GESTIÓN DE ACTIVOS, CLASIFICACIÓN Y CONTROL DE LA INFORMACIÓN

TIPO DE DOCUMENTO: Procedimiento

CÓDIGO: PRO GSI 015

I. AUTORIZACIONES

Elaboró:	*Revisó:*	*Autorizó:*
Ing. Salvador Santiago Araujo *Gerente Administrativo*	*C.P. Jerónimo Javier Mendoza Lara / Lic. Irais Dafne Mendoza Sánchez* *Director General / Director General Adjunto*	*C.P. Jerónimo Javier Mendoza Lara / Lic. Irais Dafne Mendoza Sánchez* *Director General / Director General Adjunto*

Última revisión: octubre 2025

No. de versión: 11

Fecha de emisión: Agosto 2015

Revisó: DGE

Aprobó: DGE

INDICE

CONTENIDO **PÁGINA**

II. OBJETIVO

Definir los lineamientos y la metodología para gestionar los activos de la información, la responsabilidad sobre los activos, así como la clasificación y etiquetado de la información.

III. ALCANCE

Aplica a todas las áreas, procesos y activos de la Organización, involucradas en el Sistema de Gestión de Seguridad de la Información.

IV. HISTORIAL DE CAMBIOS

Versión	Descripción de cambios	Autor(es)	Fecha de cambio
1	Versión inicial.	MBS	Agosto 2015
2	Adecuación para agregar el etiquetado y manipulación de la información.	MBS	Noviembre 2015
3	Cambio de Formato	LBR	Octubre 2016
4	Adecuación en el apartado 2 con respecto al uso de la carta responsiva.	LBR	Diciembre 2016
5	Adecuaciones al punto 6 y se agrega la tabla en el punto 9 con respecto al etiquetado de la información,	LBR	Mayo 2017
6	Se realizan adecuaciones en cuanto al etiquetado de la información	MAH	Enero 2018
7	Actualizaciones generales del procedimiento, inclusión de etiquetado de la información en cuanto información de las redes sociales e información publicada en la página web de la Organización	MAH	Junio 2019

8	Se hace mención de la vigencia de activos en el apartado 1 y se hace incorporan condiciones de actualización para la **Carta responsiva FOR GSI 031**	RFML	Mayo 2021
9	Se implementa el proceso para la realizacion del inventario de activos tecnologicos y software, asi como la conciliacion del mismo.	RFML	Julio 2021
10	Adecuaciones Generales	RFML	Enero 2022
11	Actualización del documento para reforzar la información y alinearla a los requisitos de la norma ISO/IEC 27001:2022.	SSA	Septiembre 2025

V. REFERENCIAS

- MAN GSI 001 Manual de gestión de seguridad de la información
- POL GSI 001 Políticas generales de seguridad de la información
- FOR GSI 031 Carta responsiva
- MAP REH 001 Mapa de proceso de Recursos Humanos
- PRO GSI 020 Gestión de incidentes
- PRO GSI 032 Respaldos y eliminación de la información

VI. ABREVIACIONES Y DEFINICIONES

Abreviaciones:

DGE	Director General / Director General Adjunto
GAD	Gerente Administrativo
CSG	Coordinador de Sistemas de Gestión
CST	Coordinador de Sistemas TI
N/A	No Aplica
SGC	Sistema de Gestión de Calidad
SGSI	Sistema de Gestión de Seguridad de la Información

Definiciones:

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

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

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

VII. DESARROLLO DE ACTIVIDADES

1. GESTIÓN DE ACTIVOS DE LA INFORMACIÓN

DESARROLLO DE INVENTARIO DE ACTIVOS TECNOLOGICOS Y SOFTWARE

Todos los activos de la organización están **identificados, clasificados y asignados a un responsable**, y se encuentran registrados en la plataforma **GLPI**, que funge como sistema oficial de control y seguimiento de activos.

En GLPI se documenta para cada activo:

- Fecha de alta y de asignación.
- Responsable designado (usuario y área).
- Plan de renovación y vigencia operativa.
- Estado del activo (activo, en mantenimiento, en baja).

