**Política de intercambio de información**

1. **Políticas y procedimientos para el intercambio de información y software**
2. Se deberá definir procedimientos para el intercambio de información de la RPJA, las cuales contemplaran:

* Proteger la información intercambiada de una interceptación, copiado, modificación, cambio de ruta y destrucción**.**
* Proteger la información sensible que está en forma de archivo adjunto.
* Realizar un seguimiento al tráfico de la red cuando se tenga evidencias de actividad inusual o detrimentos en el desempeño.

1. Se mantendrá un conjunto de guías y procedimientos que garanticen la mitigación de amenazas software malicioso en el uso de la comunicación electrónica.
2. Se establecerá las responsabilidades de los usuarios a fin de no comprometer a la organización por difamación, hostigamiento, personificación, reenvió de cadenas de correo y compra no autorizada.
3. **Acuerdos de intercambio**

Se debe establecer acuerdos de intercambio de información y software entre RPJA y terceros, considerando el grado de sensibilidad de la información y las consideraciones de seguridad sobre la misma.

1. Las peticiones de información por parte de organizaciones externas de control deberán ser dirigidas y aprobadas por los responsables de su custodia. Toda información institucional debe ser manejada de acuerdo a la legislación actual.
2. Procedimientos para la notificación de emisión, transmisión, envió y recepción.
3. Estándares para el empaquetado y transmisión.
4. Establecer responsabilidades y obligaciones en caso de pérdida de datos.
5. Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida.
6. Términos y condiciones de la licencia bajo la cual se suministra el software.
7. Información sobre la propiedad de la información suministrada y las condiciones de su uso.
8. Normas técnicas para la grabación y lectura de la información y del software.
9. Implementar controles especiales que puedan requerirse para proteger ítems sensibles.
10. **Medios físicos en transito**

Los medios físicos que contengan información deben ser protegidos contra acceso no autorizado, mal uso o corrupción durante su trasporte entre sedes. Las medidas para salvaguardar estos dispositivos deberán contemplar:

1. Controles especiales, cuando resulte necesario y según la sensibilidad de la información, a fin de protegerla contra divulgación o modificación no autorizadas. Como control mínimo para proteger la información durante el intercambio a través de medios removibles (pendrives, equipos portátiles, etc.), estos deberán estar protegidos mediante una aplicación de cifrado de disco.
2. Uso de recipientes cerrados y embalaje a prueba de apertura no autorizada si lo requiere.
3. **Seguridad en la mensajería electrónica**

La información en la mensajería electrónica debe ser protegida apropiadamente, para ello se debe contemplar:

1. Proteger el contenido de la mensajería de accesos no autorizados, modificaciones o negación del servicio. El acceso ilícito a la mensajería será sancionado según legislación actual.
2. Establecer procedimientos para la extracción de metadatos en documentos públicos antes de proceder a su envió.
3. Contemplar el correcto uso de las firmas electrónicas y digitales, así como las consideraciones legales correspondientes.
4. **Sistemas de información de negocios**

Se implementaran los mecanismos con el fin de proteger la información asociada con la interconexión de los sistemas de información, los cuales contemplaran:

1. Vulnerabilidades de la información en los sistemas de RPJA
2. Retención y resguardo de la información almacenada en el sistema.
3. Identificación de la posición o categoría de los usuarios, en directorios accesibles por otros usuarios.
4. Categorías de personal y contratistas o terceros a los que se permite el uso del sistema y las ubicaciones desde las cuales se puede acceder al mismo. Así como el acceso a determinadas instalaciones.
5. Limitación del acceso a la información de las actividades que desarrollan determinadas personas, por ejemplo aquellas que trabaja en proyectos sensibles.