

SEPTIEMBRE 2016

POLÍTICA DE USO, CUSTODIA Y SEGURIDAD DE LA INFORMACIÓN.



ÁREA: SISTEMAS





Código	PO-LS-04
Versión	1
Vigente a partir de	SEPTIEMBRE 2016

POLÍTICA DE USO, CUSTODIA Y SEGURIDAD DE LA INFORMACIÓN

ÍNDICE

A) Antecedente.....	3
B) Cambios del documento	3
Oficialización.....	4
1. Objetivo.....	5
2. Alcance	5
3. Definiciones	5
4. Políticas	6
4.1 En materia de normatividad interna.....	6
4.2 En materia de seguridad de activos de información	7
4.3 En materia de propiedad y responsabilidad de equipos de cómputo	7
4.4 En materia de seguridad en los sistemas de información y de cómputo	8
4.5 En materia de manipulación de medios removibles.....	8
4.6 En materia de seguridad y acceso a la información.....	9
4.7 En materia de clasificación de la información	9
4.8 En materia de identificación lógica de dispositivos conectados a la red.....	9
4.9 En materia de seguridad de cuentas de Usuario	9
4.10 En materia de seguridad de la información en el uso del correo electrónico.....	10
4.11 En materia de seguridad en el uso de internet.....	10
4.12 En materia de seguridad de la información relacionada con páginas corporativas y de servicios	10
4.13 En materia de accesos de equipos de tecnología a Oficinas Generales y Sucursales	11
4.14 En materia de seguridad en la baja y movimientos de empleados.....	11
4.15 En materia de manejo de incidentes de seguridad	11
4.16 En materia de continuidad del negocio	12
4.17 En materia de organización de seguridad de la información en la Dirección de Sistemas	12
4.18 En materia de control de accesos remotos:	13
4.19 En materia de seguridad perimetral e interna	13
4.20 En materia de destrucción de información (física/ lógica).....	13
4.21 En materia de requerimientos para la continuidad del Centro de Datos.....	13
5. Registros.....	14
6. Anexos	14
7. Referencias.....	14
8. Bibliografía.....	15



Código	PO-LS-04
Versión	1
Vigente a partir de	SEPTIEMBRE 2016

POLÍTICA DE USO, CUSTODIA Y SEGURIDAD DE LA INFORMACIÓN

Control de Cambios

A) Antecedente

Código	Documento Origen	Política/Procedimiento	Fecha de oficialización	Comentarios
03050100	Manual de Uso, Custodia y Seguridad de la Información.	Todo	Enero 2008	Se da de baja a la publicación de la Política de Uso, Custodia y Seguridad de la Información PO-LS-04

B) Cambios del documento

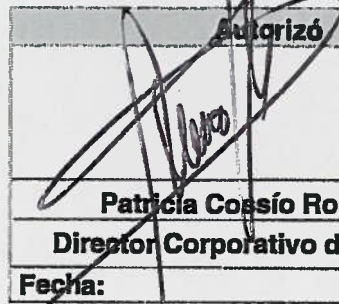
Fecha	Sección	Descripción del Cambio	Sustituye a la versión:	Justificación (Indicar el área solicitante)
Septiembre 2016	Todo el documento	Nuevo	Nuevo	Primera edición del documento, a solicitud del Subdirector de Sistemas.

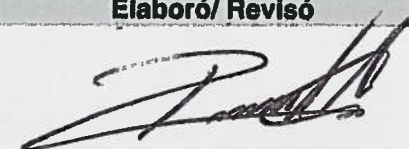


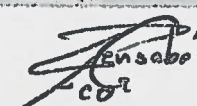
Código	PO-LS-04
Versión	1
Vigente a partir de	SEPTIEMBRE 2016


POLÍTICA DE USO, CUSTODIA Y SEGURIDAD DE LA INFORMACIÓN

Oficialización

Autorizó

Patricia Cossío Rodríguez
Director Corporativo de Sistemas
Fecha:

Elaboró/ Revisó

Roberto Aviña González
Subdirector de Sistemas
Fecha:

Revisó

Francisco Pensabé Gómez
Gerente de Seguridad y Gobierno de Sistemas
Fecha: 3/sep/2016

Elaboró

Vanessa Contreras Prado
Gerente de Normatividad y Control
Fecha: 03/sep/2016

Los dueños del proceso se comprometen a realizar la revisión y actualización del presente documento en el tiempo máximo establecido en la "Lista Maestra de Documentos".