El **Gerente Administrativo** es responsable de establecer la **vigencia operativa** de cada activo, con el objetivo de garantizar que todos los equipos y software se mantengan actualizados, funcionales y seguros.

Cuando un activo llegue al fin de su vigencia (por obsolescencia, incompatibilidad con parches de seguridad o bajo rendimiento), deberá ser retirado de la operación y reemplazado por un nuevo equipo o versión de software, asegurando la continuidad de los procesos de la organización.

Este inventario es revisado de manera **trimestral** por el área de Sistemas y la Gerencia Administrativa, conciliando la información registrada en GLPI con los resultados del **Monitoreo de Seguridad Informática (FOR-SIS-003)**, a fin de validar la exactitud de la información técnica y garantizar que los activos cumplen con los lineamientos de clasificación establecidos en el **apartado 6 – Clasificación de Activos de la Información** de este documento.

INVENTARIO DE HARDWARE

1. **Inventario completo**
    - Se ejecuta cuando se realiza el levantamiento inicial de activos tecnológicos o cuando se requiera una validación general del inventario.
    - El responsable de esta actividad es el Coordinador de Sistemas TI, con apoyo de los auxiliares de sistemas.
    - El inventario completo debe realizarse al menos una vez al años y documentarse en GLPI.

2. **Planificación del inventario**
    - El Gerente Administrativo o el Coordinador de Sistemas TI planifica la actividad con base en:
        - Activos disponibles.
        - Altas y bajas registradas en CIA-Desk.
        - Programas de renovación vigentes.
    - La planificación se realiza de forma trimestral, antes de cada ejercicio de conciliación de activos.

3. **Coordinación del inventario**
    - El Coordinador de TI organiza al equipo de auxiliares de sistemas, entregando instrucciones y formatos de apoyo.
    - Se asegura que cada auxiliar tenga acceso a GLPI para registrar y actualizar la información de los activos revisados.

4. Desarrollo de la actividad

- El auxiliar de sistemas recopila la información en presencia del usuario responsable.
- Los datos mínimos a registrar en GLPI son:

  a) Responsable (RRHH)
  b) Tipo de activo
  c) Marca y modelo
  d) Número de serie
  e) Procesador
  f) Memoria RAM
  g) Dirección MAC
  h) Tipo y capacidad de almacenamiento
  i) Software instalado
  j) Estado de BitLocker
  k) Estado del agente SentinelOne
  l) Certificado SSL Fortinet instalado

- Esta información se ingresa en GLPI en tiempo real y queda vinculada al ticket en CIA-Desk que dio origen a la revisión.

5. Novedades del inventario

- Cada nuevo activo adquirido debe ser registrado en GLPI por el Coordinador de TI en un plazo máximo de 5 días hábiles después de su recepción.
- La Gerencia Administrativa y el área de Sistemas revisan de forma trimestral las novedades para validar que el inventario se mantenga actualizado.

6. Detección de necesidad de modificación

- Cuando un usuario solicita soporte en CIA-Desk y se detecta un fallo o bajo rendimiento por obsolescencia, el auxiliar de sistemas genera un diagnóstico.
- El Gerente Administrativo determina la sustitución parcial (pieza) o total (equipo).
- Una vez realizado el cambio, GLPI se actualiza de inmediato y se cierra el ticket del usuario con evidencia.

7. Mantenimiento del inventario

- Durante los mantenimientos preventivos programados semestralmente, se valida que la configuración física de los equipos coincida con lo declarado en GLPI.
- La evidencia queda registrada en el formato FOR-SIS-001 – Conformidad de mantenimiento preventivo.

8. Actualización del inventario de activos tecnológicos

- Al finalizar cualquier cambio físico o sustitución de equipo, el auxiliar de sistemas informa al Coordinador de TI para actualizar GLPI con los nuevos datos.

- Se debe:

- Colocar la etiqueta de control de activo.
- Anexar la Carta Responsiva FOR-GSI-031 firmada por el usuario.
- Actualizar todos los campos técnicos en GLPI.

