformación e intercambio de información dentro del IPT entre los Funcionarios, departamentos, oficinas y hacia afuera a través de conexiones con otras redes o otras entidades de orden territorial.

b) La DTIC no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el Funcionario que los genere o solicite.

c) Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.

d) No se permite el uso de los servicios de la red cuando no cumplan con las labores propias dentro del IPTA.

e) Las cuentas de ingreso a los sistemas y los recursos informáticos son propiedad del IPTA y se usarán exclusivamente para actividades relacionadas con la labor asignada.

f) Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.

g) La DTIC es el único que cuenta con permisos para el uso de analizadores de red los cuales son usados para monitorear la funcionalidad de las redes.

h) No se permitirá el uso de analizadores para monitorear o censar redes ajenas al IPTA y no se deberán realizar análisis de la Red desde equipos externos a la entidad.

i) Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al Funcionario o red involucrada dependiendo de las políticas. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

3.12.3 Servidores

3.12.3.1 Configuración e instalación

a) La DTIC tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red.

b) La instalación y/o configuración de todo servidor conectado a la Red será responsabilidad de la DTIC por medio del Departamento de Redes y Comunicación.

c) Durante la configuración de los servidores la DTIC deben garantizar que las normas para el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios sean aplicadas.

d) Los servidores que proporcionen servicios a través de la red e Internet deberán:

- Funcionar 24 horas del día los 365 días del año.
- Recibir mantenimiento preventivo mínimo dos veces al año Recibir mantenimiento semestral que incluya depuración de logs.
- Recibir mantenimiento anual que incluya la revisión de su configuración.

Ing. Hugo R. Carrillo G.
Director
Dirección de TIC's

- Ser monitoreados por el Departamento de Redes y Comunicación.
- La información de los servidores deberá ser respaldada de acuerdo con políticas establecidas por la DTIC.
- Los servicios hacia Internet sólo podrán proveerse a través de los servidores autorizados por la DTIC.

3.12.4 Seguridad Perimetral

La seguridad perimetral es uno de los métodos posibles de protección de la Red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

a) La DTIC implementará soluciones lógicas y físicas que garanticen la protección de la información del IPTA de posibles ataques internos o externos.
b) Rechazar conexiones a servicios comprometidos.
c) Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico, http, https).
d) Proporcionar un único punto de interconexión con el exterior.
e) Redirigir el tráfico entrante a los dispositivos de seguridad con que cuenta el IPTA.
f) Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet
g) Auditar el tráfico entre el exterior y el interior.
h) Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red cuentas de usuarios internos.

3.12.5 Sistemas de Detección de Intrusos (IDS)

Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es una aplicación usada para detectar accesos no autorizados a un servidor o a una red. Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o a través de herramientas automáticas.

a) La DTIC implementará soluciones lógicas o físicas que impidan el acceso no autorizado a la red del IPTA.
b) Detección de ataques en el momento que están ocurriendo o poco después.
c) Automatización de la búsqueda de nuevos patrones de ataque, con herramientas estadísticas de búsqueda y al análisis de tráfico anómalo.
d) Monitorización y análisis de las actividades de los usuarios en busca de elementos anómalos.
e) Auditoría de configuraciones y vulnerabilidades de los sistemas de IDS.
f) Descubrir sistemas con servicios habilitados que no deberían de tener, mediante el análisis del tráfico y de los logs.
g) Análisis de comportamiento anormal. Si se detecta una conexión fuera de hora, reintentos de conexión fallidos y otros, existe la posibilidad de que se esté en presencia de una intrusión. Un análisis detallado del tráfico y los logs puede revelar una máquina comprometida o un usuario con su contraseña al descubierto.
h) Automatizar tareas como la actualización de reglas, la obtención y análisis de logs, la configuración de cortafuegos.
i) La Red del IPTA sólo podrá acceder a los parámetros que el Firewall tenga permitido o posibilite mediante su configuración.

