POLÍTICAS DE TECNOLOGÍAS DE LA INFORMACIÓN Y SEGURIDAD INFORMÁTICA DE SNR INFRAESTRUCTURA, MANTENIMIENTO Y SERVICIOS

Sección de Control de Cambios.

Ubicación/sección	Redacción anterior	Modificación propuesta	Comentario/ Justificación

Contenido

TÍTULO 1

Objetivo

El presente documento tiene como propósito establecer las políticas en materia de seguridad informativa de SNR Infraestructura, Mantenimiento y Servicios S. de R.L. de C.V. (SNR), mismas que deberán cumplirse con la finalidad de preservar la confidencialidad, integridad y disponibilidad de la información.

TÍTULO 2

Alcance

Las políticas contenidas en este documento aplican para todo el personal que labore o preste servicios en SNR, así como para cualquier persona que, por su relación con SNR, utilice sus tecnologías de la información y comunicaciones.

Los lineamientos, procedimientos y guías que, en su caso, se lleguen a desarrollar a partir de estas políticas deben de aplicarse en todas las fases del ciclo de la información, siendo las siguientes: generación, distribución, almacenamiento, procesamiento, trasporte, acceso, consulta y destrucción para todos los sistemas, infraestructuras tecnológicas y las instalaciones (medios de almacenamiento que los soportan).

TÍTULO 3

Definiciones

Término	Definiciones
Activo de información.	Toda aquella información y medio físico o electrónico que la contiene, que por su importancia y el valor que representa para SNR debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue. Los activos de información son necesarios para que SNR funcione correctamente y alcance los objetivos propuestos.
Amenaza.	Cualquier evento, actividad humana, fenómeno natural o evento tecnológico que tiene el potencial de causar algún tipo de daño o menoscabo a los activos de información de SNR, ocasionando daños materiales o perdidas inmateriales en los activos.
Análisis de riesgos.	Es el proceso general de identificación, análisis y evaluación de riesgos para identificar las fuentes de vulnerabilidades o amenazas a los activos de TIC, a la infraestructura esencial o a los activos de información.
Aplicación o Aplicativo.	Programa dedicado para una tarea especifica.
Áreas seguras.	Son los espacios físicos en los que se maneja información sensible o valiosa, así como equipos informativos y el personal necesario para conseguir los objetivos de negocio.
Ataque.	Evento, exitoso o no, que atenta contra el buen funcionamiento de un sistema o sistemas.
Borrado seguro.	Proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital.
Centro de datos.	El lugar físico en el que se ubiquen los activos de TIC y desde donde se proveen servicios de TI.
Código fuente.	El conjunto de líneas de texto, que son las directrices que debe seguir la computadora para realizar un programa; por lo que es en el código fuente donde se encuentra escrito el funcionamiento de la computadora.
Confidencialidad.	La característica o propiedad de la información, de poder ser conocida únicamente por individuos autorizados.
Disponibilidad.	La característica de la información de permanecer accesible para su uso cuando así lo requieran individuos o procesos autorizados.

Dispositivo móvil.	Es un activo de información de computación portátil, que se utiliza para el procesamiento de información de SNR, con la finalidad de ejecutar una función específica para el negocio.
Firewall.	Es un software o sistema de seguridad de la red basada en hardware que controla el tráfico de red entrante y saliente en base a un conjunto de reglas aplicadas. Un Firewall establece una barrera entre una red interna segura y de confianza a otra red (ej. Internet) que se supone que no es seguro y confiable.
Impacto.	Consecuencia debidamente medida o cuantificada al materializarse una amenaza.
Información sensible.	Aquella información propiedad o en posesión de SNR, cuyo conocimiento por terceros no autorizados puede causar Daño, por lo que debe ser clasificada y protegida. Comprende formatos electrónicos como archivos, documentos, correos, medios de almacenamiento y sistemas de información, tal es el caso de bases de datos; así como formatos físicos, entre otros: archivos, documentos, planos y expedientes
Incidente.	Es la afectación o interrupción a los activos, a las infraestructuras críticas, así como a los activos de información de una Empresa, incluido el acceso no autorizado o no programado a estos.
Integridad.	La acción de mantener la exactitud y corrección de la información.
Infraestructura tecnológica.	Se refiere a todos los elementos físicos o lógicos que son requeridos para brindar los servicios y soluciones informáticas, tales como: centro de cómputo y comunicaciones, equipos y redes de comunicación de voz y datos, servidores de cómputo principales, servidores de cómputo departamentales, y de oficina (de escritorio y portátil), equipos auxíliales de cómputo y comunicaciones, sistemas operativos, manejadores de bases de datos, productos computacionales (Paquetes de Software) adquiridas o generadas por SNR.
Mandos Superiores.	Se refiere al Director General y a los Gerentes de SNR, quienes tienen la responsabilidad de supervisar las actividades del personal a su cargo.
Plataforma tecnológica.	Son las acciones necesarias para realizar o brindar los servicios informáticos, tales como mantenimiento, optimización, adecuación, monitoreo, vigilancia de los componentes tecnológicos involucrados en la operación de la plataforma tecnológica.
Proceso.	Actividades estructuradas y organizadas alrededor de un conjunto de objetivos definidos en términos medibles y que se expresan como beneficios para SNR.
Programa.	Es el conjunto de iniciativas, proyectos y acciones planeadas y programadas para lograr un objetivo, ejecutándose dentro de un periodo determinado y sujetas a un presupuesto.
Proveedor.	Persona o empresa seleccionada por SNR para la prestación de un servicio o la entrega de un bien.