9. Conciliación de inventarios

- Se realiza cada 90 días por el área de Sistemas en conjunto con la Gerencia Administrativa.
- Esta conciliación se vincula con el FOR-SIS-003 – Monitoreo de Seguridad Informática, verificando que:
  - Usuarios estén actualizados.
  - Agentes SentinelOne activos.
  - BitLocker habilitado.
  - Certificado SSL Fortinet instalado.
- El reporte de conciliación es firmado por el Coordinador de TI y validado por el Gerente Administrativo.

Nota:

La renovación de equipos se realizará de acuerdo a la necesidad operativa, priorizando casos de obsolescencia frente a actualizaciones de Microsoft, incompatibilidad con parches de seguridad o firmware. La decisión será documentada mediante ticket en CIA-Desk y actualizada en GLPI.

INVENTARIO DE SOFTWARE Y LICENCIAMIENTO

La organización cuenta con el **Catálogo de Software y Aplicaciones Permitidas (LIS-GSI-004)**, en el que se definen los programas autorizados para la operación. Dicho catálogo establece de manera explícita qué software puede ser instalado en los equipos corporativos.

- Para los equipos y usuarios que están involucrados en el manejo, almacenamiento y tratamiento de información de clientes estratégicos (ej. CitiBanamex), el uso está limitado a: **Office 365, Outlook, navegador Edge, antivirus corporativo, BitLocker y Secure Zip**.
- El control del software instalado en cada activo se gestiona mediante **GLPI**, el cual reemplaza al inventario manual previo y constituye el sistema oficial de registro.
- El acceso al inventario de software y licenciamiento está restringido al **Coordinador de Sistemas TI, Gerencia Administrativa y Dirección General**.

1. Inventario completo

- Se ejecuta cuando se realiza el **inventario inicial** o cuando se requiere una **validación global del software instalado** en los activos.
- Incluye validación de licencias, versiones y cumplimiento con el catálogo LIS-GSI-004.
- El inventario completo debe realizarse al menos **una vez al año** y documentarse en GLPI.

2. Planificación del inventario

- El **Gerente Administrativo** o el **Coordinador de Sistemas TI** planifica las actividades de revisión del inventario con base en:
  - Facturas de compra y licencias vigentes.
  - Softwares instalados en activos corporativos.
  - Ciclos de renovación de licencias (ej. anuales o multianuales).

- La planificación se realiza de forma **trimestral**, considerando tanto las altas/bajas de software como las auditorías de licenciamiento.

3. Coordinación del inventario

- El **Coordinador de Sistemas TI** organiza al personal técnico para la ejecución de revisiones.
- Se entregan lineamientos claros para capturar información en GLPI y validar:
  - Licencia asignada.
  - Usuario y equipo responsable.
  - Vigencia y fecha de renovación.

4. Desarrollo de la actividad

El **auxiliar de sistemas** obtiene y registra en **GLPI** la información mínima de cada software:

a) Número de factura de compra.
b) Fecha de adquisición.
c) Fabricante/desarrollador.
d) Nombre y versión del software.
e) Número de licencia.
f) Vigencia de la licencia.
g) Usuario responsable.
h) Equipo en el que se encuentra instalado.

La información marcada como crítica (fabricante, nombre, versión, usuario y equipo) debe validarse directamente con el responsable del activo.

Cada registro en GLPI queda vinculado al **ticket en CIA-Desk** que dio origen a la revisión o instalación.

4. Conciliación del inventario de software

- El **Departamento de Sistemas** realiza una conciliación de inventario de software **cada 90 días**, en conjunto con el **FOR-SIS-003 – Monitoreo de Seguridad Informática (Usuarios Actualizados)**.
- En esta conciliación se valida:
  - Que el software instalado coincide con el inventariado en GLPI.
  - Que las licencias registradas están vigentes.
  - Que no existan softwares no autorizados fuera del catálogo LIS-GSI-004.
- El resultado de la conciliación se documenta en GLPI y se informa a la **Gerencia Administrativa**.

Propiedad de los activos

Todos los activos de la organización tienen un propietario o dueño responsable de garantizar la Confidencialidad, Integridad y Disponibilidad (CID) de la información, y un custodio o usuario que comparte corresponsabilidad sobre su uso correcto.