3.12.6 Redes Privadas Virtuales (VPN)

Los usuarios móviles y remotos del IPTA podrán tener acceso a la red interna privada cuando se encuentren fuera de esta con acceso al Internet público, utilizando las redes privadas VPN IPSec habilitadas por la DTIC.

a) La DTIC será el encargado de configurar el software necesario y asignar las claves a los usuarios que lo soliciten.
b) El Funcionario que solicite una VPN es responsable del acceso remoto y del uso de este.
c) Para que un Funcionario o proveedor del IPTA pueda acceder a los equipos, ya sean servidores u otros equipos de la red interna del IPTA desde una conexión externa con la tecnología VPN, cumplirá con el siguiente procedimiento:

Ing. Hugo H. Carrillo G.
Director

- El Funcionario o proveedor solicitará a la DTIC por los medios correspondientes de la creación de usuario para acceso a la VPN. Esto aplica a todos los funcionarios y proveedores que tiene que realizar tareas fuera de horas laborables o en instalaciones que necesiten este tipo de acceso, participar en proyectos que requieran apoyo remoto, o alguna otra circunstancia especial que así lo amerite, debidamente justificada.
- La DTIC evaluará la solicitud; si aprueba la misma, se procederá a otorgar los permisos y acceso a la VPN. De no aprobar la misma, se devuelve al funcionario o proveedor solicitante con las razones de la decisión.
- Una vez procesado el permiso, se notifica al Funcionario o proveedor y se le dan las instrucciones para conectarse vía VPN. Si es necesario, personal técnico asistirá al usuario en el proceso de configurar el VPN.

3.12.7 Seguridad física y Ambiental en centros información y de cableado

a) Las instalaciones con fines específicos que alberguen equipos de procesamiento, almacenamiento, conectividad, seguridad críticos requieren una mayor protección que la proporcionada a las instalaciones comunes. Debe considerarse a todas las funciones de IT y al material relacionado como confidencial y protegerlos de manera acorde. Esto se debe coordinar con el área encarda de la seguridad perimetral de los centros de cómputo.

b) El acceso a los centros de cómputo y centros de cableado es restringido y solo el personal por la DTIC puede tener acceso a estos.

c) Solo el personal autorizado por el operador de servicios TICs cuenta con el acceso a los gabinetes (racks) donde se encuentre alojada infraestructura de procesamiento, almacenamiento, networking y seguridad. Si alguna área requiere el acceso a estos gabinetes (rack) se debe solicitar a la DTIC por los medios correspondientes este acceso el cual será analizado.

d) Garantizar el monitoreo y diligenciamiento de la bitácora para los accesos otorgados a los centros de cómputo (CAN y Externo)

previa autorización del responsable del IPTA, al personal de soporte técnico, proveedores, operador de servicios TICs, funcionarios, etc.

e) No está permitida la toma de fotografías o grabación de video, en áreas de procesamiento de información o donde se encuentren activos de información que comprometan la seguridad o la imagen de la entidad, a menos que esté autorizado.

3.13 Vulnerabilidades

3.13.1 Objetivos Específicos

a) Identificación y evaluación de los sistemas y redes críticas del IPTA.

b) Incremento en el conocimiento sobre información de seguridad para su administración.

c) Recomendaciones para reducir las vulnerabilidades de los sistemas y para proteger sistemas, información y redes críticas.

d) Identificación de los puntos vulnerables.

e) Informes o resultados estadísticos del escaneo de vulnerabilidades.

f) Implementación de planes de remediación para mitigar posibles riesgos tecnológicos producto del escaneo de vulnerabilidades.

g) Seguimiento y/o monitoreo periódico para la identificación y mitigación de vulnerabilidades técnicas.

3.13.2 Gestión de Vulnerabilidades.

3.13.2.1 Pre requisito para la evaluación de vulnerabilidades.

a) Contar con el inventario actualizado de sistemas de información, Bases de datos e infraestructura instaladas en el IPTA.

b) Disponer de fuentes de información técnica que informen sobre las vulnerabilidades descubiertas.

c) Contar con el Comité de Gestión de Vulnerabilidades.

