

PLAN tratamiento de riesgos de seguridad y privacidad de LA INFORMACIÓN 2017- 2022

Oficina de Tecnología de la Información y las Comunicaciones ebaracaldo@ins.gov.co



Créditos

Dra. Martha Lucia Ospina Martínez

Directora General

Ing. Elsa Marlen Baracaldo Huertas

Oficina Tecnología de la Información y Comunicaciones

ELABORÓ

 Ing. Elsa Marlen Baracaldo Huertas

Jefe de Tecnología de la Información y Comunicaciones

REVISÓ

Carolina Monroy Calvo

Asesora Despacho Dirección General

 (redacción inicial del documento e introducción, consolidación

de la información, edición técnica y corrección de estilo).

Alexander Casas Castro

Grupo de comunicaciones

Diseño y aprobación de la portada e ilustraciones.

APROBÓ

 Ing. Elsa Marlen Baracaldo Huertas

Jefe de Tecnología de la Información y Comunicaciones

El documento requirió revisión por la Oficina Asesora de Jurídica SI NO X

El documento requirió revisión por una instancia externa asesora SI NO X ¿Cuál?

©

Instituto Nacional de Salud

Bogotá, Colombia

Av. Calle 26 No. 51-20



## OBJETIVO

Presentar el informe busca mitigar los riesgos realizar la socialización y asesoramiento de los planes de tratamiento de riesgos de seguridad de la información definidos por cada proceso.

## DESCRIPCIÓN

En el INS trabajo en el levantamiento de riesgos de seguridad de la información (Aquellos riesgos que puedan afectar la confidencialidad, integridad y la disponibilidad de la información) con las siguientes áreas:

|  |  |
| --- | --- |
| **Ítem** | **Riesgos de seguridad de la información por áreas** |
| 1 | Adquisición de Bienes y Servicios - (Gestión Contractual) |
| 2 | Atención al Ciudadano |
| 3 | Dirección General - (Despacho, Comunicación Institucional) |
| 4 | Equipos de Laboratorios |
| 5 | Gestión Financiera - (Tesorería, Contabilidad, Central de Cuentas, Facturación y Cartera, Presupuesto, Costos, Financiera) |
| 6 | Grupo de Gestión Ambiental |
| 7 | Grupo de Gestión Documental |
| 8 | Grupo de Talento Humano - (Gestión Humana) |
| 9 | Investigación en Salud Pública - (Salud Materna y Perinatal, Parasitología, Microbiología, Biblioteca, Entomología, Banco de Proyectos, Nutrición, Salud Ambiental y Laboral, Fisiología Molecular, Morfología Celular, Secretaria Ejecutiva del CEMIN, Dirección de Investigación en Salud Pública, Subdirección de Investigación Científica y Tecnológica, Subdirector de Innovación en Salud Pública(SISP)) |
| 10 | Observatorio Nacional de Salud |
| 11 | Oficina Asesora Jurídica - (Gestión Jurídica) |
| 12 | Oficina de Control Interno - (Control Institucional) |
| 13 | Oficina de Tecnologías de Información y Comunicaciones |
| 14 | Planeación Institucional - (Oficina Asesora de Planeación - Calidad) |
| 15 | Producción - (Grupo de Animales de laboratorio - Bioterio, Área de Hacienda Galindo ySerpentario, Área de Producción de Biológicos, Área de Medios de Cultivo, Grupo Aseguramiento de la Calidad, Comercialización) |
| 16 | Gestión Administrativa - Recursos Físicos, Área de Almacén e Inventarios, Soporte |
| 17 | Redes en Salud Pública - (Subdirección de Gestión de la Calidad, Subdirección Red Nacional de Trasplantes y Bancos de Sangre, Redes en Salud Pública, Despacho, Subdirección Laboratorio Nacional de Referencia, Grupo Entomología, Grupo Virología,Grupo Micobacterias, Grupo Microbiología, Grupo Parasitología, Grupo Patología, Grupo Genética, Química y Toxicología y virología) |



|  |  |
| --- | --- |
| 18 | Vigilancia y Análisis del Riesgo en Salud Publica - (Transmisibles, Salud mental y lesiones de causa externa, No Transmisibles, Grupo Gestión del Riesgo, Respuesta Inmediata y Comunicación del Riesgo, Grupo Formación de Talento Humano en Salud Pública, Grupo Formación de Talento Humano en Salud Pública, Grupo de comunicaciones, EquipoSIVIGILA, Grupo ERIA y Plaguicida) |