La identificación del propietario y del custodio de cada activo está registrada en GLPI, donde queda documentada la trazabilidad completa del activo, desde su adquisición hasta su baja.

- **Propietario o Dueño:**
  - Es responsable de la clasificación del activo de información.
  - Tiene autoridad para definir el alcance de acceso (consultar, crear, actualizar, borrar o destruir información).
  - Evalúa los riesgos asociados al activo y aprueba o rechaza solicitudes de acceso.
  - Promueve las sanciones en caso de accesos no autorizados, en función de la criticidad de la información afectada.
- **Custodio o Usuario:**
  - Es la persona que utiliza el activo asignado y accede a la información únicamente bajo autorización del propietario.
  - Está obligado a utilizar el activo conforme a las políticas de seguridad establecidas.
  - Es responsable del uso seguro de sus credenciales, contraseñas y del equipo asignado.
  - Debe reportar en CIA-Desk cualquier anomalía, falla técnica o uso indebido detectado.

1. USO ACEPTABLE DE LOS ACTIVOS

a. Responsabilidad sobre los activos

i. Todos los activos de la Organización tienen asignado a un responsable (propietario o usuario) para su administración y control.

ii. Los responsables deberán ser designados de acuerdo con el grado de responsabilidad del proceso en el cual intervengan.

iii. Esta responsabilidad se encuentra definida en el **GLPI** (responsable).

b. Responsabilidades de los propietarios de los activos de la información

i. Identificar los activos tecnológicos en su resguardo.

ii. Clasificar la información con base a su confidencialidad, integridad y disponibilidad.

iii. Responsabilidad de valorar los riesgos asociados a la información.

iv. Aprobar o rechazar la solicitud de accesos a la información.

v. Impulsar las sanciones para los accesos no autorizados, de acuerdo con su naturaleza y los daños ocasionados.

c. Responsabilidades de los usuarios de los activos de la información

i. Responsabilidad del uso de su cuenta, contraseña y equipo de cómputo asignado, así como de los medios de transmisión de información.

ii. Obtener la autorización formal del dueño a través del custodio, antes de intentar acceder a cualquier activo de información.

iii. Utilizar los sistemas de información solo para actividades de la Organización.

iv. No divulgar información clasificada sin autorización del dueño y conocer la clasificación de los activos de información que maneja.

2. REGLAS PARA EL PERSONAL

El personal acatará lo estipulado en el **Manual de gestión de seguridad de la información MAN GSI 001**, **Políticas generales de seguridad de la información POL GSI 001** y demás procedimientos que sean referentes al uso de activos propiedad de la Organización.

3. CRITICIDAD DE LOS ACTIVOS DE LA INFORMACIÓN

El atributo de criticidad permitirá establecer una priorización de los activos del **GLPI**, en función de los requerimientos de confidencialidad, integridad y disponibilidad, cuyos valores consideran la caracterización previamente realizada para cada activo. Los valores que pueden tomar cada uno de estos tres atributos se encuentran detallados en la **Tabla 1**.

- **Confidencialidad:** Necesidad de permitir el acceso al activo sola a las personas debidamente autorizadas de acuerdo con lo definido por la Organización. El acceso no autorizado tiene impacto para la Organización o terceros.

- **Integridad:** Necesidad de preservar la configuración y contenido de un activo de Información. Su modificación no deseada tiene consecuencias que generan distintos niveles de impacto.

- **Disponibilidad:** Necesidad de preservar el tiempo de acceso al activo bajo un umbral predefinido por la Organización. Sobrepasar dicho umbral implica indisponibilidad del activo, la que genera distintos niveles de impacto para la Organización o terceros. El valor de este atributo está directamente relacionado con la magnitud de dicho impacto.

Tabla 1

Variables asociadas a	Grado	Significado de la criticidad
CONFIDENCIALIDAD	Pública	El activo no tiene restricciones de acceso.
	Reservada	Activo de información cuyo acceso no autorizado tiene impacto para la Organización o terceros.
INTEGRIDAD	Baja	Activo de Información cuya modificación no deseada tiene consecuencias con impacto leve para la Organización o terceros.
	Media	Activo de Información cuya modificación no deseada tiene consecuencias con impacto significativo para la Organización o terceros.
	Alta	Activo de Información cuya modificación no deseada tiene consecuencias con impacto grave para la Organización o terceros.
DISPONIBILIDAD	Baja	Activo de Información cuya inaccesibilidad, tiene impacto leve para la Organización o terceros.
	Media	Activo de Información cuya inaccesibilidad, tiene impacto significativo para la Organización o terceros.
	Alta	Activo de Información cuya inaccesibilidad, tiene impacto grave para la Organización o terceros.