Privilegio especial.	Es el usuario facultado para realizar actividades de mantenimiento y/o soporte operativo y/o funcional a un aplicativo o base de datos.
Responsable Funcional.	Es la persona encargada de supervisar, identificar y gestionar mejoras en los aplicativos o sistemas, así como su correcto funcionamiento de uno o más aplicativos que le sean asignados por la Dirección en la que se encuentre adscrito.
Repositorio.	El espacio en medio magnético u óptico en el que se almacena y mantiene la información digital.
Requerimiento.	Condición o capacidad definida a una necesidad por un usuario, para solucionar un problema o lograr un objetivo, y existen diversos tipos como: funcionales, de rendimiento esperado, de Interfaces con otros sistemas, de definición de restricciones, del cliente, etc.
Riesgo.	La posibilidad de que una amenaza pueda explotar una vulnerabilidad y causar una pérdida o daño sobre los activos de TI, las infraestructuras críticas o los activos de información de SNR.
Roles.	Conjunto de responsabilidades, actividades y autorizaciones que se otorga a una persona o equipo. Una persona o equipo pueden tener varios roles.
Seguridad de la información.	La capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.
Sistemas o Aplicativos Institucionales.	Conjunto de elementos informáticos e infraestructura tecnológicas interrelacionados que interactúan entre sí para lograr un objetivo de negocio.
SNR.	SNR Infraestructura, Mantenimiento y Servicios S. de R.L. de C.V.
TI.	Tecnologías de la Información.
TIC.	Tecnologías de la Información y las Comunicaciones.
User-id.	Conjunto de caracteres que sirve para identificar a un usuario, para su acceso a algún sistema.
Vulnerabilidad.	Son las debilidades en la seguridad de la información que influyen negativamente en un activo dentro de una organización que potencialmente permite que una amenaza se materialice y afecte a los recursos de TI, a la infraestructura critica, así como a toda la información.

TÍTULO 4

Seguridad de la Información.

La Dirección General de SNR, a través del Responsable de Seguridad de la Información, proveerá los mecanismos de identificación, autorización y protección suficientes para garantizar una operación segura, tanto en las plataformas y aplicativos de SNR como en las interfaces entre los distintos aplicativos que participan en los procesos, asegurando que se generen reportes confiables de información, que permitan, entre otras tareas, una conciliación automática y eviten tanto entradas múltiples como la manipulación de datos.

La Dirección General de SNR designa como Responsable de Seguridad de la Información al Gerente de Gobierno Corporativo, quien debe coordinar la revisión anual del cumplimiento de los objetivos y las métricas de seguridad de la información así como, debe verificar que se definan e implementen los controles que se deriven de estas políticas.

4.1 Organización para la Seguridad de la Información (Roles y Responsabilidades).
En cumplimiento a la normativa externa e interna aplicable, la administración de la seguridad de la información institucional SNR corre a cargo de las siguientes personas:

- El Director General de SNR es quien tiene la responsabilidad de promover la seguridad de la información Institucional.
- El Gerente de Gobierno Corporativo es responsable del cumplimiento de las normativas aplicables a la seguridad de la Información de SNR.
- La Gerencia de Gobierno Corporativo es responsable de asegurar la alineación operativa de TI a la normativa aplicable en materia de seguridad de la Información.
- La Gerencia de Cumplimiento Normativo deberá asegurarse de que los contratos de prestación de servicios que celebre la Gerencia de Gobierno Corporativo, cuenten con cláusulas que promuevan el cumplimiento de esta política.
- Los Mandos Superiores de las áreas dueñas de los procesos sustantivos y de apoyo son responsables de la observancia y cumplimiento de estas Políticas en Materia de Seguridad Informática
- Todos los colaboradores en general que presten sus servicios a SNR, son responsables de conocer y cumplir las presentes políticas.

4.2 Segregación de funciones.

Los Gerentes de SNR tienen a su cargo los procesos sustantivos y de apoyo, quienes deben definir las funciones para que se preserve una adecuada segregación de actividades, por tipo de producto, operación, monto, nivel jerárquico, área, unidad de negocio o administrativa y comités.

Esta segregación debe evitar conflictos de interés que minimicen al máximo el riesgo de ser juez y parte en tareas de ejecución, validación y autorización.

4.3 Contacto con autoridades.

En caso de ocurrir algún incidente de seguridad que involucre algún contacto con cualquier autoridad administrativa o judicial en materia de seguridad de la información, será la Gerencia de Gobierno Corporativo quien mantendrá la comunicación y coordinación con las autoridades correspondientes, siempre con el apoyo y asesoría de la Gerencia de Cumplimiento Normativo.

4.4 Contacto con grupos de interés especial.

El Gerente de Gobierno Corporativo coordinará el proceso de comunicación con grupos de interés especial, previo análisis de la necesidad de contacto con estos grupos, entre los que se incluyen, de manera enunciativa más no limitativa:

1. Consultorías,
2. Asociaciones,
3. Publicaciones especializadas, y
4. Equipo de respuesta ante emergencias informáticas.