## RESULTADOS

Se da a conocer los riesgos de seguridad de la información a las áreas mencionadas anteriormente, así como socializar, revisar y establecer planes de tratamiento que permitan mitigar los riesgos identificados. A continuación, se presentan los planes de tratamiento aprobados por cada una de las áreas:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Área Responsable** | **ID****Plan** | **Plan de tratamiento** | **Riesgo asociado** | **Tiempo para****implementar los planes de****tratamiento** | **Fecha de seguimiento** |
| Atención al ciudadano | PT043 | Verificar que las carpetas compartidas no sean locales, que se encuentren provistas por laOTIC, y que se le lleven a cabo backups periódicos | RSI0751 | 20 | 7/11/2021 |
| Atención alciudadano | PT044 | Transferir al archivo central ladocumentación histórica que no sea necesaria | RSI0204 RSI0205 | 45 | 2/12/2021 |
| Atención al ciudadano | PT045 | Implementar mejores prácticas en la administración del sistema SISDOC | RSI0145 RSI0146 RSI0147 RSI0148RSI0149 | 20 | 7/11/2021 |
| Control interno | PT046 | Verificar que las carpetas compartidas no sean locales, que se encuentren provistas por laOTIC, y que se le lleven a cabo backups periódicos | RSI0536 RSI0663 | 20 | 10/11/2021 |
| Control interno | PT047 | Verificar la restauración de backups | RSI0536RSI0663 | 20 | 10/11/2021 |
| Control interno | PT048 | Implementar una solución para la gestión adecuada de usuarios y contraseñas, ejemplokeepass | RSI0536 | 20 | 10/11/2021 |
| Oficina jurídica | PT049 | Transferir al archivo central ladocumentación histórica que no sea necesaria | RSI0202 RSI0204 | 45 | 5/12/2021 |
| Oficina jurídica | PT050 | Revisar el control de llave para el archivode gestión del área | RSI0202 | 20 | 10/11/2021 |
| Oficina jurídica | PT051 | Verificar que las carpetas compartidas no sean locales, que se encuentren provistas por laOTIC, y que se le lleven a cabo backups periódicos | RSI0687 | 20 | 10/11/2021 |
| Oficina jurídica | PT052 | Verificar la restauración de backups | RSI0687 | 20 | 10/11/2021 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Área Responsable** | **ID****Plan** | **Plan de tratamiento** | **Riesgo asociado** | **Tiempo para****implementar los planes de****tratamiento** | **Fecha de seguimiento** |
| Oficina jurídica | PT053 | Implementar una solución para la gestión adecuada de usuarios y contraseñas, ejemplokeepass | RSI0521 RSI0519 | 20 | 10/11/2021 |
| Gestión Humana | PT054 | Verificar que las carpetas compartidas no sean locales, que se encuentren provistas por laOTIC, y que se le lleven a cabo backups periódicos | RS0622 | 20 | 12/11/2021 |
| Gestión Humana | PT055 | Verificar que se estén haciendo backupsperiódicos de equipos en solución de la OTIC | RS0622 | 20 | 12/11/2021 |
| Gestión Humana | PT056 | Verificar la restauración de backups | RS0622 | 20 | 12/11/2021 |
| Gestión Humana | PT057 | Implementar una solución para la gestión adecuada de usuarios y contraseñas, ejemplokeepass | RS0621 | 20 | 12/11/2021 |
| Adquisición de bienes y servicios | PT058 | Hacer backup de equipos y carpetas compartidas en los recursos de TI, Backup T | RSI0533 RSI0648 RSI0650RSI0651 | 20 | 12/11/2021 |
| Adquisición de bienes y servicios | PT059 | Verificar la restauración de backups | RSI0533 RSI0648 RSI0650RSI0651 | 20 | 12/11/2021 |
| Adquisición de bienes y servicios | PT060 | Una vez se realice backup de la información del área validar si es posible borrar la información del disco duro o asignar unacontraseña a dicha información | RSI0737 | 20 | 12/11/2021 |
| Contabilidad | PT061 | Implementar un formato de préstamo dearchivo físico | RSI0425 | 30 | 12/11/2021 |
| Contabilidad | PT062 | Verificar llave de los escritorios | RSI0425RSI0730 | 20 | 12/11/2021 |
| Contabilidad | PT063 | Transferir información a Backup T | RSI0609RSI0610 | 20 | 12/11/2021 |
| Contabilidad | PT064 | Usar la aplicación Keepass | RSI0609 | 20 | 12/11/2021 |
| Contabilidad | PT065 | Implementar política de escritorio limpio | RSI0425RSI0730 | 20 | 12/11/2021 |
| Facturación | PT066 | Hacer transferencia al archivo central o transferir a bodega temporal | RSI0434 RSI0435RSI0436 | 45 | 12/11/2021 |
| Facturación | PT067 | Solicitar archivador más grande | RSI0434 | 45 | 12/11/2021 |
| Facturación | PT068 | Transferir información a Backup T | RSI0619 | 20 | 12/11/2021 |
| Facturación | PT069 | Usar la aplicación Keepass | RSI0618 | 20 | 12/11/2021 |
| Facturación | PT070 | Implementar política de escritorio limpio | RSI0732RSI0434 | 20 | 12/11/2021 |
| Tesorería | PT071 | Implementar un formato de préstamo dearchivo físico | RSI0464 | 30 | 23/11/2021 |
| Tesorería | PT072 | Transferir información a Backup T | RSI0630RSI0631 | 20 | 13/11/2021 |
| Tesorería | PT073 | Usar la aplicación Keepass | RSI0630 | 20 | 13/11/2021 |
| Tesorería | PT074 | Implementar política de escritorio limpio | RSI0464RSI0735 | 20 | 13/11/2021 |
| Costos | PT075 | Implementar un formato de préstamo dearchivo físico | RSI0428 | 30 | 23/11/2021 |
| Costos | PT076 | Implementar carpeta compartida en elgrupo de costos | RSI0752 RSI0753 | 20 | 13/11/2021 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Área Responsable** | **ID****Plan** | **Plan de tratamiento** | **Riesgo asociado** | **Tiempo para****implementar los planes de****tratamiento** | **Fecha de seguimiento** |
| Costos | PT077 | Transferir información a Backup T | RSI0752RSI0753 | 20 | 13/11/2021 |
| Costos | PT078 | Usar la aplicación Keepass | RSI0752 | 20 | 13/11/2021 |
| Costos | PT079 | Implementar política de escritorio limpio | RSI0428 | 20 | 13/11/2021 |
| Oficina asesora de planeación | PT080 | Transferir información a Backup T porusuario | RSI0546 RSI0588 RSI0589RSI0591 | 20 | 17/11/2021 |
| Oficina asesorade planeación | PT081 | Usar la aplicación Keepass por usuario | RSI0546 | 20 | 17/11/2021 |
| Oficina asesora de planeación | PT082 | Evitar préstamo de contraseñas solicitando usuarios adicionales para cada usuario que accedeal sistema | RSI0640 | 20 | 17/11/2021 |
| Oficina asesorade planeación | PT083 | Evitar uso de Dropbox y solicitar carpetacompartida para transferir información | RSI0641 RSI0642 | 20 | 17/11/2021 |
| Vigilancia y Análisis del Riesgo enSalud Pública | PT084 | Usar la aplicación Keepass | RSI0499 RSI0511 RSI0523 | 20 | 17/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública | PT085 | Transferir información a Backup T porusuario | RSI0542 RSI0545 RSI0580 RSI0581 RSI0582 RSI0583 RSI0596 RSI0597 RSI0598 RSI0599 RSI0624RSI0625 | 20 | 17/11/2021 |
