LINEAMIENTOS DE SEGURIDAD PARA PROVEEDORES Y/O TERCEROS

Primera Edición

Integratel Perú S.A.A.

Código	Área		Fecha
IP-SEG-LS_007	Elaborado por	Gerencia de Seguridad Operacional	25/02/2026
	Aprobado por	Dirección de Seguridad e Inspección	23/04/2026

USO INTERNO

DERECHOS DE USO

CONTROL DE VERSIONES

Versión	Responsable	Fecha	Modificaciones
1	Gerencia de Seguridad Operacional	25.02 2026	Elaboración inicial del documento

ÍNDICE

1. Introducción o exposición de motivos

En Integratel Perú S.A.A. (en adelante, “INTEGRATEL” o la “Compañía”), la información, las personas, procesos, sistemas y redes que la soportan, son activos fundamentales cuya confidencialidad, integridad, disponibilidad y auditabilidad resultan esenciales para la continuidad del negocio. La protección de estos pilares no solo asegura el estricto cumplimiento de los requerimientos legales y regulatorios vigentes, sino que es un factor determinante para salvaguardar la reputación y la buena imagen de la Compañía ante sus clientes y el mercado.

Para garantizar este entorno de seguridad, la gestión de los activos debe basarse estrictamente en los lineamientos, normativas y procedimientos establecidos por la Compañía. El cumplimiento de estas directrices es de carácter obligatorio para todos los colaboradores, proveedores y terceros que se relacionen con INTEGRATEL, estableciendo así un compromiso conjunto para mitigar riesgos y promover un manejo responsable y transparente de la información en todos sus niveles.

2. Objeto

Establecer los requisitos de seguridad de la información, así como las obligaciones contractuales y regulatorias, que los proveedores deben cumplir obligatoriamente, con el fin de garantizar la protección, confidencialidad, integridad y disponibilidad de los activos de información de INTEGRATEL durante toda la relación comercial.

3. Alcance

El presente documento aplica a todos los proveedores y terceros. Su aplicación rige sobre cualquier servicio o producto que implique el acceso, procesamiento, almacenamiento o transmisión de activos de información de la Compañía, así como el acceso a su infraestructura física o lógica.

4. Definiciones

- Activo de Información: La información y su medio de soporte (por ejemplo, expedientes, bases de datos), así como los activos asociados con el procesamiento de dicha información (tales como computadoras, red interna, aplicativos).
- Vulnerabilidad: Una debilidad del activo o grupo de bienes que puede ser explotada por una amenaza.
- Amenaza: Una posible causa de una incidencia no deseada que puede provocar un daño a un sistema u organización.

- Impacto: Cambio adverso en el nivel de objetivos empresariales logrados.
- Probabilidad: Posibilidad de que se materialice el riesgo y afecte al negocio o la consecución de los objetivos.

- Cifrado: Proceso mediante el cual se toma un mensaje en claro, se le aplica una función matemática, y se obtiene un mensaje codificado.
- Correlación: En detección de intrusiones, relación que se establece entre diferentes fuentes de información.
- Denegación de servicio (DoS): Estrategia de ataque que consiste en saturar de información a la víctima con información inútil para detener los servicios que ofrece.
- Integración: En ingeniería de sistemas, combinación de componentes en una entidad coherente.
- Interfaz Común de Acceso (CGI): Especificación para la transmisión datos entre programas residentes en servidores Web y navegadores.
- Interfaz de programación de aplicaciones (API): Conjunto de rutinas, protocolos, y herramientas para la construcción de aplicaciones software.
- Interoperabilidad: Capacidad de un sistema para trabajar con otros sin que sean necesarios grandes esfuerzos por parte del usuario.
- Intrusión: Violación intencionada de las políticas de seguridad de un sistema.
- Red Privada Virtual (VPN): Red generalmente construida sobre infraestructura pública, que utiliza métodos de cifrado y otros mecanismos de seguridad para proteger el acceso y la privacidad de sus comunicaciones.
- Capa de Conexión Segura (TLS): Protocolo criptográfico que permite la transmisión cifrada y segura de información a través de redes. Se debe utilizar TLS en su versión 1.2 o superior, garantizando la confidencialidad, integridad y autenticación de los datos en tránsito.
- Paquete: Estructura de datos con una cabecera que puede estar o no lógicamente completa. Más a menudo, se refiere a un empaquetamiento físico de datos que lógico. Se utiliza para enviar datos a través de una red conmutada de paquetes.
- Parche: En seguridad informática, código que corrige un fallo (agujero) de seguridad.
- ACL: Listas de control de acceso.
- NE: Elementos de red.
- Terceros: Cualquier entidad externa, persona física o moral, ajena a la Compañía, con la que se establece un acuerdo, contrato o relación de colaboración para el intercambio de información, acceso a activos críticos o prestación de servicios. Esta categoría es omnicomprensiva e incluye proveedores, terceros, consultores externos, entes reguladores y subcontratistas.
- Proveedores: Entidad externa que suministra productos, licencias o servicios específicos a la Compañía mediante una transacción comercial. El proveedor es un tipo de tercero cuyo riesgo principal reside en la integridad de la cadena de suministro y la continuidad operativa del suministro entregado.