4.5 Seguridad de la información en la gestión de proyectos.

El Gerente de Gobierno Corporativo debe implementar los estándares funcionales, operativos y tecnológicos, que deben incorporarse en el desarrollo de proyectos, adquisición de servicios y componentes de tecnologías de información y comunicación para SNR, atendiendo a las necesidades específicas. El Gerente de Gobierno Corporativo debe validar el cumplimiento de los estándares funcionales, operativos y tecnológicos mínimos indicados en estas políticas.

4.6. Dispositivos Móviles.

Es responsabilidad del personal usuario de los equipos informáticos proteger los bienes que les han sido asignados para el desempeño de sus funciones, siguiendo las recomendaciones del fabricante y medidas de seguridad, así como las que a continuación se describen, como mínimo:

1. No exponer el equipo a condiciones de inseguridad física y/o ambiental.
2. Proteger las claves de acceso que les han sido asignadas.
3. No dejar el equipo desatendido en lugares públicos o en lugares donde pueda ser sustraído o dañado con relativa facilidad, como autos, maletas de viaje, cerca de ventanas, en el piso, mesas de comida o bebida, etc.

La Dirección General de SNR y la Gerencia de Gobierno Corporativo deben asegurar que todos los equipos móviles que SNR haya asignado al personal para el cumplimiento de sus funciones cuenten con las herramientas necesarias para garantizar la seguridad de la información. Estas herramientas, incluyen, en forma enunciativa, más no limitativa: antivirus, software, licenciamiento, aplicaciones seguras, entre otras.

Los equipos móviles de uso personal no otorgados por SNR que requieran acceso a los servicios de SNR, deben contar con la validación de la Gerencia de Gobierno Corporativo, para asegurar de que éstos cuentan con los elementos tecnológicos de seguridad informática requeridos.

TÍTULO 5

Capacitación de la Seguridad Informática Nuevos Talentos.

5.1 Previo al Empleo.

Es responsabilidad de la Gerencia de Gobierno Corporativo a través de la instancia que realice la contratación laboral correspondiente, informar a todo el personal de nuevo ingreso acerca de la existencia de estas Políticas en Materia de Seguridad Informática, así como las cláusulas de confidencialidad de datos vigentes.

5.2 Durante el Empleo.

Es responsabilidad de las Gerencias, promover ante el personal a su cargo la existencia de las Políticas en Materia de Seguridad Informática y del buen uso y protección de los activos de información de SNR.

5.3 Concientización, educación y formación en seguridad de la información.

Corresponde a las Gerencias promover en todo momento la participación en los procesos de concientización, capacitación y prevención a incidentes de seguridad, así como cualquier otra actividad que haya sido aprobada por SNR, para fortalecer una cultura de seguridad de la información. La Gerencia de Gobierno Corporativo debe establecer programas orientados a fortalecer y afianzar una cultura de seguridad de la información en el personal de SNR. Asimismo, debe coordinar los programas o campañas de sensibilización en temas relativos a la seguridad de la información y debe mantener evidencia de estos.

5.4 Terminación o Separación del Puesto.

Toda terminación laboral (renuncia, liquidación, jubilación, etcétera) debe apegarse a los procesos que realice la instancia encargada de la contratación, será la Gerencia de Gobierno Corporativo, quien se asegure que la separación del puesto se lleve a cabo de una manera ordenada, disminuyendo así el riesgo hacia los activos de información que son propiedad de SNR.

La terminación o separación de funciones, debe dejar evidencia de la inhabilitación y de los accesos a aplicaciones de SNR.

Son las Gerencias de SNR las responsables de comunicar de forma inmediata y oportuna a la instancia correspondiente la finalización del nombramiento o cambio de puesto o funciones de los empleados, prestadores de servicios o terceros.

TÍTULO 6

Gestión de Activos

6.1 Inventario de activos.

Un activo de información, es entendido como aquella información y el medio físico o electrónico que la contiene, que por su importancia y el valor que representa para SNR debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, y que en la práctica es un elemento reconocible que almacena datos, registros, información en cualquier medio, con las características siguientes:

1. Es valioso para SNR por la información que contiene.
2. No es de fácil reemplazo y en algunos casos pudiera ser irrepetible.

Es responsabilidad de los Mandos Superiores de SNR identificar sus activos de información.

La Gerencia de Gobierno Corporativo debe mantener un registro actualizado sobre los activos informáticos que soporten los servicios TI de SNR.

6.2 Propiedad de los activos.

Toda información que se genere a partir de un Dispositivo móvil ya sea propio, arrendado o contratado por un servicio, es propiedad de SNR y quien la resguarda, se convierte en responsable de esta.

Todo activo de información debe ser asignado a un responsable y autorizado por su jefe inmediato (nivel mínimo Gerente).

La persona responsable del activo debe:

1. Salvaguardar la integridad, disponibilidad y confidencialidad del activo.
2. Hacer uso del activo únicamente para los propósitos y actividades de la Institución.
3. Reportar cualquier incidente o problema relacionado con el activo de información.
4. Cualquier omisión (con dolo o involuntariamente) al reportar algún incidente relacionado con cualquier activo bajo su guarda y custodia, se considerará una falta hacia la seguridad de la información que, en su caso, deberá de ser informado a las autoridades competentes.

5. Realizar las acciones necesarias para mantener el activo de información en buenas condiciones que garanticen y cumplan su función.