| Vigilancia y Análisis del Riesgo enSalud Pública | PT086 | Revisar uso de puertos USB en el área | RSI0712 RSI0713 RSI0723 | 20 | 17/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública | PT087 | Archivo de gestión del Grupo ERIA y Plaguicidas debe tener llave | RSI0347 RSI0348 RSI0366 RSI0392 RSI0449 RSI0450RSI0451 | 45 | 17/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública | PT088 | Verificar el control de rastreo en office 365 | RSI0680 RSI0681 RSI0682RSI0683 | 20 | 17/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública - Grupo de enfermedades NoTransmisibles | PT089 | Hacer backup en T con contraseña deWinRAR | RSI0545 | 20 | 17/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública - Grupo de enfermedades NoTransmisibles | PT090 | backup en discos duros personales con contraseña en WinRAR | RSI0712 RSI0713 RSI0723 | 20 | 17/11/2021 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Área Responsable** | **ID****Plan** | **Plan de tratamiento** | **Riesgo asociado** | **Tiempo para****implementar los planes de****tratamiento** | **Fecha de seguimiento** |
| Vigilancia y Análisis del Riesgo en Salud Pública - Grupo de enfermedades NoTransmisibles | PT091 | USB, borrar información después de uso o asignar contraseña a los archivos | RSI0712 RSI0713 RSI0723 | 20 | 17/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública - EquipoAdministrativo | PT092 | Transferir información a Backup T porusuario | RSI0754 | 20 | 17/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública - EquipoAdministrativo | PT093 | Usar la aplicación Keepass | RSI0755 | 20 | 17/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública - Grupo Formación de TalentoHumano en Salud Pública | PT094 | Hacer desarrollo para que Certificación de personas y Aula Virtual permita que el usuario asigne su propia contraseña | RSI0089 | 30 | 17/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública - Grupo Formación de TalentoHumano en Salud Pública | PT095 | Colocar nota de manejo de datos personales en formulario de inscripción de cursos y un check de si desea que le sigan llegando correos relacionadoshttps://forms.office.com/Pages/ResponsePage.aspx | RSI0756 | 30 | 17/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública - Grupo Formación de TalentoHumano en Salud Pública | PT096 | Solicitar a OTIC servidor para trasladar la BD de estudiantes (access) EPIINFO | RSI0757 | 30 | 17/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública - Grupo Formación de TalentoHumano en Salud Pública | PT097 | Implementar un formato del solicitante de los discos duros externos | RSI0758 | 30 | 17/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública - Grupo Formación de TalentoHumano en Salud Pública | PT098 | Toda información de carácter confidencial (Listado de estudiantes) que sea retirada del INS mediante disco duros personales debe pedir contraseña WinRAR | RSI0758 | 20 | 17/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública - Grupo Formación de TalentoHumano en Salud Pública | PT099 | Toda información de carácter confidencial (Listado de estudiantes) que se cargue en Office 365 de pedir contraseña de WinRAR | RSI0759 | 20 | 17/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública - Grupo Formación de TalentoHumano en Salud Pública | PT100 | Transferir información a Backup T porusuario | RSI0542 RSI0580 RSI0581 RSI0582 RSI0583 | 20 | 17/11/2021 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Área Responsable** | **ID****Plan** | **Plan de tratamiento** | **Riesgo asociado** | **Tiempo para****implementar los planes de****tratamiento** | **Fecha de seguimiento** |
| Vigilancia y Análisis del Riesgo en Salud Pública - Factores deriesgo ambiental | PT101 | Transferir información a Backup T porusuario | RSI0760 | 20 | 21/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública - Factores deriesgo ambiental | PT102 | Borrar información de USB después de uso | RSI0761 | 20 | 21/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública - Factores deriesgo ambiental | PT103 | Toda información de carácter confidencial (Listado de estudiantes) que se cargue en Office 365 de pedir contraseña de WinRAR | RSI0762 | 20 | 21/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública - Grupo ERIAy Plaguicidas | PT104 | Transferir información a Backup T por usuario, en caso de que se encuentre lleno solicitar espacio adicional con la OTIC | RSI0680 RSI0682 | 20 | 21/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública - Grupo ERIAy Plaguicidas | PT105 | Toda información de carácter confidencial que se cargue en Office 365, One Drive, Dropox de pedir contraseña de WinRAR | RSI0763 | 20 | 21/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública - Grupo Gestión del Riesgo, Respuesta Inmediata yComunicación del Riesgo | PT106 | Tener copia de los backups del sistema de alertas tempranas en un repositorio de la OTIC (quincenal) | RSI0764 | 30 | 21/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública - Grupo Gestión del Riesgo, Respuesta Inmediata yComunicación del Riesgo | PT107 | Se debe restaurar los backups del sistema una vez al mes | RSI0764 | 20 | 21/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública - Grupo Gestión del Riesgo, Respuesta Inmediata yComunicación del Riesgo | PT108 | Restringir el acceso al sistema solo a los autorizados | RSI0764 | 20 | 21/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública - Grupo Gestión del Riesgo, Respuesta Inmediata yComunicación del Riesgo | PT109 | Hacer copia en Backup T por usuario | RSI0765 | 20 | 21/11/2021 |
| Vigilancia y Análisis del Riesgo en Salud Pública - Grupo Gestión del Riesgo, Respuesta Inmediata yComunicación del Riesgo | PT110 | Cifrado de discos duros de portátiles por parte de la OTIC | RSI0766 | 45 | 16/12/2021 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Área Responsable** | **ID****Plan** | **Plan de tratamiento** | **Riesgo asociado** | **Tiempo para****implementar los planes de****tratamiento** | **Fecha de seguimiento** |
| Gestión Documental | PT111 | Hacer backup de los equipos de cómputo en la carpeta Backup T de la OTIC por usuario, si no cuenta con espacio suficiente solicitar el aumentode capacidad | RSI0539 | 20 | 2/12/2021 |
| Gestión Documental | PT112 | Usar WinRAR para transferir información de carácter confidencial en USB, correo electrónico,WeTransfer | RSI0739 | 20 | 2/12/2021 |
| GestiónDocumental | PT113 | Se recomienda iniciar el proceso dedigitalización del archivo central | RSI0767 | 75 | 26/01/2021 |
| GestiónDocumental | PT114 | Usar la aplicación Keepass por usuario parala gestión adecuada de contraseñas | RSI0539 | 20 | 2/12/2021 |
| Oficina asesora de planeación | PT115 | Trabaja en conjunto con la OTIC la clasificación y etiquetado de la informaciónelectrónica y física del INS | RSI0588 RSI0589 RSI0641 | 45 | 12/12/2021 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Oficina de Tecnologías de Información y Comunicaciones | PT116 | Hacer análisis vulnerabilidades a la infraestructura de servidores al menos 2 veces al año | RSI0039 RSI0067 RSI0169 RSI0211 RSI0217 RSI0223 RSI0228 RSI0234 RSI0241 RSI0247 RSI0253 RSI0259 RSI0265 RSI0271 RSI0277 RSI0282 RSI0289 RSI0296 RSI0303 RSI0309 RSI0315 RSI0316 RSI0041 RSI0042 RSI0043 RSI0044 RSI0045 RSI0046 RSI0047 RSI0048 RSI0069 RSI0070 RSI0071 RSI0072 RSI0128 RSI0129 RSI0130 RSI0131 RSI0170 RSI0171 RSI0172 RSI0173 RSI0210 RSI0214 RSI0216 RSI0220 RSI0222 RSI0226 RSI0229 RSI0230 RSI0235 RSI0236 RSI0240 RSI0244 RSI0246 RSI0250 RSI0252 RSI0256 RSI0258 RSI0262 RSI0264 RSI0268 RSI0270RSI0274 | 45 | 12/12/2021 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Área Responsable** | **ID****Plan** | **Plan de tratamiento** | **Riesgo asociado** | **Tiempo para****implementar los planes de****tratamiento** | **Fecha de seguimiento** |