Los impactos para la Organización o terceros pueden ser cuantificables (monto monetario o entrega de servicio) y no cuantificables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.).

Criticidad: Esta columna es calculada automáticamente en el **GLPI**, en función de la tríada Confidencialidad-Integridad-Disponibilidad y puede tomar los siguientes Valores:

- **Baja:** Ninguno de los valores asignados a la tríada supera el valor “Público” o “Bajo”.
- **Media:** Alguno de los valores asignados a la tríada es “Medio”.

- **Alta:** Alguno de los valores asignados a la tríada es “Reservado” o “Alto”.

4. CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN

Para llevar a cabo la clasificación de los activos de la información, dentro del **GLPI** se cuenta con las siguientes indicaciones para su llenado, clasificación, etiquetado y manipulación:

a. **No. de serie:** Indica el número de serie dado por el fabricante al activo. No aplica para todos los activos.
b. **Dirección IP:** La dirección IP fija asignado al activo. No aplica para todos los activos.
c. **Identificador:** En este campo se debe incluir el código asignado al activo por la Organización (nuevo o preexistente). Este atributo debe permitir identificar de forma única al activo.
d. **Nombre del activo:** Nombre de identificación del activo de información, en este campo debe incluirse todos los activos de información identificados para la etapa, independiente de su medio de soporte y sus características.
e. **Tipo de activo:** Este atributo permite establecer la naturaleza del activo, calificándolo según los siguientes valores:
    a. **Equipo:** dispositivos que realizan o apoyan la realización de un proceso y contienen información.
    b. **Componente:** dispositivo, aparato, o elemento que apoya la realización de los procesos.
f. **Usuario del activo:** Nombre del usuario autorizado para utilizar el activo. No aplica para todos los activos.
g. **Descripción del uso del activo:** Breve descripción sobre el uso o las funciones que el activo desempeña.
h. **Propietario del activo:** Nombre del propietario autorizado para tomar decisiones respecto al activo. Se puede tratar de una persona concreta o de un área. Esto no implica necesariamente derecho de propiedad sobre el activo.
i. **Custodio del activo:** Nombre del responsable para el resguardo del activo. Se puede tratar de una persona concreta o área.
j. **Información de contacto del custodio del activo:** Datos de ubicación o área y extensión o teléfono del custodio del activo.
k. **Ubicación:** Corresponde al lugar físico o lógico donde se encuentra el activo mientras es utilizado en el proceso, esta descripción debe ser lo suficientemente detallada como para determinar a partir de esta información las condiciones de seguridad física en las que se encuentra el activo.
l. **Estatus del activo:** Puede ser desarrollo, producción, en desuso o baja.
m. **Clasificación:** De acuerdo a lo comentado en punto 5. Criticidad de los Activos de la Información.

5. DEVOLUCIÓN DE ACTIVOS

Cuando un propietario o usuario cause **baja de la organización** (según el **MAP-REH-001 – Mapa de proceso de Recursos Humanos**), se deberán ejecutar las siguientes actividades de forma inmediata para garantizar el control de los activos tecnológicos:

1. **Recepción del activo:**
    - El área de Recursos Humanos notifica al área de Sistemas mediante **CIA-Desk** sobre la baja del colaborador.
    - El usuario entrega el activo asignado en presencia del personal de Sistemas.
2. **Verificación técnica:**
    - El **auxiliar de sistemas** valida que el activo se encuentre en condiciones operativas y que no haya alteraciones de hardware o software no autorizadas.
    - Se verifica la correcta desactivación de credenciales, cuentas y accesos vinculados al activo.
    - Se comprueba que los controles de seguridad obligatorios (BitLocker, SentinelOne, certificado SSL Fortinet) permanezcan activos.