Todos los aplicativos y sistemas de SNR que soporten los procesos sustantivos deben tener un responsable funcional del área de la empresa y ser integrados por la Gerencia de Gobierno Corporativo a su catálogo de servicios.

6.3 Uso aceptable de los activos.

SNR considera que los recursos para el procesamiento de la información son prioritarios para el desarrollo de los procesos de negocio y el adecuado cumplimiento de sus funciones; por lo que es responsabilidad del personal salvaguardarlos de cualquier alteración o modificación no autorizada, daño o destrucción que límite su disponibilidad para el adecuado desarrollo de sus actividades.

El uso aceptable de los activos de información incluye:

1. Evitar daños temporales o permanentes a los activos de información, causados por accidentes, imprudencias o daños dolosos.
2. Reportar cualquier falla o mal funcionamiento detectado.
3. Informar a los jefes inmediatos, cualquier falla o vulnerabilidad de los activos de información.
4. Notificar de cualquier necesidad de protección o mejora, en los controles de los activos de información.
5. Usar los activos de información únicamente para los propósitos de SNR.
6. Reportar cualquier uso no adecuado del activo de información a su jefe inmediato.

6.4 Devolución de activos.

Todo personal que preste sus servicios a SNR, al concluir sus funciones, tiene la obligación de entregar los activos informáticos asignados en buen estado físico y de operación, así como los activos de información y la documentación correspondiente.

TÍTULO 7

Clasificación de la Información.

7.1 Directrices de clasificación.

Cada área debe clasificar y etiquetar su información, esta debe clasificarse como:

1. **Restringida**: (nivel de protección **Alto**).

   Contratos, convenios, acuerdos, alianzas estratégicas, compromisos arbitrales, substanciación de procedimientos, actas y acuerdos de los consejos de administración, sentencias, laudos, convenios judiciales, demandas, contestaciones personales, información confidencial, salud y expedientes médicos de los trabajadores, salarios, prestaciones y nómina, procesos de contratación de adquisiciones, arrendamientos y servicios, proyectos, desarrollo de servicios, comercio internacional, estudios de mercado, planeación, secretos industriales, secretos comerciales, propiedad intelectual, estados financieros, cuentas bancarias, inversiones, valores, documentación fiscal, así como toda información relacionada con seguridad nacional, seguridad pública, seguridad energética.

2. **Controlada**: (nivel de protección **Medio**).

   Pagos, facturación, carpetas, informes, compras por montos menores, así como la información que ha perdido carácter de restringida pero que debe continuar bajo control de los propietarios de la información.

Los listados anteriores son enunciativos mas no limitativos, por lo que los propietarios y encargados de la información pueden incorporar otros documentos en las categorías restringida y controlada.

7.2 Etiquetado de la información.

La información clasificada como restringida o controlada, debe ser confirmada por el responsable de la información.

El etiquetado de la información se aplica sólo para la información restringida.

7.3 Protección y manejo de la información

1. La Gerencia de Gobierno Corporativo debe proveer mecanismos de protección de la información, de acuerdo con su clasificación.
2. Todo activo de información protegido debe contar con un control de acceso formal, donde establezca qué personas son autorizadas para el manejo de la información.
3. La información debe respaldarse en un nivel de protección consistente con su clasificación.
4. Todo el personal de SNR está obligado a no revelar a terceras personas la información que conozcan por el ejercicio de sus funciones, por lo que están obligados a mantenerla confidencial y privada para evitar su divulgación.
5. Los usuarios de acuerdo con sus funciones podrán trabajar y hacer uso de la información de SNR en los activos de información asignados y resguardar la versión final.

TÍTULO 8

Manejo de los Medios de Almacenamiento

8.1 Gestión de medios extraíbles

La Gerencia de Gobierno Corporativo debe proporcionar los servicios y medios necesarios para asegurar el manejo de la información dentro de SNR.

La Gerencia de Gobierno Corporativo debe concientizar sobre el buen uso y mejores prácticas del manejo de medios removibles de almacenamiento, para el traslado de la información fuera de SNR.

8.2 Eliminación de medios.

La Gerencia de Gobierno Corporativo debe asegurarse de la baja y el borrado confiable de los activos informáticos.

Todo activo informático que contenga información de SNR, debe contar con procedimientos de migración, respaldo y borrado seguro antes de que el activo sea eliminado.

TÍTULO 9

Control de Accesos

9.1 Requisitos de Negocio para el Control de Acceso.

La Gerencia de Gobierno Corporativo debe establecer controles de seguridad para la Gestión de Cuentas de Usuarios en SNR.

9.2 Control de acceso a las redes y servicios asociados.

1. Los controles de acceso a los servicios de información deben asignarse con base en los roles y perfiles de los usuarios, según el nivel de servicio requerido.

2. La autentificación de usuarios debe hacerse a través de contraseñas seguras y alta complejidad de las mismas.

9.3 Gestión de Accesos a Usuarios.

Todos los aplicativos y servicios de SNR deben tener un registro de altas, bajas y cambios.

9.4 Gestión de los derechos de acceso asignados a usuarios.

Todos los accesos a servicios de SNR deben ser solicitados por el Gerente del área que corresponda haciendo la petición de acuerdo con su función, mediante roles y perfiles, asegurando una correcta operatividad.