|  |  |  | RSI0276RSI0280 |  |  |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Oficina de Tecnologías de Información y Comunicaciones | PT117 | Hacer Ethical hacking a la infraestructura de servidores al menos 1 vez al año | RSI0039 RSI0067 RSI0169 RSI0211 RSI0217 RSI0223 RSI0228 RSI0234 RSI0241 RSI0247 RSI0253 RSI0259 RSI0265 RSI0271 RSI0277 RSI0282 RSI0289 RSI0296 RSI0303 RSI0309 RSI0315 RSI0316 RSI0041 RSI0042 RSI0043 RSI0044 RSI0045 RSI0046 RSI0047 RSI0048 RSI0069 RSI0070 RSI0071 RSI0072 RSI0128 RSI0129 RSI0130 RSI0131 RSI0170 RSI0171 RSI0172 RSI0173 RSI0210 RSI0214 RSI0216 RSI0220 RSI0222 RSI0226 RSI0229 RSI0230 RSI0235 RSI0236 RSI0240 RSI0244 RSI0246 RSI0250 RSI0252 RSI0256 RSI0258 RSI0262 RSI0264 RSI0268 RSI0270RSI0274 | 45 | 12/12/2021 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Área Responsable** | **ID****Plan** | **Plan de tratamiento** | **Riesgo asociado** | **Tiempo para****implementar los planes de****tratamiento** | **Fecha de seguimiento** |
|  |  |  | RSI0276RSI0280 RSI0281 RSI0288RSI0295 |  |  |
| Oficina de Tecnologías de Información y Comunicaciones | PT118 | Hacer hardening de la infraestructura de servidores | RSI0039 RSI0067 RSI0169 RSI0211 RSI0217 RSI0223 RSI0228 RSI0234 RSI0241 RSI0247 RSI0253 RSI0259 RSI0265 RSI0271 RSI0277 RSI0282 RSI0289 RSI0296 RSI0303 RSI0309 RSI0315RSI0316 | 45 | 12/12/2021 |
| Oficina de Tecnologías de Información y Comunicaciones | PT119 | Garantizar contrato de mantenimiento preventivo y correctivo de los servidores | RSI0046 RSI0047 RSI0048 RSI0071 RSI0072 RSI0130 RSI0131 RSI0173 RSI0213 RSI0219 RSI0225 RSI0232 RSI0238 RSI0243 RSI0249 RSI0255 RSI0261 RSI0267 RSI0273 RSI0279RSI0307 | 45 | 12/12/2021 |
| Oficina de Tecnologías de Información yComunicaciones | PT120 | Cambiar el sistema de aire acondicionado temporal del Datacenter por uno de precisión | RSI0768 | 45 | 12/12/2021 |
| Oficina de Tecnologías de Información yComunicaciones | PT121 | Poner en funcionamiento el sistema contraincendios del DataCenter | RSI0769 | 45 | 12/12/2021 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Área Responsable** | **ID****Plan** | **Plan de tratamiento** | **Riesgo asociado** | **Tiempo para****implementar los planes de****tratamiento** | **Fecha de seguimiento** |
| Oficina de Tecnologías de Información y Comunicaciones | PT122 | No permitir el acceso del equipo de desarrollo a bases de datos de producción | RSI0001 RSI0015 RSI0027 RSI0039 RSI0053 RSI0067 RSI0075 RSI0081 RSI0089 RSI0095 RSI0101 RSI0115 RSI0133 RSI0139 RSI0145 RSI0151 RSI0157 RSI0169 RSI0175 RSI0181 RSI0211 RSI0217 RSI0223 RSI0228 RSI0234 RSI0241 RSI0247 RSI0253 RSI0259 RSI0265 RSI0271 RSI0277 RSI0303 RSI0315 RSI0316 RSI0325 RSI0331 RSI0337RSI0764 | 45 | 12/12/2021 |
| Oficina de Tecnologías de Información y Comunicaciones | PT123 | No compartir credenciales de acceso a las bases de datos con el equipo de desarrollo | RSI0633 RSI0637 RSI0641 RSI0645 RSI0649 RSI0653 RSI0657 RSI0661 RSI0665 RSI0669 RSI0673 RSI0677 RSI0681RSI0685 | 45 | 12/12/2021 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Oficina de Tecnologías de Información y Comunicaciones | PT124 | Implementar el procedimiento de gestión de cambios | RSI0003 RSI0004 RSI0005 RSI0006 RSI0007 RSI0017 RSI0018 RSI0019 RSI0020 RSI0021 RSI0029 RSI0030 RSI0031 RSI0032 RSI0033 RSI0041 RSI0042 RSI0043 RSI0044 RSI0045 RSI0055 RSI0056 RSI0062 RSI0063 RSI0069 RSI0070 RSI0076 RSI0077 RSI0083 RSI0090 RSI0091 RSI0096 RSI0097 RSI0103 RSI0104 RSI0110 RSI0111 RSI0116 RSI0117 RSI0122 RSI0123 RSI0128 RSI0129 RSI0134 RSI0135 RSI0136 RSI0140 RSI0141 RSI0142 RSI0146 RSI0147 RSI0148 RSI0152 RSI0153 RSI0154 RSI0158 RSI0159 RSI0160 RSI0170 RSI0171 RSI0172 RSI0176 RSI0177RSI0178 | 45 | 12/12/2021 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Área Responsable** | **ID****Plan** | **Plan de tratamiento** | **Riesgo asociado** | **Tiempo para****implementar los planes de****tratamiento** | **Fecha de seguimiento** |
|  |  |  | RSI0182RSI0756RSI0757 |  |  |
| Equipos de Laboratorios - Grupo deEquipos de Laboratorio | PT125 | Hacer backups en la unidad T por usuario, así mismo el responsable de la carpeta compartidadebe hacer backup en dicha unidad | RSI0614 RSI0615 RSI0616 | 30 | 12/12/2021 |
| Equipos de Laboratorios - Grupo deEquipos de Laboratorio | PT126 | Backups en USB y disco personales, correos electrónicos comprimir con clave | RSI0770 | 30 | 12/12/2021 |
| Equipos de Laboratorios - Grupo deEquipos de Laboratorio | PT127 | Cifrar disco duro de portátiles por parte dela OTIC | RSI0614 RSI0615 RSI0616 | 45 | 12/12/2021 |
| Producción - Hacienda Galindo ySerpentario | PT128 | Digitalizar la información almacenada en el archivo para garantizar copia de la informaciónrelevante | RSI0416 RSI0417 | 45 | 12/12/2021 |
| Producción -Bioterio | PT129 | Ejecutar análisis de vulnerabilidades de seguridad sobre el servidor del piso técnico del bioterio | RSI0095 RSI0096 RSI0097 RSI0098 RSI0099RSI0100 | 45 | 12/12/2021 |
| Producción - Aseguramiento de laCalidad | PT130 | Comprimir el backup en USB con contraseña para su protección | RSI0710 RSI0711 | 20 | 12/12/2021 |
| Producción - Aseguramiento de la Calidad | PT131 | Implementación de Keepass para administración adecuada de contraseñas | RSI0053 RSI0095 RSI0476 RSI0477 RSI0488 RSI0489 RSI0492 RSI0493 RSI0632 RSI0633 RSI0634 RSI0644 RSI0645 RSI0646 RSI0652 RSI0653 RSI0654 RSI0710RSI0711 | 20 | 12/12/2021 |
| Gestión Ambiental - Área de Gestión Ambiental | PT132 | Hacer backups por usuario en Backup T periódicamente, quincenal incluyendo la carpeta compartida | RSI0551 RSI0604 RSI0605 RSI0606 RSI0607 RSI0676RSI0678 | 20 | 12/12/2021 |
| Gestión Ambiental - Área deGestión Ambiental | PT133 | Usar y borrar la USB después de uso | RSI0721 | 20 | 12/12/2021 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Área Responsable** | **ID****Plan** | **Plan de tratamiento** | **Riesgo asociado** | **Tiempo para****implementar los planes de****tratamiento** | **Fecha de seguimiento** |
| Gestión Ambiental - Área de Gestión Ambiental | PT134 | Enviar información en We Transfer, Google drive, mediante WinRAR con clave. | RSI0175 RSI0176 RSI0177RSI0178 | 20 | 12/12/2021 |
| Gestión Ambiental - Área de Gestión Ambiental | PT135 | El área donde se encuentra el archivo debe mantenerse con llave o alguien presente. | RSI0354 RSI0372 RSI0373 RSI0374RSI0375 | 25 | 12/12/2021 |
| Recursos Físicos | PT136 | Socializar que se debe hacer backup en la carpeta Backup T por usuario | RSI0537 RSI0568 RSI0569 RSI0570RSI0571 | 23 | 12/12/2021 |
| Recursos Físicos | PT137 | Gestionar la solicitud de adquisición de licencia de AutoCAD con OTIC para el arquitecto delárea | RSI0772 | 23 | 12/12/2021 |
| Recursos Físicos | PT138 | Asignar disco duro externo en custodia deljefe del área, y debe estar bajo llave | RSI0771 | 23 | 12/12/2021 |