Código	PO-LS-04
Versión	1
Vigente a partir de	SEPTIEMBRE 2016

POLÍTICA DE USO, CUSTODIA Y SEGURIDAD DE LA INFORMACIÓN

1. Objetivo

Establecer los lineamientos, directrices y criterios que regulen el uso, custodia y seguridad de la información que manejan los colaboradores de Nadro, dentro y fuera de la empresa.

2. Alcance

Aplica a todos los empleados de Nadro, en la observación y cumplimiento de las políticas definidas en el presente documento, en particular a los responsables de área en la supervisión del uso, custodia y seguridad de la información, por parte de los empleados.

3. Definiciones

Término	Definición
Activos de Información	Son aquellos recursos de información que poseen valor para la organización. Por tanto deben protegerse como: archivos, base de datos, contratos y acuerdos, documentación de sistemas, manuales de usuarios, material de formación, aplicaciones, software, equipos informáticos, equipos de comunicación, servicios informáticos y de comunicación, etc.
Amenaza	Es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos que causen pérdidas o daños a la información de la empresa.
Anti virus	Es un software diseñado para detectar y eliminar potencialmente virus y código malicioso, antes de que tengan oportunidad de causar daños a la información o en los sistemas.
Clasificación de Información	Es organizar la información según su contenido, tipo y atributos, así como su uso indicando si es de acceso restringido, confidencial, de uso interno y/o público.
Confidencialidad	Es asegurar la protección de la información y que sea compartida solamente entre organizaciones o personas autorizadas, para que no sea divulgada sin consentimiento.
Derechos de autor	Conjunto de normas jurídicas y principios incluidos en la normatividad informática, las cuales se encuentran regulados en la Ley Federal de Derechos de Autor.
Equipo (hardware)	Componentes físicos que forman parte de un equipo de cómputo (monitor, teclado, mouse, tarjetas de red, disco duro, procesador, etc.).
Firewall	Es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, el firewall determina los servicios de red que pueden ser accesados dentro y fuera de la red de la organización.
Impacto	Es un efecto producido por un agente interno o externo que puede o no ser medido en términos financieros.

POLÍTICA DE USO, CUSTODIA Y SEGURIDAD DE LA INFORMACIÓN

Término	Definición
Integridad	Asegurar que la información no es alterada en su contenido sin permiso ni control.
Password (contraseñas)	Es la palabra clave de acceso a los sistemas.
Red	Conjunto de dos o más computadoras interconectadas.
Respaldo	Copia de la información, archivos o documentos, con el objeto de tener la seguridad de que siempre se contará con ella, si el original se pierde.
Restauración	Es la recuperación o arreglo de los daños causados a un sistema, archivo o información.
Seguridad de información	Tiene como propósito proteger la información de los procesos del negocio, en todos los medios en los cuales se encuentre (información impresa en papel, almacenada en medio electrónicos o incluso, la información que cada persona conoce).
Sistemas de información	Conjunto de programas por los que se transmiten datos organizados, clasificados y útiles.
Software	Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.
Spyware	Los programas espía o spyware, son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento.
Spam	También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios no solicitados.
Virus	Programa informático que altera e infecta el funcionamiento de una computadora causando daños, efectos indeseables y hasta daños irreparables.

4. Políticas

4.1 En materia de normatividad interna

- 4.1.1 La Gerencia de Seguridad y Gobierno de Sistemas, debe vigilar los cambios en las plataformas vigentes y sus procesos operativos que expongan amenazas significativas, así como de revisar y supervisar los incidentes de seguridad y de proponer iniciativas que mitiguen los riesgos que afectan la seguridad de los sistemas de Nadro.
- 4.1.2 Todas las instalaciones e implementaciones de sistemas y equipos, deben apegarse al esquema de control de cambios con la participación de la Gerencia de Seguridad y Gobierno de Sistemas. Ver **“Procedimiento para la Gestión de Cambios en Sistemas PR-LS-20”**.