9.5 Gestión de derechos de acceso con privilegios especiales.

Las solicitudes de usuarios con privilegios o permisos especiales de acceso deben contar con la autorización del gerente de área o propietario del sistema informático. Las cuentas de

usuarios con privilegios especiales de acceso deben ser diferentes a las cuentas que utilizan para la operación regular.

9.6 Gestión de información confidencial de autenticación de usuarios.
La Gerencia de Gobierno Corporativo debe garantizar la confidencialidad de la entrega de contraseñas en todos sus procesos.

9.7 Revisión de los derechos de acceso de usuarios.
Los derechos de acceso de los usuarios deben ser revisados anualmente por la Gerencia de Gobierno Corporativo y validados por las Gerencias correspondientes.

9.8 Baja o modificación en cuentas y roles de acceso.
Es responsabilidad de los Mandos Superiores de las áreas que cuenten con personal externo y/o proveedores que deban interactuar con sus procesos informáticos, solicitar el acceso a los servicios y aplicativos de SNR, así como notificar las bajas o cambios de funciones del personal a la Gerencia de Gobierno Corporativo, para la ejecución del cambio o remoción de los derechos de acceso.

TÍTULO 10

Responsabilidades del Usuario

10.1 Uso de información confidencial para la autenticación.
Cada uno de los miembros del personal de SNR es individualmente responsable de las contraseñas asignadas para los equipos informáticos a su cargo, las cuales son confidenciales e intransferibles y deben mantenerse secretas.

El usuario debe cambiar la contraseña inicial después de que le fue asignada al sistema o aplicativo, mismo que debe estar configurado para que esto sea de forma automática.

Solo deben tener acceso a los aplicativos de SNR los usuarios autorizados con la cuenta asignada para tal efecto; en ningún caso deben acceder usando una cuenta diferente a la proporcionada.

10.2 Control de Acceso a Sistemas y Aplicaciones.

La Gerencia de Gobierno Corporativo debe garantizar que las aplicaciones cuenten con un control de acceso centralizado, donde el usuario debe ser identificado con un User-Id y una contraseña segura.

La administración de los permisos de acceso a los aplicativos de SNR se realiza mediante roles y perfiles.

Todos los usuarios con acceso a los aplicativos de SNR deben identificarse en forma única y contar con los permisos de acceso asignados previamente, de acuerdo a su rol y perfil.

10.3 Procedimientos seguros de inicio de sesión.

Todo aplicativo de SNR debe contar con las configuraciones necesarias para limitar el tiempo de la sesión activa.

10.4 Gestión de contraseñas de usuario.

Los sistemas o aplicativos de SNR deben contar con un control de contraseñas seguro y un mecanismo de historial, para garantizar la no reutilización de estas.

10.5 Uso de herramientas de administración de sistemas.

La Gerencia de Gobierno Corporativo debe restringir y controlar estrictamente el uso de herramientas que puedan estar en capacidad de anular los controles del mismo sistema; en caso de existir se debe contar con un registro documental del personal que tiene acceso.

10.6 Control de acceso al código fuente de los programas.

La Gerencia de Gobierno Corporativo debe contar con un procedimiento de solicitud de acceso a código fuente de los sistemas o aplicativos de SNR.

TÍTULO 11

Seguridad Física y Centros de Datos.

11.1 Áreas Seguras.

Se deberán implementar los mecanismos necesarios que permitan limitar el acceso a las áreas seguras para albergar equipos de cómputo y solamente para el personal autorizado.

No se permitirá el acceso a las áreas seguras para albergar equipos de cómputo al personal que no esté expresamente autorizado.

11.2 Seguridad de oficinas, despachos y recursos.

La Gerencia de Gobierno Corporativo debe proporcionar a cada empleado un espacio físico asignado que cuente con mobiliario protegido para el resguardo de información física.

La Gerencia de Gobierno Corporativo debe proporcionar a cada empleado un acceso controlado para el uso de las instalaciones de acuerdo con sus funciones dentro de SNR.

11.3 Protección contra amenazas externas y ambientales.

La Gerencia de Gobierno Corporativo debe facilitar los recursos necesarios para establecer perímetros de seguridad física con el fin de proteger áreas que contengan información crítica de SNR, así como el área de procesamiento de datos.

11.4 Trabajo en áreas seguras.

Las áreas de acceso a las instalaciones de SNR deben ser controladas y debe restringirse el acceso a las áreas seguras para evitar el acceso no autorizado.

11.5 Seguridad de los Equipos.

Todo equipo que almacene procese o transmita información esencial para la operación de SNR, debe ser protegido para disminuir el riesgo de amenazas ambientales o físicas; tales como, inundaciones, rayos, sismos, radiaciones, polvo, humedad, vandalismo, explosión, humo etc.

SNR debe contar con un centro de datos que garantice la protección de los equipos que soportan los procesos de SNR, así como los equipos de respaldo.

Todos los equipos de respaldo o asignados que se encuentran fuera de los centros de datos deben estar ubicados y protegidos de acuerdo con las especificaciones del fabricante.

11.6 Mantenimiento de los equipos.
Todo activo de información debe contar con programas de soporte y mantenimiento, para asegurar su correcto funcionamiento y garantizar su disponibilidad.

11.7 Salida de activos.
La Gerencia de Gobierno Corporativo debe establecer el Procedimiento Entrada y Salida de Equipo de Cómputo de las instalaciones de SNR, en coordinación con las instancias competentes.