| Recursos Físicos | PT139 | Socializar la medida de que Después deuso de USB se debe borrar la información del INS | RSI0771 | 23 | 12/12/2021 |
| Recursos Físicos | PT140 | Socializar toda información confidencial que sea transferida debe ir con clave con WinRAR,aplica para Contenedores no institucionales | RSI0743 RSI0744 | 23 | 12/12/2021 |
| Recursos Físicos | PT141 | Solicitud a TICS del cambio periódico de contraseña en el sistema SIAI | RSI0133 RSI0134 RSI0135 RSI0136RSI0138 | 23 | 12/12/2021 |
| Recursos Físicos | PT142 | Recomendar el uso de Keepass en caso de que se gestionen muchas contraseñas por usuario. | RSI0133 RSI0134 RSI0135 RSI0136 RSI0138 RSI0329 RSI0330 RSI0331 RSI0334 RSI0335 RSI0336 RSI0337 RSI0340 RSI0480 RSI0481 RSI0482 RSI0537 RSI0568 RSI0569RSI0771 | 23 | 12/12/2021 |
| Recursos Físicos | PT143 | Revisar contratos para verificar el funcionamiento de los controles de acceso, ej.:puesta en funcionamiento de talanqueras | RSI0773 | 23 | 12/12/2021 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Área Responsable** | **ID****Plan** | **Plan de tratamiento** | **Riesgo asociado** | **Tiempo para****implementar los planes de****tratamiento** | **Fecha de seguimiento** |
| Dirección General | PT144 | Hacer backup en carpeta de OTIC Backup T manual por usuario, quincenal | RSI0531 RSI0552 RSI0553 RSI0554 RSI0555 RSI0576 RSI0577 RSI0578RSI0579 | 20 | 12/12/2021 |
| Dirección General | PT145 | Solicitar repositorio autorizado parabackup histórico Outlook, trimestral | RSI0555 RSI0579 | 20 | 12/12/2021 |
| Dirección General | PT146 | El responsable de la carpeta compartidadebe hacer backup en backup T | RSI0774 | 20 | 12/12/2021 |
| Dirección General | PT147 | Cifrar discos duros de los portátiles delárea OTIC | RSI0775 | 45 | 12/12/2021 |
| Dirección General | PT148 | Borrar USB después de uso | RSI0776 | 20 | 12/12/2021 |
| Dirección General | PT149 | Para toda información que se transmita a repositorio externos, Dropbox, Google drive, WeTransfer, correos personales, asignar clavemediante WinRAR a la información confidencial | RSI0777 | 20 | 12/12/2021 |
| Dirección General- Comunicaciones | PT150 | Hacer backup en la unidad de T de la OTIC y si está lleno solicitar espacio adicional | RSI0576 RSI0577 RSI0578RSI0579 | 20 | 12/12/2021 |
| Dirección General- Comunicaciones | PT151 | Borrar USB después de uso | RSI0778 | 20 | 12/12/2021 |
| Dirección General- Comunicaciones | PT152 | toda información de carácter confidencial que se transmita en medios personales y externos ej.: WeTransfer, Dropbox, disco duro personal debetener clave con WinRAR | RSI0779 | 20 | 12/12/2021 |
| Dirección General- Comunicaciones | PT153 | Validar el uso de carpetas compartidas con personal contratista que trae equipos portátilespersonales | RSI0579 | 35 | 12/12/2021 |
| Dirección General- Comunicaciones | PT154 | Validar si es posible asignar un celular corporativo para el manejo de redes socialesinstitucionales | RSI0779 | 45 | 12/12/2021 |
| Redes en SaludPública - Grupo Virología | PT155 | Hacer backup T de la OTIC, quincenal y decarpetas compartidas | RSI0780 RSI0781 | 20 | 12/12/2021 |
| Redes en SaludPública - Grupo Virología | PT156 | Evitar el uso de información institucionalportátiles personales | RSI0782 | 20 | 12/12/2021 |
| Redes en SaludPública - Grupo Virología | PT157 | USB Usarla y después de uso borrarla | RSI0783 | 20 | 12/12/2021 |
| Redes en Salud Pública - Grupo Virología | PT158 | Toda información que se transmita externamente a sitios como. Dropbox, Google drive, WeTransfer y discos duros externos debeestar en archivo comprimido con clave WinRAR | RSI0784 | 20 | 12/12/2021 |
| Redes en SaludPública - Grupo Virología | PT159 | En caso de manejar muchas contraseñasusar la aplicación Keepass | RSI0784 | 20 | 12/12/2021 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Área Responsable** | **ID****Plan** | **Plan de tratamiento** | **Riesgo asociado** | **Tiempo para****implementar los planes de****tratamiento** | **Fecha de seguimiento** |
| Redes en Salud Pública - Grupo Química y Toxicología | PT160 | Hacer backup T de la OTIC, quincenal y de carpetas compartidas | RSI0550 RSI0600 RSI0601 RSI0602RSI0603 | 20 | 12/12/2021 |
| Redes en Salud Pública - Grupo Química yToxicología | PT161 | Evitar el uso de información institucional portátiles personales | RSI0528 RSI0529 | 45 | 12/12/2021 |
| Redes en Salud Pública - Grupo Química yToxicología | PT162 | USB Usarla y después de uso borrarla | RSI0530 RSI0785 | 20 | 12/12/2021 |
| Redes en Salud Pública - Grupo Química y Toxicología | PT163 | Toda información que se transmita externamente a sitios como. Dropbox, Google drive, WeTransfer y discos duros externos debeestar en archivo comprimido con clave WinRAR | RSI0786 | 20 | 12/12/2021 |
| Redes en Salud Pública - Grupo Química yToxicología | PT164 | En caso de manejar muchas contraseñas usar la aplicación Keepass | RSI0527 | 20 | 12/12/2021 |
| Investigación en Salud Pública - Salud Ambiental y Laboral | PT165 | Hacer backup en repositorio de la OTIC, mensual, Carpetas compartidas | RSI0664 RSI0666 RSI0667 RSI0787 RSI0788RSI0789 | 20 | 12/12/2021 |
| Investigación en Salud Pública - SaludAmbiental y Laboral | PT166 | Borrar USBs después de su uso | RSI0790 | 20 | 12/12/2021 |
| Investigación en Salud Pública - SaludAmbiental y Laboral | PT167 | Hacer bakcup con contraseña de WinRAR | RSI0787 RSI0788 RSI0789 | 30 | 12/12/2021 |
| Investigación en Salud Pública - SaludAmbiental y Laboral | PT168 | Verificar la posibilidad de compartir y crear usuarios a repositorios oficiales del INS | RSI0791 | 45 | 12/12/2021 |
| Investigación en Salud Pública - SaludAmbiental y Laboral | PT169 | En caso de manejar muchas contraseñas usar la aplicación Keepass | RSI0665 | 20 | 12/12/2021 |
| Investigación en salud pública -Microbiología | PT170 | Backup de computadores del área en repositorio de la OTIC mensual | RSI0797 RSI0798 RSI0799 | 20 | 12/12/2021 |
| Investigación en salud pública -Microbiología | PT171 | Hacer backup de las carpetas en repositorio de la OTIC | RSI0797 RSI0798 RSI0799 | 20 | 12/12/2021 |
| Investigación en salud pública -Microbiología | PT172 | USB usarla y borrarla después de su uso | RSI0800 | 20 | 12/12/2021 |
| Investigación en salud pública -Microbiología | PT173 | Cuando se maneje Dropbox, disco duro externo, correos personales, WeTransfer, Googledrive comprimir archivo con WinRAR y clave | RSI0801 | 20 | 12/12/2021 |
| Redes en salud pública - Microbiología | PT174 | Solicitar espacio en SharePoint para publicar y compartir información (BD Reporte dehospitales) | RSI0801 | 45 | 12/12/2021 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Área Responsable** | **ID****Plan** | **Plan de tratamiento** | **Riesgo asociado** | **Tiempo para****implementar los planes de****tratamiento** | **Fecha de seguimiento** |
| Investigación en salud pública -Microbiología | PT175 | La información confidencial que se envíe a cuentas personales debe tener clave con WinRAR | RSI0801 | 30 | 12/12/2021 |
| Investigación en salud pública -Microbiología | PT176 | Uso de keepass para gestión de contraseñas | RSI0800 RSI0801 | 20 | 12/12/2021 |