Código	PO-LS-04
Versión	1
Vigente a partir de	SEPTIEMBRE 2016

POLÍTICA DE USO, CUSTODIA Y SEGURIDAD DE LA INFORMACIÓN

4.2 En materia de seguridad de activos de información

- 4.2.1 La Gerencia de Seguridad y Gobierno de Sistemas, debe vigilar todos los cambios significativos en los activos de información que expongan amenazas mayores, la revisión y supervisión de los incidentes a la seguridad; así como proponer iniciativas que incrementen la Seguridad en los sistemas de NADRO.
- 4.2.2 Todas las instalaciones e implementaciones de sistemas y equipos, deben estar planeadas y notificadas al Director de negocio (Dueño del proceso), propietarios de los procesos del negocio y a la Gerencia de Seguridad y Gobierno de Sistemas. Ver **“Procedimiento para la Gestión de Cambios en Sistemas PR-LS-20”**.
- 4.2.3 Cada empleado es responsable de la seguridad de **los activos de información** que de manera individual manejen como parte del desempeño de sus labores diarias, sin embargo, cada empleado sabe que dicha información **es propiedad de NADRO**.
- 4.2.4 Cada administrador o custodio de los activos de información, debe establecer mecanismos para su acceso, incluyendo su validación.
- 4.2.5 Para el control físico (resguardo de equipo) y lógico (usuario y contraseña), todo empleado debe observar y cumplir los siguientes lineamientos:
- El equipo que permanezca dentro de las instalaciones deberá estar en un lugar seguro con llave, cuando sea posible.
 - En caso de que el empleado responsable del equipo tenga que ausentarse de su lugar, el equipo de cómputo deberá estar bloqueado para accesos no autorizados.
 - El equipo que no esté dentro de la organización nunca deberá ser desatendido en lugares públicos, por ejemplo: en los carros, conferencias, en los viajes, hoteles, taxis, aeropuertos, etc.
 - El Usuario no deberá poner los equipos de cómputo a la exposición de campos magnéticos.

4.3 En materia de propiedad y responsabilidad de equipos de cómputo

- 4.3.1 Toda la información y dispositivos de cómputo deben tener una persona responsable. Ver **“Procedimiento para la Gestión de Equipos de Trabajo para Usuarios del Negocio PR-LS-16”**.
- 4.3.2 La Gerencia de Seguridad y Gobierno de Sistemas, debe emitir un reporte que enliste una muestra variable de los accesos con los que cuenta cada usuario y validarlos de acuerdo a la descriptiva de puesto y funciones vigentes aprobadas por el negocio.
- 4.3.3 El Usuario debe dar aviso inmediatamente a la Mesa de Ayuda de Sistemas la desaparición, robo o extravió del equipo de cómputo o accesorios bajo su resguardo. Ver **“Procedimiento para la Gestión de Equipos de Trabajo para Usuarios del Negocio PR-LS-16”**.
- 4.3.4 El Usuario no debe instalar ningún tipo de software diferente al estándar de la organización, si no es justificado y autorizado por el Subdirector o Director del área de Sistemas. Ver **“Política para el Control de Licencias y Software PO-LS-02”**.

Código	PO-LS-04
Versión	1
Vigente a partir de	SEPTIEMBRE 2016

POLÍTICA DE USO, CUSTODIA Y SEGURIDAD DE LA INFORMACIÓN

4.3.5 Para optimizar el tiempo de vida útil de la batería de los dispositivos de cómputo, del cual el Usuario es responsable, se deberá apagar el equipo de cómputo al concluir la jornada laboral.

4.4 En materia de seguridad en los sistemas de información y de cómputo

4.4.1 La Dirección Corporativa de Sistemas es la encargada de aprobar la gestión de la demanda de dispositivos de cómputo, así como de cualquier adquisición de Software o actualización de licencias, captada por la Gerencia de Servicios de Soporte y Mesa de Ayuda, apegada al **“Procedimiento para la Adquisición de Bienes y Servicios PR-AC-35”**, para ratificar que ninguna otra área podrá evaluar Hardware o Software sin conocimiento de las Dirección Corporativa de Sistemas.

4.4.2 La Gerencia de Seguridad y Gobierno de Sistemas, debe verificar que el diseño de cualquier sistema, interface, o interconexión entre aplicativos, cuente con los controles apropiados y alineados a los requerimientos de seguridad e integridad de información, mismos que sólo deberán ser diseñados y ejecutados por el personal responsable, que deberá apegarse a los procedimientos vigentes de control de cambios del área. Ver **“Procedimiento para la Gestión de Cambios en Sistemas PR-LS-20”**.