11.8 Seguridad de los equipos y activos fuera de las instalaciones.
Todo equipo que almacene, procese o transmita información restringida debe operar dentro de las instalaciones de SNR o de las contratadas para tal efecto.

Los equipos de cómputo móviles y laptops de SNR deben ser protegidos conforme lo establece la sección Responsabilidad por los activos y con las medidas de seguridad que establezca el fabricante para su buen funcionamiento.

Los equipos de cómputo de SNR que se encuentran fuera de las instalaciones y requieran conectarse a la red interna de SNR solamente podrán realizarlo por medio del cliente de VPN.

11.9 Reutilización o baja de dispositivos de almacenamiento.
La Gerencia de Gobierno Corporativo debe implementar el Proceso de Baja y Devolución de Equipos de Cómputo que garantice el borrado seguro de los activos de información.

11.10 Bloqueo de equipo por inactividad.

La Gerencia de Gobierno Corporativo debe implementar en todo equipo informático las configuraciones necesarias para su bloqueo de forma automática, una vez que éste se encuentre sin actividad.

TÍTULO 12

Políticas de Seguridad en las Operaciones.

12.1 Responsabilidades y Procedimientos de Operación.

Los procedimientos de operación y los procesos de todas las áreas de SNR deben documentarse en los manuales de operación que al efecto se emitan.

La Gerencia de Gobierno Corporativo es responsable de documentar sus procedimientos y de contar con memorias técnicas para las aplicaciones y sistemas de información, mismos que deben estar actualizados y vigentes.

12.2 Protección Contra Código Malicioso.

La Gerencia de Gobierno Corporativo debe asegurar que todos los equipos de escritorio, móviles, laptops y servidores utilizados en la red de SNR tengan instalado el software antivirus, anti-malware, anti-xploits, anti-spam y anti-spyware licenciado y mantenerlo actualizado, tanto en versión como en definición de firmas. Así mismo, deben cumplir con una configuración base de parches de seguridad.

Los proveedores o personal externo que tengan equipos y que necesiten conectarse a la red de SNR, deben contar con un software de antivirus autorizado previamente por la Dirección General a través de la Gerencia de Gobierno Corporativo.

El software de antivirus anti-malware, anti-xploits, anti-spam y anti-spyware de SNR debe permitir como mínimo:

1. Ejecutar búsqueda automática, manual o programable.
2. Limpiar archivos infectados.
3. Mantener en cuarentena los archivos que no puedan ser limpiados.

4. Contar con mecanismos para prevenir y contener amenazas, así como, negación de servicios.
5. Proveer la capacidad de actualizaciones automáticas y programables.
6. Registrar los incidentes de virus y contar con la capacidad de análisis de registro.
7. Detectar código malicioso.
8. Generar alertas.
9. Llevar una administración centralizada.

El software contra código malicioso y sus componentes deben ser actualizados cuando exista una nueva versión o definición de firmas, con base a los contratos con el fabricante.

12.3 Respaldo y Borrado de Información.

Todos los Mandos Superiores de las áreas dentro de SNR son responsables de identificar la información que sea sensible para la operación de su área de acuerdo con su criticidad y deben avisar a la Gerencia de Gobierno Corporativo para gestionar su respaldo y periodicidad.

La información que se genere derivada de la operación debe encontrarse documentada y resguardada para su consulta durante el tiempo que establezcan las disposiciones jurídicas aplicables.

12.4 Restauración e integridad.

La Gerencia de Gobierno Corporativo debe establecer y actualizar los planes y procedimientos de recuperación de acuerdo con los requerimientos del negocio, garantizar que los respaldos no sean alterados, así como la integridad, disponibilidad y confidencialidad de los respaldos por lo menos cinco años, desde su último respaldo.

12.5 Almacenamiento de información.

La Gerencia de Gobierno Corporativo debe proporcionar y administrar espacio de almacenamiento suficiente para que las áreas puedan resguardar copia de su información.

Queda prohibido la utilización de recursos de almacenamiento de SNR para archivos de uso personal o de diversión.

Se debe contar con procedimientos de borrado o destrucción segura de la información de SNR, que ya no sea necesaria, ni por la operación, ni por requerimientos legales.

Toda la información que ya no sea utilizada se debe eliminar de forma segura.

12.6 Registro de Actividad.

Todos los sistemas y aplicaciones críticos de SNR, bases de datos, dispositivos de red y servidores, deben contar con registros de eventos y bitácoras de seguridad protegidos debidamente.

12.7 Control de Software en Sistemas Operacionales.

La Gerencia de Gobierno Corporativo debe asegurarse que todo el software que se instale en los servidores y equipos de cómputo personal cuente con el licenciamiento vigente, suficiente para atender los requerimientos del negocio, siendo responsable de administrar y resguardar las licencias del software institucional.

La Gerencia de Gobierno Corporativo es la única instancia autorizada para instalar, actualizar y desinstalar el software de los equipos de cómputo

12.7 Gestión de la Vulnerabilidad Técnica.

SNR a través de la Gerencia de Gobierno Corporativo deben establecer el alcance de las evaluaciones que se realicen para identificar vulnerabilidades en el hardware, software, sistemas, aplicaciones, seguridad, recuperación de información y redes.