| Investigación en salud pública - Nutrición | PT177 | Los Backup de computadores del área deben realizarse en repositorio de la OTIC cada dos meses | RSI0543 RSI0584 RSI0585 RSI0586RSI0587 | 20 | 12/12/2021 |
| Investigación en salud pública - Nutrición | PT178 | Hacer backup de las carpetas en repositorio de la OTIC | RSI0543 RSI0584 RSI0585 RSI0586RSI0587 | 20 | 12/12/2021 |
| Investigación en salud pública - Nutrición | PT179 | USB usarla y borrarla después de su uso | RSI0704 RSI0705 RSI0708RSI0709 | 20 | 12/12/2021 |
| Investigación en salud pública - Nutrición | PT180 | Cuando se maneje Dropbox, disco duro externo, correos personales, WeTransfer, Google drive comprimir archivo con WinRAR y clave | RSI0704 RSI0705 RSI0708 RSI0709 RSI0724 RSI0725 RSI0726 RSI0727 RSI0728RSI0729 | 20 | 12/12/2021 |
| Investigación ensalud pública - Nutrición | PT181 | Solicitar espacio en SharePoint parapublicar y compartir información | RSI0802 | 45 | 12/12/2021 |
| Investigación ensalud pública - Nutrición | PT182 | Información confidencial que se envíe acuentas personales debe tener clave | RSI0802 | 20 | 12/12/2021 |
| Investigación ensalud pública - Nutrición | PT183 | Uso de keepass para gestión decontraseñas | RSI0503 RSI0802 | 20 | 12/12/2021 |
| Investigación en salud pública -Entomología | PT184 | Hacer backup de computadores del área en repositorio de la OTIC cada 2 meses | RSI0803 RSI0804 RSI0805 | 20 | 12/12/2021 |
| Investigación en salud pública -Entomología | PT185 | Hacer backup de las carpetas en repositorio de la OTIC | RSI0803 RSI0804 RSI0805 | 20 | 12/12/2021 |
| Investigación en salud pública -Entomología | PT186 | USB usarla y borrarla después de su uso | RSI0806 | 20 | 12/12/2021 |
| Investigación en salud pública -Entomología | PT187 | Cuando se maneje Dropbox, disco duro externo, correos personales, WeTransfer, Googledrive comprimir archivo con WinRAR y clave | RSI0807 | 20 | 12/12/2021 |
| Investigación en salud pública -Entomología | PT188 | Solicitar espacio en SharePoint para publicar y compartir información | RSI0806 | 30 | 12/12/2021 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Área Responsable** | **ID****Plan** | **Plan de tratamiento** | **Riesgo asociado** | **Tiempo para****implementar los planes de****tratamiento** | **Fecha de seguimiento** |
| Investigación en salud pública -Entomología | PT189 | Información confidencial que se envíe a cuentas personales debe tener clave | RSI0807 | 20 | 12/12/2021 |
| Investigación en salud pública -Entomología | PT190 | Uso de keepass para gestión de contraseñas | RSI0807 | 20 | 12/12/2021 |
| Investigación en salud pública -Parasitología | PT191 | Hacer backup de computadores del área en repositorio de la OTIC cada dos meses | RSI0808 RSI0809 RSI0810 | 20 | 12/12/2021 |
| Investigación en salud pública -Parasitología | PT192 | Hacer backup de las carpetas en repositorio de la OTIC | RSI0808 RSI0809 RSI0810 | 20 | 12/12/2021 |
| Investigación en salud pública -Parasitología | PT193 | USB usarla y borrarla después de su uso | RSI0811 | 20 | 12/12/2021 |
| Investigación en salud pública -Parasitología | PT194 | Cuando se maneje Dropbox, disco duro externo, correos personales, WeTransfer, Googledrive comprimir archivo con WinRAR y clave | RSI0812 | 20 | 12/12/2021 |
| Investigación en salud pública -Parasitología | PT195 | Solicitar espacio en SharePoint para publicar y compartir información | RSI0812 | 30 | 12/12/2021 |
| Investigación en salud pública -Parasitología | PT196 | Información confidencial que se envíe a cuentas personales debe tener clave | RSI0812 | 20 | 12/12/2021 |
| Investigación en salud pública -Parasitología | PT197 | Uso de keepass para gestión de contraseñas | RSI0812 | 20 | 12/12/2021 |
| Investigación en salud pública - Parasitología | PT198 | Se requiere acceso al sistema, poner en funcionamiento nuevamente, desde hace un año no se ha podido usar, las historias se manejanfísicas. Gestionar con la OTIC | RSI0812 | 45 | 12/12/2021 |
| Investigación en salud pública - Morfología | PT199 | Hacer backup de computadores del área en repositorio de la OTIC cada dos meses | RSI0813 RSI0814RSI0815 | 20 | 12/12/2021 |
| Investigación en salud pública - Morfología | PT200 | Hacer backup de las carpetas en repositorio de la OTIC | RSI0813 RSI0814RSI0815 | 20 | 12/12/2021 |
| Investigación ensalud pública - Morfología | PT201 | USB usarla y borrarla después de su uso | RSI0816 | 20 | 12/12/2021 |
| Investigación en salud pública - Morfología | PT202 | Cuando se maneje Dropbox, disco duro externo, correos personales, WeTransfer, Googledrive comprimir archivo con WinRAR y clave | RSI0817 | 20 | 12/12/2021 |
| Investigación ensalud pública - Morfología | PT203 | Solicitar espacio en SharePoint parapublicar y compartir información | RSI0817 | 30 | 12/12/2021 |
| Investigación ensalud pública - Morfología | PT204 | Información confidencial que se envíe acuentas personales debe tener clave | RSI0817 | 20 | 12/12/2021 |
| Investigación ensalud pública - Morfología | PT205 | Uso de keepass para gestión decontraseñas | RSI0817 | 20 | 12/12/2021 |
| Investigación en salud pública - Fisiología | PT206 | Hacer backup de computadores en el repositorio de la OTIC cada dos meses | RSI0818 RSI0819RSI0820 | 20 | 12/12/2021 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Área Responsable** | **ID****Plan** | **Plan de tratamiento** | **Riesgo asociado** | **Tiempo para****implementar los planes de****tratamiento** | **Fecha de seguimiento** |
| Investigación en salud pública - Fisiología | PT207 | Hacer backup de las carpetas en repositorio de la OTIC | RSI0818 RSI0819RSI0820 | 20 | 12/12/2021 |
| Investigación ensalud pública - Fisiología | PT208 | USB usarla y borrarla después de su uso | RSI0821 | 20 | 12/12/2021 |
| Investigación en salud pública - Fisiología | PT209 | Cuando se maneje Dropbox, disco duro externo, correos personales, WeTransfer, Googledrive comprimir archivo con WinRAR y clave | RSI0822 | 20 | 12/12/2021 |
| Investigación ensalud pública - Fisiología | PT210 | Solicitar espacio en SharePoint parapublicar y compartir información | RSI0822 | 30 | 12/12/2021 |
| Investigación ensalud pública - Fisiología | PT211 | Información confidencial que se envíe acuentas personales debe tener clave | RSI0822 | 20 | 12/12/2021 |
| Investigación ensalud pública - Fisiología | PT212 | Uso de keepass para gestión decontraseñas | RSI0822 | 20 | 12/12/2021 |
| Redes en saludpública- Entomología | PT213 | Hacer backup de computadores en repositorio de la OTIC cada dos meses | RSI0823 RSI0824 RSI0825 | 20 | 12/12/2021 |
| Redes en saludpública- Entomología | PT214 | Hacer backup de las carpetas en repositorio de la OTIC | RSI0823 RSI0824 RSI0825 | 20 | 12/12/2021 |
| Redes en saludpública- Entomología | PT215 | USB usarla y borrarla después de su uso | RSI0826 | 20 | 12/12/2021 |
| Redes en saludpública- Entomología | PT216 | Cuando se maneje Dropbox, disco duro externo, correos personales, WeTransfer, Googledrive comprimir archivo con WinRAR y clave | RSI0827 | 20 | 12/12/2021 |