3.13.3 Caracterización de Gestión de Vulnerabilidades:

3.13.3.1 Fases de Gestión de Vulnerabilidades:

3.13.3.1.1 Fase de Identificación de la Vulnerabilidad.

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

Para la identificación, caracterización y tratamiento de la vulnerabilidad la DTIC, define los siguientes métodos:

a) Método de Ponderación de las Fuentes que son Vulnerables.

El método de ponderación a las fuentes que son vulnerables en el IPTA se encuentra definidos en la siguiente matriz de ponderación de las fuentes de vulnerabilidad.

FUENTES	PUNTUACIÓN (CVSS)
CATEGORIA I	15
CATEGORIA II	10
CATEGORIA III	5
SERVIDORES	15
EQUIPOS PERIMETRALES	15
NETWORKING	10
ESTACIONES DE TRABAJO	5

Matriz de ponderación de las fuentes de vulnerabilidad.

b) Método para caracterizar el grado del Riesgo de la Vulnerabilidad.

El método de caracterizar el grado del Riesgo de las fuentes que son vulnerables en el IPTA se encuentra definidos en la siguiente matriz de caracterización del grado del Riesgo de la Vulnerabilidad de las fuentes de vulnerabilidad.

Instituto de Tecnología Agraria
Dirección de Información y Comunicación
IPTA

Hugo H. Carrillo G.
Director
Dirección de TIC's

Puntaje	Rango del Riesgo	Descripción
20	Crítico	Estas vulnerabilidades incluyen riesgo que podrían comprometer los equipos e inclusive interrumpir el servicio de las aplicaciones Categoría I, Categoría II y Categoría III.
15		Estas vulnerabilidades incluyen riesgo que podrían comprometer los equipos con degradación en el servicio de las aplicaciones Categoría I, Categoría II y Categoría III
10	Medio	Estas vulnerabilidades incluyen riesgo que podrían comprometer los equipos e inclusive interrumpir el servicio de las aplicaciones Categoría I, Categoría II y Categoría III.
5	Bajo	Estas vulnerabilidades incluyen riesgo que podrían comprometer los equipos e inclusive interrumpir el servicio de las aplicaciones Categoría I, Categoría II y Categoría III.

Matriz de caracterizar el grado del Riesgo de la Vulnerabilidad de las fuentes de vulnerabilidad

c) Método para caracterizar de la Criticidad de las Fuentes de Vulnerabilidad.

El método de caracterizar la criticidad a las fuentes que son vulnerables en el IPTA, se encuentra definidos en la siguiente matriz de caracterizar el grado del Riesgo de la Vulnerabilidad de las fuentes de vulnerabilidad.

		FUENTES						
		CATEGORIA I	CATEGORIA II	CATEGORIA III	SERVIDORES	EQUIPOS PERIMETRALES	NETWORKING	ESTACIONES DE TRABAJO
CRITICIDAD		X			X	X		
	MEDIA			X				
	BAJA							X

Matriz de caracterizar de la criticidad de las fuentes de vulnerabilidad

3.13.3.2 Administ ración de las Vulnerabilidades.

3.13.3.2.1 Asignación de Vulnerabilidades.

La administración de las vulnerabilidades después de haberse realizado una depuración, e identificada la fuente vulnerable, esta información

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

es enviada los responsables de cada área, como se especifica en la siguiente matriz.

FUENTES						
CATEGORIA I	CATEGORIA II	CATEGORIA III	SERVIDORES	EQUIPOS PERIMETRALES	NETWORKING	ESTACIONES DE TRABAJO
APLICACIONES	APLICACIONES	APLICACIONES	INFRAESTRCUTURA	INFRAESTRUCTURA	INFRAESTRCUTURA	INFRAESTRCUTURA

Matriz de asignación de vulnerabilidad

3.13.3.3 Remediación.

3.13.3.3.1 Priorización atención de Vulnerabilidad.

La priorización de la atención de las vulnerables en el IPTA se encuentra definidos en la siguiente matriz.