12.8 Las restricciones a la instalación de software.

Queda prohibido al personal no autorizado instalar y/o ejecutar software para explorar (escanear) redes, equipos de cómputo y sistemas de información, en busca de protocolos, puertos, recursos compartidos y vulnerabilidades; así como el descubrimiento y monitoreo no autorizado del tráfico de la red de SNR. La Gerencia de Gobierno Corporativo debe implementar mecanismos para restringir la instalación de software no autorizado.

TÍTULO 13

Seguridad de las Comunicaciones

13.1 Gestión de la Seguridad de Red.

La Gerencia de Gobierno Corporativo será responsable de solicitar el diseño, implementación, establecimiento, contratación, administración, mantenimiento y soporte de las redes de voz y datos y de toda la infraestructura de comunicaciones que las soportan al proveedor encargado de este servicio.

La Gerencia de Gobierno Corporativo debe solicitar lo relacionado a la implementación, procedimientos y controles de seguridad que garanticen la integridad, disponibilidad y confidencialidad de la información, en su transmisión en las redes e infraestructuras de comunicaciones de SNR al proveedor de este servicio.

La Gerencia de Gobierno Corporativo debe establecer junto con el proveedor de servicios de red los requerimientos técnicos para la conexión a la red y los servicios necesarios para la protección de la información y sus activos tecnológicos, así como, para el monitoreo y detección oportuna de incidentes de seguridad.

La Gerencia de Gobierno Corporativo y el proveedor de los servicios de red deben elaborar mecanismos para el uso del servicio de internet en SNR, el cual debe contar con herramientas de seguridad y de filtrado de contenido, búsquedas e imágenes en internet, que permitan la segmentación del mismo en distintas categorías, reportes y soporte de sitios de nueva generación y/o micro-aplicaciones.

La Gerencia de Gobierno Corporativo debe proteger la información que de estos servicios que se deriven, mediante la correcta configuración de los servidores y/o dispositivos sobre los que operan estos servicios.

13.2 Seguridad de los servicios de red.

La Gerencia de Gobierno Corporativo y el proveedor de servicios de red deben implementar:

- Mecanismos que midan y aseguren niveles de disponibilidad y tiempos de respuesta, que garanticen la adecuada ejecución de las operaciones y servicios bancarios que se realizan.

- Medidas de control que garanticen la protección, seguridad y confidencialidad de la información, generada por la realización de operaciones bancarias, a través de cualquier medio tecnológico.

Se pueden establecer redes abiertas, únicamente al proporcionar servicios a la población, las cuales deben estar separadas y aisladas de la red de datos.

13.3 Trasferencia de la Información.

Los recursos de red de SNR no deben ser utilizados para propósitos personales, específicamente:

1. No está permitido descargar o intercambiar documentos con información institucional, música, video e imágenes de internet en cualquier medio y desde cualquier medio y sólo se autorizará en caso de que la Institución o actividad específica lo justifique.
2. Dentro de la red de SNR, no está permitido conectar a internet equipos personales o servidores de red por otro medio que no sea el oficialmente autorizado por la Gerencia de Gobierno Corporativo.
3. El acceso a blogs, redes sociales y páginas de entretenimiento, juegos, deportes, pornografía, música, videos, contenido violento, religión, y otros contenidos, que no tengan que ver con las actividades de trabajo no está permitido, salvo autorización previa de la Gerencia solicitante.
4. La Gerencia de Gobierno Corporativo, es la única con autoridad para permitir monitorear el tráfico de la red. Este monitoreo se debe efectuar solamente con la finalidad de detectar anomalías, fallas o actividades sospechosas, los informes deben estar disponibles para la Gerencia de Gobierno Corporativo.
5. Será sancionado cualquier uso comercial de los recursos y servicios de red e internet con fines diferentes a los de SNR.
6. Está prohibido descargar programas de internet "no autorizados" o sin licencia de uso de SNR.

13.4 Mensajería electrónica

La Gerencia de Gobierno Corporativo debe garantizar la disponibilidad y confiabilidad del correo electrónico de SNR.

El personal de SNR está obligado a utilizar de forma adecuada los servicios de red y el servicio de correo electrónico institucional.

La Gerencia de Gobierno Corporativo tiene la facultad de suspender el servicio de correo electrónico de SNR a la persona que haga mal uso.

No está permitido el uso del correo electrónico de SNR para:

a. Difundir cadenas de correos.

b. Difundir mensajes de discriminación racial, religiosa, política o de cualquier otra naturaleza.

c. Difundir mensajes que promocionen negocios personales o particulares.

Las únicas cuentas de correo autorizadas para el envío de mensajes de correo masivo son aquellas que por la naturaleza de sus funciones en SNR hayan sido creadas con este propósito específico.

Toda la información recibida, transmitida y almacenada en los servidores de correo electrónico se considera propiedad de SNR.

TÍTULO 14

Adquisición, Desarrollo y Mantenimiento de Sistemas de la Información

14.1 Seguridad de las Comunicaciones en Redes Públicas.

Protección de las transacciones por redes públicas

La Gerencia de Gobierno Corporativo y el proveedor de servicios de red deben establecer los mecanismos necesarios para la protección de la información, incluyendo como mínimo los siguientes aspectos:

1. Redes Privadas Virtuales (VPN).
2. Responsabilidades en torno a la seguridad de las bancas electrónicas contratadas por la Institución.
3. Lineamientos de control generales.
4. Autenticación de usuarios.