| Redes en saludpública- Entomología | PT217 | Solicitar espacio en SharePoint para publicar y compartir información | RSI0827 | 30 | 12/12/2021 |
| Redes en saludpública- Entomología | PT218 | Información confidencial que se envíe a cuentas personales debe tener clave | RSI0827 | 20 | 12/12/2021 |
| Redes en saludpública- Entomología | PT219 | Uso de keepass para gestión de contraseñas | RSI0827 | 20 | 12/12/2021 |
| Redes en saludpública- Entomología | PT220 | Solicitar que pida cambio de contraseña periódico | RSI0828 RSI0829 | 20 | 12/12/2021 |
| Redes en saludpública- Entomología | PT221 | Probar los backups del área | RSI0828 RSI0829 | 20 | 12/12/2021 |
| Redes en saludpublica Subdirección detrasplantes REDATA y bancos de sangre SIHEVI - Sistema de información dehemo vigilancia | PT222 | Solicitar análisis de vulnerabilidades y mitigación periódica del sistema SIHEVI por parte de la OTIC | RSI0830 | 75 | 12/12/2021 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Área Responsable** | **ID****Plan** | **Plan de tratamiento** | **Riesgo asociado** | **Tiempo para****implementar los planes de****tratamiento** | **Fecha de seguimiento** |
| Redes en saludpublica Subdirección detrasplantes REDATA y bancos de sangre SIHEVI - Sistema de información dehemo vigilancia | PT223 | Solicitar cambio de contraseña periódico | RSI0830 | 75 | 12/12/2021 |
| Redes en saludpublica Subdirección detrasplantes REDATA y bancos de sangre SIHEVI - Sistema de información dehemo vigilancia | PT224 | Solicitar Keepass a la mesa de ayuda | RSI0830 | 20 | 12/12/2021 |
| Investigación en salud publicaSalud materna y perinatal | PT225 | Hacer backup periódico en repositorio dela OTIC | RSI0831 RSI0832 RSI0833 | 20 | 12/12/2021 |
| Investigación en salud publicaSalud materna y perinatal | PT226 | Información en discos duros, o que sea enviado a repositorios externos debe tener clavecon WinRAR | RSI0738 | 30 | 12/12/2021 |
| Investigación en salud publicaSalud materna y perinatal | PT227 | USB deben usarse y borrarse después desu uso | RSI0834 | 20 | 12/12/2021 |
| Dirección de Vigilancia - Salud mental ylesiones de causa externa | PT228 | Hacer backup periódico en repositorio dela OTIC | RSI0623 RSI0624 RSI0625 | 20 | 12/12/2021 |
| Dirección de Vigilancia - Salud mental ylesiones de causa externa | PT229 | Información en discos duros, o que sea enviado a repositorios externos debe tener clavecon WinRAR | RSI0779 | 20 | 12/12/2021 |
| Dirección de Vigilancia - Salud mental ylesiones de causa externa | PT230 | USB deben usarse y borrarse después desu uso | RSI0778 | 20 | 12/12/2021 |
| Dirección de Vigilancia - Salud mental ylesiones de causa externa | PT231 | Solicitar Keepass a la mesa de ayuda | RSI0779 | 20 | 12/12/2021 |
| Investigación en Salud Pública - Biblioteca | PT232 | Hacer backup de información en repositorio institucional de la OTIC, trimestral | RSI0564 RSI0565 RSI0566RSI0567 | 20 | 12/12/2021 |
| Investigación enSalud Pública - Biblioteca | PT233 | USB deben usarse y borrarse después desu uso | RSI0837 | 20 | 12/12/2021 |
| Investigación en Salud Pública - Biblioteca | PT234 | Usar keepass en caso de manejar muchas contraseñas | RSI0564 RSI0565 RSI0566RSI0567 | 20 | 12/12/2021 |
| Investigación en Salud Pública - Biblioteca | PT235 | Información en discos duros, o que sea enviado a repositorios externos debe tener clavecon WinRAR | RSI0837 | 20 | 12/12/2021 |
| Investigación en Salud Pública -Micobacterias | PT236 | Hacer backup de información en repositorio institucional de la OTIC, trimestral | RSI0838 RSI0839 RSI0840 | 20 | 12/12/2021 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Área Responsable** | **ID****Plan** | **Plan de tratamiento** | **Riesgo asociado** | **Tiempo para****implementar los planes de****tratamiento** | **Fecha de seguimiento** |
| Investigación en Salud Pública -Micobacterias | PT237 | USB deben usarse y borrarse después desu uso | RSI0841 | 20 | 12/12/2021 |
| Investigación en Salud Pública -Micobacterias | PT238 | Usar keepass en caso de manejar muchas contraseñas | RSI0842 | 20 | 12/12/2021 |
| Investigación en Salud Pública -Micobacterias | PT239 | Información en discos duros, o que sea enviado a repositorios externos debe tener clavecon WinRAR | RSI0842 | 20 | 12/12/2021 |
| Investigación en Salud Pública - CEMIN | PT240 | Hacer backup de información en repositorio institucional de la OTIC, quincenal | RSI0843 RSI0844RSI0845 | 20 | 12/12/2021 |
| Investigación enSalud Pública - CEMIN | PT241 | USB deben usarse y borrarse después desu uso | RSI0846 | 20 | 12/12/2021 |
| Investigación enSalud Pública - CEMIN | PT242 | Usar keepass en caso de manejar muchascontraseñas | RSI0847 | 20 | 12/12/2021 |
| Investigación en Salud Pública - CEMIN | PT243 | Información en discos duros, o que sea enviado a repositorios externos debe tener clavecon WinRAR | RSI0847 | 20 | 12/12/2021 |
| Investigación en Salud Pública - Subdirección investigacióncientífica y tecnológica | PT244 | Hacer backup de información en repositorio institucional de la OTIC, mensual | RSI0848 RSI0849 RSI0850 | 20 | 12/12/2021 |
| Investigación en Salud Pública - Subdirección investigacióncientífica y tecnológica | PT245 | USB deben usarse y borrarse después desu uso | RSI0851 | 20 | 12/12/2021 |
| Investigación en Salud Pública - Subdirección investigacióncientífica y tecnológica | PT246 | Información en discos duros, o que sea enviado a repositorios externos debe tener clave con WinRAR | RSI0852 | 20 | 12/12/2021 |
| Investigación en Salud Pública - Subdirección investigacióncientífica y tecnológica | PT247 | Usar keepass en caso de manejar muchas contraseñas | RSI0852 | 20 | 12/12/2021 |
| Investigación en Salud Pública - Subdirección deinnovación | PT248 | Hacer backup de información en repositorio institucional de la OTIC, mensual | RSI0853 RSI0854 RSI0855 | 20 | 12/12/2021 |
| Investigación en Salud Pública - Subdirección deinnovación | PT249 | USB deben usarse y borrarse después desu uso | RSI0856 | 20 | 12/12/2021 |
| Investigación en Salud Pública - Subdirección deinnovación | PT250 | Información en discos duros, o que sea enviado a repositorios externos debe tener clave con WinRAR | RSI0857 | 20 | 12/12/2021 |
| Observatorio Nacional de Salud Grupo de Análisis y Divulgación | PT251 | Solicitar equipos propios del INS, evitar el uso de equipos personales | RSI0515 RSI0516 RSI0517RSI0518 | 45 | 12/12/2021 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Área Responsable** | **ID****Plan** | **Plan de tratamiento** | **Riesgo asociado** | **Tiempo para****implementar los planes de****tratamiento** | **Fecha de seguimiento** |
| Observatorio Nacional de Salud Grupode Análisis y Divulgación | PT252 | Solicitar espacio en SharePoint o One Drive para publicar y compartir información | RSI0740 RSI0741 RSI0742 | 45 | 12/12/2021 |
| Observatorio Nacional de Salud Grupo de Análisis y Divulgación | PT253 | Hacer seguimiento de análisis de vulnerabilidades con la OTIC a los repositorios donde se tiene información del observatorio | RSI0101 RSI0102 RSI0103 RSI0104 RSI0105 RSI0106 RSI0107RSI0108 | 45 | 12/12/2021 |