3. **Actualización en GLPI:**
   - El **Coordinador de TI** actualiza en **GLPI** el estatus del activo, cambiándolo de "Asignado" a "Disponible" o "En revisión técnica", según corresponda.
   - Se reasigna a un nuevo responsable en GLPI una vez que Recursos Humanos confirme la nueva asignación.
4. **Carta Responsiva FOR-GSI-031:**
   - Se cancela la carta firmada por el colaborador saliente.
   - Se emite una nueva carta responsiva a nombre del nuevo usuario asignado.
5. **Reasignación del activo:**
   - El activo es asignado a un nuevo usuario autorizado, quedando reflejado en **GLPI** y respaldado con una nueva **Carta Responsiva FOR-GSI-031**.

2. CLASIFICACIÓN Y CONTROL DE LA INFORMACIÓN

6. ETIQUETADO DE LA INFORMACIÓN

Por funcionalidad para la Organización se declara el tipo de información en todos los mapas de proceso para que el personal tenga conocimiento de la clasificación de la información que maneja y las precauciones que debe tener en todo momento.

Declaramos que solo cuando se archiva la información físicamente es cuando será visible el sello de nivel de confidencialidad.

Información	Descripción	Clasificación	Quien tiene acceso	Disposición final
Los documentos de carácter electrónico	Formatos requisitados, registros internos y externos.	Restringido	Solo podrán tener acceso en dicha información el personal indicado en los mapas de proceso y los dueños de los activos e información.	El Área de Sistemas en conjunto con los dueños de la Información determinaran el tiempo de resguardo de la información.
Bases de datos	Información de clientes, información interna, información de proveedores.	Restringido	Solo podrán tener acceso en dicha información el personal indicado en los mapas de proceso y los dueños de los activos e información.	El Área de Sistemas en conjunto con los dueños de la información determinaran el tiempo de resguardo de la información.
Documentos en formato papel	Con información externa o interna donde que se obtiene como resultado de la operación del día a día, pero que se debe conservar como evidencia documentada.	Restringido	Solo podrán tener acceso en dicha información el personal indicado en los mapas de proceso.	Archivado en archivo muerto con cajas selladas "restringido". Se realiza la destrucción con un proveedor externo de acuerdo al procedimiento **Respaldos y eliminación de la información PRO GSI 032**.

Información en papel no necesaria de resguardar como información documentada	Información que surge de las áreas en el día a día, pero que su contenido no tiene información sensible interna, ni de clientes y que no es necesario guardar con evidencia documentada.	Interno	Personal indicado en mapas de proceso.	Se realiza la destrucción en la trituradora de la Organización.
Información verbal	Toda aquella que por la funcionalidad del proceso se transmite de modo verbal directo o por cualquier medio.	Restringido	Solo está permitida cuando es expresamente necesario para la prestación del servicio.	No aplica.
Información publicada en la página de Sistemas de Gestión	Documentación de los Sistemas de gestión y resultados generados de los mismos que es de interés de la alta Dirección se esté difundiendo constantemente.	Interno	Todo el personal de la Organización.	Coordinador de Sistemas de Gestión es el responsable de mantener las actualizaciones pertinentes.
Información contractual	Contratos donde se estipulan los términos y condiciones del negocio y que solo tiene acceso Dirección.	Confidencial	Dirección y solo cuando la misma requiere personal autorizado.	No aplica
Información publicada en la página web de la Organización	Nosotros, Servicios, Contacto y Aviso de privacidad de la Organización.	Público	Accesible públicamente.	La Dirección en conjunto con el Gerente Administrativo son los responsables de determinar la información publicada.
Redes sociales	Vacantes, dinámicas con personal, foto, puesto y nombre de colaboradores, infografías y videos orientados a buenas prácticas.	Público	Accesible públicamente	El Área de Recursos Humanos es el responsable de administrar la información publicada.

- **Confidencial:** Cuando el nivel de confidencialidad es tal que no puede tener acceso nadie más que el dueño de la información.