5. Autenticación de transacciones.
6. Trazabilidad de las operaciones.
7. Control de sesiones.

14.2 Seguridad en el Desarrollo.
Todo cambio o modificación en ambiente productivo del software de SNR, debe autorizarse por la Gerencia de Gobierno Corporativo.

La administración, mantenimiento y soporte de los sistemas de SNR, son responsabilidad de la Gerencia de Gobierno Corporativo, quien designa al personal capacitado para cumplir tales funciones.

TÍTULO 15

Relación con Proveedores.

15.1 Seguridad de Información en las Relaciones con Proveedores.
SNR reconoce que aun cuando la protección de los activos de información sea provista mediante un servicio tercerizado, ésta continúa siendo responsabilidad de SNR, por lo cual, se deberán aplicar las siguientes políticas:

Todos los contratos que formalice SNR con un prestador de servicios deben incluir una cláusula específica que asegure el cumplimiento a la política de seguridad de la información y los cambios que de ésta se deriven, durante el periodo de vigencia del contrato.

En caso de requerirse el trabajo de un tercero en las instalaciones de SNR o bien su acceso remoto a las redes y sistemas, debe existir un responsable por parte de SNR que solicite los accesos requeridos por el tercero.

15.2 La seguridad dentro de los acuerdos con los proveedores.
Todos los requisitos de seguridad de la información deben establecerse y acordarse con cada proveedor que pueda acceder, procesar, almacenar, transmitir, o proveer los componentes de

la infraestructura de TI para la información de SNR, asegurando el cumplimiento de los lineamientos que apliquen, de esta política.

Asimismo, se debe contar con acuerdos de confidencialidad firmados por los representantes legales de las empresas proveedoras de servicios, para asegurar que la información y los activos de información de la Institución a los que se tengan acceso durante la relación laboral y después, no se divulgue sin autorización, ni sea utilizada o modificada en perjuicio de la Institución.

15.3 Informar eventos de seguridad de la información

Es responsabilidad de todo el personal de SNR de reportar a la Gerencia de Gobierno Corporativo los incidentes de seguridad de la información que tengan una probabilidad de materializar un riesgo.

TÍTULO 16

Continuidad de la Seguridad de la Información.

16.1 Planificación de la continuidad de la seguridad de la información.

Se debe nombrar a un responsable para la coordinación del Plan de Contingencia y Continuidad del Negocio, en caso de un desastre.

El coordinador del Plan de Contingencia y Continuidad del Negocio debe mantener una estrecha comunicación con las áreas directivas, operativas, tecnológicas, personal de seguridad física y Protección Civil.

La Gerencia de Gobierno Corporativo debe proporcionar soluciones y servicios tecnológicos que permitan la redundancia para los procesos contemplados en el Plan de Contingencia y Continuidad del Negocio.

16.2 Implantación del plan de la continuidad de la seguridad de la información.
SNR dueña de sus procesos sustantivos y de apoyo, a través de sus responsables designados, deben contar con una estrategia de recuperación documentada y validada, siguiendo el Plan de Contingencia y Continuidad del Negocio vigente.

La Gerencia de Gobierno Corporativo debe contar con un programa de servicios de mantenimiento y soporte para conservar el adecuado funcionamiento de la infraestructura tecnológica con el objeto de contribuir a la continuidad de la operación.

16.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
La Gerencia de Gobierno Corporativo debe estar en conocimiento de los planes de recuperación, afín de validar el apego a la normativa vigente de SNR, antes de su aprobación para identificar posibles fallas, suposiciones inciertas, cambios en responsabilidades, nuevos requerimientos del negocio o regulaciones especiales, en estricto apego al Plan de Contingencia y Continuidad del Negocio vigente de SNR.

16.4 Derechos de propiedad intelectual.
La Gerencia de Gobierno Corporativo debe validar el uso de licencias y el cumplimiento con los derechos de autor de toda aplicación y herramienta de software utilizada en las estaciones de trabajo. Todo el software instalado en las computadoras de SNR debe ser legal.

Para cualquier desarrollo y en su caso mantenimiento de aplicativos de cómputo, se debe señalar que se constituirán a favor de SNR los derechos patrimoniales inherentes a la propiedad intelectual, a través del registro correspondiente, en el que se incluyan la totalidad de los componentes del aplicativo de cómputo de que se trate, como son: el código fuente, el diseño físico y lógico, los manuales técnicos y de usuario.

16.5 Revisión de Seguridad de la Información.
El personal que labora en SNR tiene la obligación de adoptar cualquier regulación en materia de seguridad de la información, que sea aplicable a SNR, o bien, cualquier normatividad que sea aprobada.

HOJA DE AUTORIZACIÓN

ELABORÓ

Lic. Lucio Crisban Manriquez Garnica
Analista de Fiscalización

REVISÓ

Lic. Bibiana del Carmen Palacio Azpeitia
Gerente de Gobierno Corporativo

AUTORIZÓ

Mtro. Víctor Manuel Cruz Martínez
Director General

Versión:	Aprobado/Autorizado					Vigente a partir de		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año	Día	Mes	Año
Elaboró: LCMG	Consejo de Gerentes de SNR Infraestructura, Mantenimiento y Servicios S. de R. L. de C. V.		08	05	2023	09	05	2023
Revisó: ECA								
Autorizó: VMCM								