		FUENTES						
		CATEGORIA I	CATEGORIA II	CATEGORIA III	SERVIDORES	EQUIPOS PERIMETRALES	NETWORKIG	ESTACIONES DE TRABAJO
CRITICIDAD								
	MEDIA			8 HORAS				
	BAJA							24 HORAS

Matriz de Priorización atención de vulnerabilidad de las fuentes de vulnerabilidad

3.13.3.3.2 Tratamiento de la Vulnerabilidad.

El tratamiento de las Vulnerabilidades identificadas en donde se analizara si se:

i. Mitiga la Vulnerabilidad.
ii. Transfiere la Vulnerabilidad.
iii. Acepta la Vulnerabilidad.
iv. Evita la vulnerabilidad.

Pre requisitos para determinar el **tratamiento**.

v. Identificar las acciones.
vi. Recursos.

vii. Responsabilidades.

viii. Prioridades en la gestión de riesgos de seguridad de la información.

3.13.3.3.3 Priorización atención de la Remediación de la Vulnerabilidad

La priorización de la atención de la remediación de las vulnerables en el IPTA se encuentra definidos en la siguiente matriz

		CUSTOM						
		CATEGORIA I	CATEGORIA II	CATEGORIA III	SERVIDORES	EQUIPOS PERIMETRALES	NETWORKING	ESTACIONES DE TRABAJO
CRITICIDAD		INMEDIATA	INMEDIATA	INMEDIATA	INMEDIATA	INMEDIATA	INMEDIATA	INMEDIATA
		INMEDIATA	INMEDIATA	INMEDIATA	INMEDIATA	INMEDIATA	INMEDIATA	INMEDIATA
	MEDIA	EVUALACION COMITÉ	EVUALACION COMITÉ	EVUALACION COMITÉ	EVUALACION COMITÉ	EVUALACION COMITÉ	EVUALACION COMITÉ	EVUALACION COMITÉ
		EVUALACION COMITÉ	EVUALACION COMITÉ	EVUALACION COMITÉ	EVUALACION COMITÉ	EVUALACION COMITÉ	EVUALACION COMITÉ	EVUALACION COMITÉ

Matriz de Priorización atención de la remediación de la vulnerabilidad

3.13.3.4

3.13.3.5 Actividades de Gestión de Vulnerabilidades.

Las actividades contempladas para gestión de Vulnerabilidades se detallan en la siguiente matriz:

Fas	Actividades	Fuentes
Identificar vulnerabilidades	Identificación del grado de riesgo que representa la vulnerabilidad/evento identificado. Las alertas son recibidas desde fuentes externas y herramientas internas. Las alertas son revisadas y son ponderadas según su potencial riesgo. Se utilizan herramientas para El seguimiento de vulnerabilidades.	Escaneos (de infraestructura y de aplicación). Pentesting. Auditorías o revisiones de seguridad (tanto técnicas como no técnicas). Notificaciones de terceros. Reporte de Logs.
Administración de la vulnerabilidad:	Asignar un nivel de riesgo a la vulnerabilidad o evento en base al impacto que podría tener sobre el MEN. Identificar los sistemas y equipos afectados. Asignar la revisión de la vulnerabilidad o evento al responsable de la aplicación / plataforma / dispositivo.	Asignar un nivel de riesgo a la vulnerabilidad o evento en base al impacto que podría tener sobre el MEN. Identificar los sistemas y equipos afectados. Asignar la revisión de la vulnerabilidad o evento al responsable de la aplicación / plataforma / dispositivo.