- **Restringido:** El nivel de confidencialidad está limitado solo a los puestos especificados en los Mapas de proceso.
- **Interno:** Información con un nivel bajo de confidencialidad que puede estar publicada o es generada por las actividades del día a día, pero no contiene información sensible.
- **Público:** Esta información no está sujeta a ningún tipo de tratamiento especial y sin restricciones de difusión.

Documentos en papel

- Documentos controlados con alguna de las siguientes leyendas:
  - ***DOCUMENTO CONTROLADO:*** *Su consulta en cualquier medio diferente a Intranet, no es válida como copia maestra de la Organización. Por ello,* ***su impresión en papel queda restringida a usos de formato y registro siempre validados por firmas autorizadas***.
  - La impresión en papel de este DOCUMENTO, o su consulta en cualquier otro medio diferente a Intranet, no es válida como documento oficial de la Organización, por lo que su uso es responsabilidad de la persona que lo imprima o consulte.
- Se declara que los contratos con proveedores y clientes son de acceso restringido, al igual que los expedientes del personal y los expedientes judiciales, así como la información contable, financiera y fiscal de la Organización.

Documentos electrónicos

- Se indica el nivel de confidencialidad en el pie de página o encabezado de cada documento.
- Se declara que las bases de datos que contienen datos personales de terceros, independientemente del medio y etapa de proceso, se etiquetan como confidenciales.
- La información electrónica contenida en la página de Sistemas de Gestión se etiqueta como de uso interno.
- La información publicada en la página web de la Organización y redes sociales se etiquetan como de acceso público.

Correo electrónico

Se indica el nivel de confidencialidad en el cuerpo del correo electrónico si el usuario lo considera necesario.

7. ASPECTOS A CONSIDERAR PARA EL MANEJO DE LA INFORMACIÓN

- Todas las personas que tienen acceso a información clasificada deben seguir las reglas enumeradas en el siguiente cuadro.
- La Dirección debe activar acciones disciplinarias cada vez que no se cumplan las reglas o si la información se transmite a personas no autorizadas.
- Cada incidente relacionado con el manejo de información clasificada debe ser reportado de acuerdo con el procedimiento **Gestión de incidentes PRO GSI 020**.
- Los activos de información pueden ser llevados fuera de las instalaciones solamente con autorización, de acuerdo a lo establecido en las **Políticas generales de seguridad de la información POL GSI 001**.

	Uso interno	Restringida *	Confidencial *

Documentos en papel	➢ Sólo las personas autorizadas pueden tener acceso. ➢ Si es enviado fuera de la Organización, el documento puede ir en sobre simple. ➢ Los documentos sólo pueden ser guardados en habitaciones sin acceso público. ➢ Los documentos deben ser retirados frecuentemente de impresoras.	➢ El documento puede ser almacenado en un gabinete, sin que quede expuesto. ➢ Los documentos pueden ser transferidos solo cuando el mapa de proceso lo indique. ➢ Si es enviado fuera a otra dependencia por especificación del cliente, el documento debe ser enviado con acuse de recibo. ➢ Los documentos deben ser retirados inmediatamente de impresoras. ➢ Solamente el propietario del documento puede copiarlo.	➢ El documento debe ser almacenado en lugar seguro y con llave. ➢ El documento puede ser transferido dentro y fuera de la Organización solamente por una persona confiable y en un sobre cerrado. ➢ No está permitido enviar el documento escaneado.
Documentos electrónicos	➢ Sólo las personas autorizadas pueden tener acceso. ➢ Cuando se intercambian archivos internamente a través de servicios como VPN, mensajería instantánea, archivos comunes, etc., no es necesario protegerse con contraseña. ➢ El acceso a los sistemas de información en los que están almacenados los documentos debe estar protegido por una clave segura.	➢ Sólo las personas con autorización para este documento pueden acceder a la parte del sistema de información en el que está guardado el documento. ➢ Cuando se intercambian archivos a través de servicios como VPN, mensajería instantánea, etc., de acuerdo a los Mapas de proceso.	➢ El documento debe ser almacenado en un formato encriptado (si el cliente lo requiere). ➢ El documento puede ser intercambiado a través de servicios como VPN, mensajería instantánea, encriptado o con contraseña (si el cliente lo requiere), etc.