***Nota:*** *Los riesgos a los cuales están asociados dichos planes de tratamiento pueden ser consultados mediante el código del riesgo en la Matriz de Análisis de Riesgos de Seguridad de la información del INS.*



# CONCLUSIONES

Como se mencionó en los dos informes previos en general se identificó baja concienciación a nivel de los posibles riesgos de seguridad de la información que se pueden materializar afectando la confidencialidad, integridad o disponibilidad de la información requerida para el desarrollo de los procesos organizacionales. De hecho, en cada socialización de riesgos se vio la necesidad de explicar conceptos básicos relacionados con la seguridad de la información y la gestión de riesgos, como: activo de información, contenedor, controles, tipos de riesgos, confidencialidad, integridad, disponibilidad, planes de tratamiento.

Se explico que la actividad era una consultoría razón por la cual se requería la mayor sinceridad posible con el fin de mejorar la seguridad de la información en la entidad.

Se identificó una periodicidad muy alta en la ejecución de backups de la información almacenada en los equipos de trabajo institucionales, la mayoría de las áreas indicaban que los backups se ejecutaban trimestral o semestralmente, o cuando una persona del área se retiraba.

Se identificaron contenedores de información personales en los que se almacena información institucional, junto con información personal de los propietarios, como son: Memorias USB, discos duros externos, y portátiles.

También se identificó el intercambio de información a correos electrónicos personales, o repositorios de almacenamiento en la nube personales como: Dropbox, Google Drive, We Transfer.

Adicionalmente se identificó el almacenamiento de contraseñas en repositorios no seguros, como: agendas, bloc de notas, archivos en Excel.

Por otra parte, en cuanto a la seguridad informática se identificaron riesgos que pueden afectar la información almacenada en los servidores administrados por el INS, y que están relacionados con la ausencia de análisis y mitigación de vulnerabilidades de manera periódica, contratos de mantenimiento preventivo y correctivo, control de acceso a sistemas informáticos, gestión de control de cambios, gestión de incidentes y gestión de continuidad del negocio.



# RECOMENDACIONES

Teniendo en cuenta que el Manual de Políticas de Seguridad de la Información aún no se encuentra aprobado por el INS, y es el documento en el que se establecen controles específicos para evitar este tipo de riesgos, se recomendó la implementación de planes de tratamiento en cada una de las áreas con el fin de minimizar la probabilidad y el impacto de dichos riesgos, algunos de los planes de tratamiento sugeridos son:

* Hacer backups periódicos en el repositorio autorizado por la OTIC, teniendo en cuenta factores como la cantidad de información producida o modificada a la semana, quincenalmente o mensualmente. Esto ayudo a definir unas periodicidades en la ejecución de los backups de acuerdo a las necesidades de cada área.
* Una vez utilizada las USBs borrar su contenido.
* Evitar el uso de repositorios en la nube personales, como: Dropbox, Google Drive o We Transfer, y solicitar el apoyo de la OTIC para compartir información de manera segura mediante medios institucionales como Sharepoint o One Drive.
* Comprimir archivos confidenciales con contraseña para el intercambio de información a repositorios externos.
* Usar la aplicación KeePass para almacenar las contraseñas a cargo de manera segura.
* Usar contraseñas fuertes, se explicó un método sencillo de para generar contraseñas fuertes difíciles de vulnerar por atacantes informáticos.

En cuanto a la seguridad informática se recomendaron los siguientes planes de tratamiento:

* Llevar a cabo análisis y la correspondiente mitigación de vulnerabilidades a la infraestructura de servidores administrados por el INS, al menos 2 veces al año.
* Ejecutar actividades de Ethical hacking a la infraestructura de servidores al menos 1 vez al año.
* Garantizar contrato de mantenimiento preventivo y correctivo de los servidores administrados por el INS.
	+ Cambiar el sistema de aire acondicionado temporal del Datacenter por uno de precisión.
	+ Poner en funcionamiento o cambiar el sistema contraincendios del DataCenter.
	+ Definir e implementar políticas de control de acceso a sistemas que prohíban el acceso del equipo de desarrollo a bases de datos de producción.
	+ Definir e implementar un proceso adecuado de gestión de cambios.
	+ Definir e implementar un proceso adecuado de gestión de incidentes.
	+ Definir e implementar un plan de recuperación de desastres tecnológicos DRP, que garantice la recuperación oportuna de los sistemas de información y aplicaciones críticas del INS.

Por otra parte, se mencionó que se llevaría a cabo seguimiento de la implementación de los planes de tratamiento acordados, mediante una aplicación que se encuentra en desarrollo por parte de la OTIC.