ES COPIA

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

Fase de Aplicación o Remediación:	Evaluación del Comité de Gestión de Vulnerabilidades. Determinar el procedimiento a seguir en base al nivel de riesgo detectado. Deshabilitar los equipos y sistemas expuestos en caso de ser necesario. Determinar el tipo de solución necesaria. Probar solución. Implementación de la solución en los equipos productivos. Reportar la remediación de los sistemas a "Cumplimiento".	Acta de reunión del comité de gestión de vulnerabilidades. Plan de remediación de las vulnerabilidades.
Reporte	Documentar cualquier lección aprendida en el proceso de resolución de esta vulnerabilidad con el objetivo de que futuras vulnerabilidades que guarden alguna semejanza con ésta puedan ser resueltas de manera más eficiente.	KMDB para mesa de ayuda y área de seguridad.
Cumplimiento	Una vez resuelta una vulnerabilidad, debe verificarse que su resolución ha sido eficaz y la vulnerabilidad ha sido realmente eliminada según lo esperado	Comité de gestión de Vulnerabilidades
Gestión de seguimiento vulnerabilidades tratadas en	Realizar un análisis de la efectividad de las acciones propuestas para la mitigación de vulnerabilidades.	Actas de Comité de gestión de Vulnerabilidades

3.14 Gestión de LOGs

Aplica para toda la plataforma tecnológica que cuente con Sistemas operativos, o Dispositivos de red o dispositivos de seguridad del IPTA como:

a) Equipos de seguridad perimetral (Firewall, balanceadores, IPS entre otros).
b) Equipos Servidores.
c) Equipos de Networking.
d) Aplicaciones.
e) Equipos de Control de Acceso.

Instituto Paraguayo de Tecnología Agraria
Dirección de Tecnologías
Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

Fuente	Frecuencia de Generación (En días)	Priorización
Sistemas operativos (Servidores y equipos de red).		
1. Logs de Sistemas,	1	Baja
2. Logs de auditabilidad.	1	Media
3. Logs de Accesos de usuario.	1	Media
4. Logs de antivirus	1	Media
Dispositivos perimetrales (Firewall, balanceadores, IPS entre otros) y Aplicaciones de seguridad.		
1. Logs de servidor de autenticación	1	Alta
2. Logs de VPN+Firewall.	1	Alta
3. Logs Malware.	1	Alta
4. Logs de Accesos de usuario	1	Media
Aplicaciones.		
1. Logs de servidor de correos.	1	Alta
2. Logs de servidor WEB. 1 Alta	1	Alta
3. Logs de servidor de archivo.	1	Alta
4. Logs de servidor de bases de datos. 1 Alta	1	Alta
6. Logs de Accesos de usuario.	1	Media

3.14.1 Almacenamiento y Retencion

Se considera determinar los requerimientos de retención y almacenamiento para los Logs generados en un ambiente productivo, como se indica en la siguiente matriz.

FUENTE	Almacenamiento (Tamaño máximo)	Registro
1. Logs de Sistemas.	2 Gigas Diario	Localmente
2. Logs de auditabilidad.	2 Gigas Diario	Localmente
3. Logs de Accesos de usuario.	2 Gigas Diario	Localmente
4. Logs de Accesos inalámbricos.	2 Gigas Diario	Localmente
5. Logs de antivirus	1 Giga Diario	Localmente
1. Logs de servidor de autenticación	2 Gigas Diario	Localmente
2. Logs de VPN+Firewall.	2 Gigas Diario	Localmente
3. Malware.	2 Gigas Diario	Localmente
4. Logs de Accesos de usuario	2 Gigas Diario	Localmente
1. Logs de servidor de correos.	2 Gigas Diario	Localmente
2. Logs de servidor WEB.	2 Gigas Diario	Localmente
3. Logs de servidor de archivo.	2 Gigas Diario	Localmente
4. Logs de servidor de bases de datos.	2 Gigas Diario	Localmente
5. Logs de Accesos de usuario.	2 Gigas Diario	Localmente

Matriz de almacenamiento y retención de Logs

Instituto Paraguayo de Tecnología Agraria
Dirección de Tecnologías de la Información y Comunicación

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

Nota: El tiempo de retención de los Logs es de 3 meses tiempo realizara una compresión de 100:1 es decir aproximadamente 1.8 Gigas y se llevara a un repositorio de información a través del proceso de copias de respaldo.