4.4.3 Los mecanismos para la realización de respaldos y restauraciones en los equipos, sistemas y plataformas vigentes, están definidos en el **“Procedimiento para la Ejecución de Respaldos y Restauraciones Iseries, SAP/AIX, Bodega de Facturación y Carpetas Privadas y Compartidas PR-LS-13”**.

4.4.4 La Gerencia de Administración de Redes, debe administrar, mantener vigentes las versiones recomendadas por los fabricantes, así como operar los Dispositivos de Seguridad, tales como, Firewall, Anti-Spam, Anti-Spyware, bajo el estricto esquema de configuración definido por la Gerencia de Seguridad y Gobierno de Sistemas, lo cual garantizará la integridad de la información y el esquema de monitoreo de los procesos que operan con éstos dispositivos.

4.5 En materia de manipulación de medios removibles

4.5.1 El uso de los medios removibles (Dispositivos periféricos de cómputo de lectura o almacenamiento de información que no forman parte del equipo), será de uso exclusivo de aquellos usuarios que lo tengan declarado en su perfil de puesto, con la aprobación del Director del área responsable y de la Dirección Corporativa de Sistemas. Ver **“Política para el Control de Licencias y Software PO-LS-02”**.

4.5.2 La Gerencia de Seguridad y Gobierno de Sistemas es la única que puede auditar aleatoriamente los medios removibles, al menos 2 veces al año.

4.5.3 La activación o desactivación de cualquier medio removible debe efectuarlo sólo el personal de la Mesa de Ayuda de Sistemas, en apego al **“Procedimiento para la Atención de Incidentes y Requerimientos a Sistemas (Modelo de Soporte) PR-LS-20”**.

4.5.4 Todos los medios removibles que sean utilizados fuera de la arquitectura tecnológica de la organización, deben ser revisados por el Usuario ante una posible presencia de virus.

Código	PO-LS-04
Versión	1
Vigente a partir de	SEPTIEMBRE 2016

POLÍTICA DE USO, CUSTODIA Y SEGURIDAD DE LA INFORMACIÓN

4.6 En materia de seguridad y acceso a la información

- 4.6.1 Los accesos a la información de sistemas informáticos deben ser otorgados en apego al perfil de puesto autorizado previamente, o bien, las excepciones solicitadas debidamente justificadas y aprobadas en apego al **“Procedimiento para el ABC de Usuarios de SAP/AS400/Directorio Activo y Asignación de Roles PR-LS-09”**.
- 4.6.2 La baja de cuentas de usuarios, se realizarán en apego al **“Procedimiento para el ABC de Usuarios de SAP/AS400/Directorio Activo y Asignación de Roles PR-LS-09”**, previo al análisis del impacto al negocio

4.7 En materia de clasificación de la información

- 4.7.1 Los niveles de clasificación de información que NADRO establezca, deben ser definidos por el negocio y el área de Sistemas dará las normas a seguir, en lo referente a la seguridad, portabilidad, distribución y respaldo que desde el punto de vista de Sistemas corresponda.
- 4.7.2 Cada usuario debe asegurar la información contenida en los dispositivos o sistemas donde éste tenga algún tipo de acceso.

4.8 En materia de identificación lógica de dispositivos conectados a la red

- 4.8.1 La Gerencia de Servicios de Soporte y Mesa de Ayuda debe vigilar que:
- a) Todos los equipos de cómputo cuenten con (dependiendo el perfil autorizado del usuario):
 - i. Conectividad a los sistemas autorizados
 - ii. Versiones vigentes definidas por sistemas
 - b) Todo equipo de cómputo que no sea propiedad de la organización, debe contar con antivirus y parches actualizado para entrar a la red.

4.9 En materia de seguridad de cuentas de Usuario

- 4.9.1 Toda contraseña de Usuario de red de cualquier módulo, aplicación, Internet, AS/400, SAP, entre otros, es de carácter confidencial, por lo que por ningún motivo el Usuario debe proporcionar su contraseña a otro Usuario.
- 4.9.2 Las cuentas de Administrador son de uso exclusivo de Administradores de Sistemas, por lo que no deben ser transmitidas a ningún otro Usuario.
- 4.9.3 Todas las cuentas de Administrador y de operadores deben ser controladas por el área de Sistemas.
- 4.9.4 Los mecanismos para la parametrización de contraseñas en los sistemas de NADRO, su resguardo y custodia, así como lineamientos para el restablecimiento se encuentran definidas en la **“Política de Strong Password PO-LS-03”**.