3.14.2 Frecuencia de Auditoria de LOGS.

La frecuencia de revisión y auditoria de los Logs para dispositivos y aplicaciones catalogados con riesgo alto, se realizará a través del Comité de Gestión de Vulnerabilidades o de acuerdo con la demanda por el área de aplicaciones o infraestructura.

3.15 Conectividad

La autorización de acceso a Internet se concede exclusivamente para actividades relevantes a las funciones desempeñadas. Todos los funcionarios del IPTA tienen las mismas responsabilidades en cuanto al uso de Internet.

a) El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con Firewall incorporado en la misma.
b) No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de Internet conectándose con un módem.

3.15.1 Red Inalámbrica (WIFI)

3.15.1.1 Acceso a funcionarios:

a) La red inalámbrica del IPTA es un servicio que permite conectarse a la red de la entidad e Internet sin la necesidad de algún tipo de cableado. La Red inalámbrica le permitirá utilizar los servicios de Red, en las zonas de cobertura de esta.
b) Donde además de hacer uso del servicio de acceso a los sistemas, podrán acceder al servicio de Internet de manera controlada.
c) Las condiciones de uso presentadas definen los aspectos más importantes que deben tenerse en cuenta para la utilización del

Ing. Hugo H. Carrillo C.
Director
Dirección de TIC's

servicio de red inalámbrica, estas condiciones abarcan todos los dispositivos de comunicación inalámbrica (computadoras portátiles, Ipod, celulares, etc.) con capacidad de conexión Wireless.

d) La DTIC, es el encargado de la administración, habilitación y/o bajas de usuarios en la red inalámbrica dentro del IPTA.

3.16 Evaluación de los Riesgos de Seguridad Informática

Se podrán aplicar las técnicas de gestión de riesgos a todos los sistemas informáticos o a los servicios o componentes individuales de los sistemas, cuando sea posible y conveniente.

El proceso de evaluación de riesgos debe considerar:

a) La importancia de la información, del software y de otros activos del sistema informático en cuestión;

b) Las actividades del IPTA, los productos y servicios respaldados por los sistemas informáticos en cuestión;

c) El daño que pueda causarse como consecuencia de una violación seria de la seguridad de la información. Los impactos potenciales incluyen la pérdida financiera, el daño a la reputación de la entidad ante el estado paraguayo y el público en general, la mala publicidad y el incumplimiento potencial de las funciones de la entidad.

d) La probabilidad real de que ocurra dicha violación, teniendo en cuenta los controles existentes y las amenazas imperantes, el entorno en el que se utiliza o funciona el sistema, y la vida útil real de la información en cuestión;

e) Los controles adicionales requeridos para reducir los riesgos a un nivel aceptable;

f) Las acciones necesarias para implementar y aplicar los controles adicionales correspondientes. Si la Dirección considera que los riesgos identificados por esta evaluación son inaceptables, y estos no se pueden evitar ni reducir satisfactoriamente a través de métodos más efectivos, entonces se deben planificar e implementar mejoras en la seguridad informática.

3.17 Gestión de Borrado Seguro.

3.17.1 Generalidades.

La DTIC considera los siguientes requisitos mínimos antes de realizar un procedimiento de borrado seguro.

a) Acta de entrega equipo con las documentaciones correspondientes
b) Hacer una copia de respaldo de la información del activo y ponerla a disposición del funcionario al cual pertenecía el equipo de cómputo previa autorización del jefe inmediato.
c) Realizar una validación de las licencias de software asignado al usuario del equipo a realizar el borrado seguro.

3.17.2 Método de Borrado seguro de la Información.

3.17.2.1. Formateo abajo nivel.

La DTIC considera el método de borrado seguro el formateo abajo nivel con el formateo de las unidades de almacenamiento que a continuación se listan.

Soporte	Tipo
Discos Duros	Magnético
Pen Drive (USB)	Electrónico

Una vez cumplido el tiempo de retención se puede realizar el borrado seguro de estas realizándola con las herramientas que cuente la DTIC, garantizando la correcta eliminación de la información que allí se encontraba.