Código	PO-LS-04
Versión	1
Vigente a partir de	SEPTIEMBRE 2016

POLÍTICA DE USO, CUSTODIA Y SEGURIDAD DE LA INFORMACIÓN

4.10 En materia de seguridad de la información en el uso del correo electrónico

- 4.10.1 El correo electrónico es una herramienta de trabajo, por lo que el empleado no debe usarlo para envío de información que no esté relacionada con sus actividades laborales.
- 4.10.2 El Usuario debe mantener depurado, clasificado y resguardado el contenido de su correo electrónico como medida de seguridad y para el buen funcionamiento del equipo.
- 4.10.3 Queda estrictamente prohibido enviar información de la Empresa a cuentas de correo públicas personales, así como enviar información de la Empresa por este tipo de cuentas de correo, cualquiera que sea su fin.

4.11 En materia de seguridad en el uso de internet

- 4.11.1 Por ningún motivo el Usuario debe consultar páginas que no sean relacionadas con sus actividades laborales o con los objetivos de la empresa.
- 4.11.2 Se prohíbe a todo empleado el acceso a Internet con perfil “abierto”, se deberá asignar un perfil con las limitantes de acceso acorde a su perfil de puesto y función. En caso de existir alguna excepción, ésta deberá de apegarse al “**Procedimiento para el ABC de Usuarios de SAP/AS400/Directorio Activo y Asignación de Roles PR-LS-09**”, para contar con la justificación y aprobación correspondientes.
- 4.11.3 La Gerencia de Administración de Redes en coordinación con la Gerencia de Seguridad y Gobierno de Sistemas, es responsable de la operación y validación de la funcionalidad de seguridad definida para el negocio.
- 4.11.4 La Dirección Corporativa de Sistemas es la responsable de la definición, estrategia y contratación de los servicios de seguridad en sistemas convenientes al negocio.

4.12 En materia de seguridad de la información relacionada con páginas corporativas y de servicios

- 4.12.1 Los contenidos de las páginas corporativas y/o de servicios (internas o públicas), así como los derechos de autor y de propiedad intelectual de las mismas pertenecen a Nadro, quien autoriza únicamente a sus empleados de Corporativo y Sucursales, el acceso a éstas. Por lo anterior, queda prohibido el uso indebido de las páginas y su contenido, incluyendo la modificación, publicación, transmisión, creación de trabajos derivados, incorporación a otras páginas web o reproducciones de éstas.
- 4.12.2 Los empleados de Corporativo y Sucursales de Nadro y sus empresas relacionadas, que cuenten por escrito con la autorización al uso de éstos medios, están regidos bajo las normas de confidencialidad de Nadro y a estas Condiciones de Uso.
- 4.12.3 Nadro se reserva el derecho, siempre que lo considere oportuno, a cambiar, adicionar o eliminar total o parcialmente tanto las Condiciones de Uso como las Normas de Confidencialidad.

Código	PO-LS-04
Versión	1
Vigente a partir de	SEPTIEMBRE 2016

POLÍTICA DE USO, CUSTODIA Y SEGURIDAD DE LA INFORMACIÓN

4.13 En materia de accesos de equipos de tecnología a Oficinas Generales y Sucursales

- 4.13.1 El uso de dispositivos móviles y/o teléfonos celulares está permitido, siempre y cuando su uso no infrinja la presente política (copia, almacenamiento y/o difusión de información fuera de la red corporativa de Nadro).
- 4.13.2 La Dirección Corporativa de Sistemas es la única área facultada para autorizar el acceso y uso permanente o temporal de equipos de cómputo personales (bajo una excepción autorizada por escrito y con vigencia implícita).
- 4.13.3 Los equipos de cómputo que la Empresa otorga como herramienta de trabajo a sus colaboradores, deben ser registrados invariablemente a su entrada o salida, así como el movimiento de paquetes de dispositivos de cómputo, de acuerdo a las **“Políticas de Accesos Seguridad y Vigilancia PO-DG-01”**.
- 4.13.4 Los controles de accesos a las instalaciones en general, así como al SITE y EDP, tanto para Corporativo como para Sucursal se encuentran definidos en las **“Políticas de Accesos Seguridad y Vigilancia PO-DG-01”**.