3.17.3 Herramienta para el Formateo abajo nivel.

Todo activo informático que cumpla su ciclo de vida y sea asignado para donación, destrucción o que sea reasignado, se debe garantizar el backup total de la información, sistemas operativos, configuraciones, etc., y este ser almacenado para proceder con el borrado seguro a bajo nivel con las herramientas licenciadas.

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's

3.17.4 Tratamiento de eliminación de las licencias de Software.

El tratamiento para eliminación de las licencias de software en la gestión de borrado seguro de los equipos pertenecientes del IPTA se realizará en el caso que el equipo se de baja.

3.17.5 Paso a Paso para el Borrado Seguro.

La DTIC establece que el lineamiento de borrado seguro aplica sobre todos los equipos de propiedad y de alquiler del IPTA.

La DTIC se encargará de controlar cualquier operación realizada sobre un dispositivo: mantenimiento, reparación, sustitución, para evitar fugas de información.

Toda solicitud de borrado seguro a los activos de información del se debe realizar a través de. Esta solicitud debe quedar documentada y evidenciada donde conste que se realizó el proceso de revisión y copia de respaldo del equipo.

b)RESPONSABLES

- Director de TICs
- Jefe de Dpto. de Desarrollo de Software
- Jefe de Dpto. de Redes y Comunicaciones
- Funcionarios de la DTIC
- Funcionarios del IPTA

c) DEFINICIONES

Funcionarios: (funcionarios, contratistas y/o terceros) de todas las áreas y procesos del IPTA

Activos de información: Corresponde a elementos tales como bases de datos, documentación, manuales de usuarios, planes de continuidad, etc.

Activos de software: Son elementos tales como: Aplicaciones de software, herramientas de desarrollo, y utilidades adicionales suministradas por el IPTA.

Activos físicos: Se consideran activos físicos elementos tales como: Computadores, portátiles, módems, impresoras, Equipos de Comunicaciones, PBX, cintas, discos, UPS, etc.

Ing. Hugo H. Carrillo C.
Director
Dirección de TIC's

DTIC: Oficina de Tecnología y Sistemas de Información del IPTA de Educación Nacional.

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, deberán considerarse los conceptos de:

Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Audibilidad: 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: Se refiere al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el IPTA.

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.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Instituto Paraguayo de Tecnología Agraria
Ing. Hugo H. Carrillo G.
Director
Dirección de TICs

Tecnología de la Información: Se refiere al hardware y software operados por el IPTA o por un tercero que procese información en su nombre, para llevar a cabo una función propia del IPTA, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Vulnerabilidad: Debilidad en un sistema, permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

Analizador de Vulnerabilidades: Herramienta que analiza todos los activos conectados a la red verificando posibles vulnerabilidades y catalogándolas según los estándares internacionales, según los puertos abiertos y configuraciones de los dispositivos hallados.

Comité de Vulnerabilidades:

Grupo interdisciplinario conformado por personal de Infraestructura, Aplicaciones, Oficial de Seguridad de la Información, Oficial de Seguridad Informática del Operador de la Red del IPTA y el Oficial de Seguridad Informática de la Interventoría. Este Comité se encargará de verificar el correcto desarrollo de las pruebas de vulnerabilidades técnicas, así como implementar planes de acción para mitigar las vulnerabilidades encontradas.

Escaneo de vulnerabilidades: Es una actividad que a través de aplicaciones permite realizar una verificación de seguridad en una red mediante el análisis de los puertos abiertos en toda la red que permite identificar los riesgos de seguridad. Además, identifica las debilidades de un sistema operativo o de software de aplicación.

Falso Positivo: Es un error por el cual un software de análisis de vulnerabilidades reporta que un sistema, aplicación o bases de datos presenta una falla de seguridad, cuando en realidad esta no existe.

Infraestructura Tecnológica (IT): Es el conjunto de hardware y software, que se implementa conformando una plataforma para el funcionamiento de las actividades de una organización u empresa.

IPTA: Instituto Paraguayo de Tecnologia Agraria.

Ing. Hugo H. Carrillo G.
Director
Dirección de TIC's