4.14 En materia de seguridad en la baja y movimientos de empleados

- 4.14.1 La Subdirección de Administración de Personal y Relaciones Laborales, debe comunicar oportunamente la baja o movimiento de personal a todas las áreas responsables. Ver **“Procedimiento para la Gestión de Equipos de Trabajo para Usuarios del Negocio PR-LS-16”**.

4.15 En materia de manejo de incidentes de seguridad

- 4.15.1 La Gerencia de Seguridad y Gobierno de Sistemas debe mantener contacto apropiado con autoridades, organizaciones oficiales, proveedores de servicios y telecomunicaciones, que permitan prever y en su caso, brindar apoyo en los eventos de incidentes a la Seguridad en los Sistemas de Información de la compañía.
- 4.15.2 El usuario debe reportar inmediatamente cualquier incidente de seguridad a la Mesa de Ayuda de Sistemas, considerando que un incidente es:
 - a) Fallas en los sistemas de información o aplicaciones.
 - b) Fallas o negación en los servicios de red.
 - c) Brechas o parches de seguridad.
- 4.15.3 La Gerencia de Seguridad y Gobierno de Sistemas debe reportar al Subdirector o Director de Sistemas los incidentes de seguridad, generando un reporte donde indique el impacto, riesgo y plan de mitigación.
- 4.15.4 La Dirección Corporativa de Sistemas debe informar y aclarar a la Presidencia y Dirección General el suceso reportado y detalle del nivel de criticidad del mismo, enfatizando el impacto a la continuidad del negocio y sus alternativas de solución.

Código	PO-LS-04
Versión	1
Vigente a partir de	SEPTIEMBRE 2016

POLÍTICA DE USO, CUSTODIA Y SEGURIDAD DE LA INFORMACIÓN

4.16 En materia de continuidad del negocio

- 4.16.1 Los Usuarios dueños de la Información deben proteger los procesos críticos del negocio de los efectos de fallas significativas o desastres, aplicando los mecanismos formales definidos por la Dirección Corporativa de Sistemas.
- 4.16.2 El área de Sistemas es la responsable de realizar respaldos de los sistemas de proceso crítico para la operación del negocio y validar la integridad del mismo ante un evento fortuito. Ver **“Procedimiento para la Ejecución de Respaldos y Restauraciones: Iseries, Sap/Aix, Bóveda de Facturación y Carpetas Privadas y Compartida PR-LS-13”**.
- 4.16.3 Todas las Direcciones Corporativas, deben de identificar los procesos críticos que garanticen la continuidad del negocio (General y en su Sucursal) para posteriormente, generar procedimientos que detallen las tareas y roles del personal para lograr éste fin.
- 4.16.4 El área de Mantenimiento en Corporativo debe garantizar la operación de las instalaciones (físicas y eléctricas), de acuerdo al **“Procedimiento para Proporcionar Mantenimiento a Maquinaria y Equipo, así como Realizar Obras Nuevas, Reparaciones y Remodelaciones en las Instalaciones PR-MC-35”**.

4.17 En materia de organización de seguridad de la información en la Dirección de Sistemas

- 4.17.1 La Dirección Corporativa de Sistemas debe:
- Proporcionar los recursos necesarios para que se puedan llevar a cabo todas las políticas de Seguridad de la Información en el área de Sistemas y a nivel Compañía, en las que ella influya o tenga participación.
 - Aprobar los roles y responsabilidades de cada uno de los puestos que conforman la Gerencia de Seguridad y Gobierno de Sistemas.
- 4.17.2 La Gerencia de Seguridad y Gobierno de Sistemas debe:
- Garantizar que los objetivos sean respetados y ejecutados a nivel de la organización.
 - Crear los planes de proyecto necesarios para llevar a cabo las políticas de Seguridad de la Información.
 - Revisar, proponer y presentar las políticas de Seguridad de la información para que sean aprobadas por parte de la Dirección de Sistemas.
 - Revisar la efectividad de la implementación de las políticas de seguridad.
 - Crear planes, programas de difusión y capacitación a la organización.
 - Gestionar los incidentes y excepciones encontradas.
 - Mantenerse actualizado y en caso de ser necesario, tener proveedores especializados con el tema.
 - Revisar y en su caso, actualizar y difundir al menos una vez al año la presente política con el personal de Sistemas y del Negocio.

Código	PO-LS-04
Versión	1
Vigente a partir de	SEPTIEMBRE 2016

POLÍTICA DE USO, CUSTODIA Y SEGURIDAD DE LA INFORMACIÓN

4.18 En materia de control de accesos remotos:

- 4.18.1 El Usuario que requiera accesos remotos, debe documentar la petición en donde especifique las aplicaciones y/o plataformas que requiere acceder, así como su vigencia.
- 4.18.2 La Gerencia de Seguridad y Gobierno de Sistemas validará el nivel de riesgo para cada caso, para dar su aprobación correspondiente, así mismo deberá revisar cada mes la lista de personas que tienen accesos remotos.
- 4.18.3 La petición deberá de contar con las aprobaciones correspondientes, con base en el procedimiento vigente.

4.19 En materia de seguridad perimetral e interna

- 4.19.1 La Gerencia de Redes debe garantizar la actualización de todos los dispositivos de control de acceso perimetral, así como del resguardo y análisis de las bitácoras o logs de los equipos activos, los cuales deberán ser resguardados por un año por cuestiones de auditoría interna o externa.
- 4.19.2 Se deberá garantizar el proceso de respaldo y restauración de los equipos de seguridad perimetral e interna.

4.20 En materia de destrucción de información (física/ lógica)

- 4.20.1 Antes de borrar o destruir los dispositivos definitivamente, se debe tener el visto bueno de Comité de Seguridad.
- 4.20.2 La información de los dispositivos de almacenamiento debe ser borrada antes de su destrucción física, así como eliminar todas las licencias de software.
- 4.20.3 Todos los dispositivos que almacenan información deben ser destruidos físicamente por un proveedor certificado en destrucción de la información.
- 4.20.4 El proveedor debe entregar la documentación (manifiestos), videos o cualquier otra evidencia que asegura la destrucción de los dispositivos de almacenamiento.

4.21 En materia de requerimientos para la continuidad del Centro de Datos

a) Cableado estructurado

- 4.21.1 Todos los edificios, oficinas, almacenes pertenecientes a la organización deberán de contar con un certificado de cableado estructurado con el detalle del mapa de conexiones para cada posición y/o servicio.

Código	PO-LS-04
Versión	1
Vigente a partir de	SEPTIEMBRE 2016

POLÍTICA DE USO, CUSTODIA Y SEGURIDAD DE LA INFORMACIÓN

b) Monitoreo de Instalaciones

4.21.2 Toda afectación que se realice en el Centro de Datos a nivel arquitectura, eléctrico, telecomunicaciones y energía debe ser documentada y autorizada por la Dirección Corporativa de Sistemas

4.21.3 Se debe contar con un directorio actualizado de proveedores y de personal del Centro de Datos.

5. Registros

Código	Nombre del Formato	Medio de Resguardo (electrónico o papel)	Tiempo de Resguardo	Disposición Final (destrucción o se mantiene actualizado)
N/A	N/A	N/A	N/A	N/A

6. Anexos

Código	Título	Páginas
N/A	N/A	N/A

7. Referencias

Código	Nombre del Documento
PR-LS-20	Procedimiento para la Gestión de Cambios en Sistemas
PR-LS-16	Procedimiento para la Gestión de Equipos de Trabajo para Usuarios del Negocio
PO-LS-02	Política para el Control de Licencias y Software
PR-AC-35	Procedimiento para la Adquisición de Bienes y Servicios
PR-LS-13	Procedimiento para la Ejecución de Respaldos y Restauraciones Iseries, SAP/AIX, Boveda de Facturación y Carpetas Privadas y Compartidas
PR-LS-20	Procedimiento para la Atención de Incidentes y Requerimientos a Sistemas (Modelo de Soporte)
PR-LS-09	Procedimiento para el ABC de Usuarios de SAP/AS400/Directorio Activo y Asignación de Roles
PO-DG-01	Políticas de Accesos Seguridad y Vigilancia
PR-MC-35	Procedimiento para Proporcionar Mantenimiento a Maquinaria y Equipo, así como Realizar Obras Nuevas, Reparaciones y Remodelaciones en las Instalaciones



Código	PO-LS-04
Versión	1
Vigente a partir de	SEPTIEMBRE 2016

POLÍTICA DE USO, CUSTODIA Y SEGURIDAD DE LA INFORMACIÓN

8. Bibliografía

N/A