5. Lineamientos y Directrices de Seguridad

5.1. Gestión de activos

Los proveedores deberán identificar, gestionar y proteger adecuadamente todos los activos de información relacionados con los servicios prestados a la empresa, independientemente de su formato o medio.

Toda información nueva que sea generada, procesada o transformada por el PROVEEDOR, o por terceros subcontratados por este, en el marco de las actividades relacionadas con INTEGRATEL, será considerada automáticamente como Información Restringida, salvo que INTEGRATEL determine expresamente un nivel de clasificación distinto. La información que no sea generada por el PROVEEDOR mantendrá el nivel de clasificación previamente asignado por INTEGRATEL.

INTEGRATEL establece los siguientes niveles de clasificación de la información: Reservada, Restringida, Uso Interno y Pública. El PROVEEDOR y, cuando corresponda, los terceros de los que este se valga deberán tratar, proteger y manejar la información conforme al nivel de clasificación definido, aplicando los controles de seguridad correspondientes en cada caso.

Toda información deberá encontrarse debidamente etiquetada de manera visible y verificable, indicando su nivel de clasificación, independientemente del formato o medio en el que se encuentre.

La información clasificada como Reservada o Restringida, en formato electrónico, deberá almacenarse utilizando los mecanismos de seguridad adecuados a su criticidad, tales como controles de acceso, cifrado y medidas de protección lógica, garantizando que únicamente sea accesible por personal expresamente autorizado, tanto en los sistemas de información como en los medios de almacenamiento utilizados.

La información Reservada o Restringida en formato físico o impreso deberá mantenerse bajo custodia segura, mediante archivadores con llave u otros mecanismos equivalentes que aseguren su protección, confidencialidad y control de acceso.

La destrucción de la información clasificada como Reservada o Restringida, ya sea en formato electrónico o físico, deberá realizarse mediante métodos seguros que impidan su recuperación total o parcial por cualquier medio físico, lógico o electrónico, debiendo quedar evidencia de dicho proceso cuando así sea requerido por INTEGRATEL.

Considerando que el PROVEEDOR tendrá acceso a información y recursos confidenciales y críticos de INTEGRATEL, este deberá garantizar que dicha información no será divulgada, transferida ni compartida con terceros no autorizados, adoptando todas las medidas razonables, técnicas y organizativas, necesarias para su adecuada protección.

La obligación de proteger la información confidencial y clasificada se mantendrá vigente de forma indefinida, con independencia de la terminación, resolución o vencimiento de cualquier contrato o relación comercial entre INTEGRATEL y el PROVEEDOR.

El PROVEEDOR deberá asegurar que únicamente el personal que requiera acceso a información clasificada para la ejecución del servicio cuente con dicho acceso, aplicando el principio de mínimo privilegio.

El PROVEEDOR será responsable de capacitar a su personal en el correcto manejo y protección de la información clasificada.

Cualquier incidente de seguridad que involucre información Reservada o Restringida deberá ser notificado a INTEGRATEL de forma inmediata, conforme a los procedimientos establecidos.

La subcontratación de servicios que impliquen acceso a información clasificada requerirá autorización previa de INTEGRATEL, garantizando que los subcontratistas cumplan con los mismos niveles de protección aquí establecidos.

5.2. Cumplimiento Normativo y estándares Internacionales

El PROVEEDOR deberá cumplir en todo momento con la legislación vigente aplicable, así como con la normativa interna, políticas, lineamientos y controles que INTEGRATEL establezca o comunique durante la vigencia del Contrato.

Dicho cumplimiento incluye, sin carácter limitativo, las obligaciones relacionadas con protección de datos personales, seguridad de la información, ciberseguridad, prevención de fraude, continuidad operativa, telecomunicaciones y protección al consumidor, entre otras que resulten aplicables según la naturaleza del servicio.

El PROVEEDOR se obliga a:

- cumplir con todas las disposiciones legales, regulatorias y sectoriales que le resulten aplicables en el marco de la ejecución del Contrato;
- adecuar sus procesos y controles a los requerimientos que INTEGRATEL establezca en materia de seguridad, protección de datos personales y gestión de riesgos;
- adoptar medidas que permitan prevenir, detectar y responder a riesgos que puedan afectar la información, los servicios o los activos de INTEGRATEL.

Asimismo, el PROVEEDOR deberá adoptar y mantener buenas prácticas y estándares[1] reconocidos, nacionales o internacionales, acordes con la naturaleza de los servicios prestados y el nivel de riesgo asociado, tales como estándares de seguridad de la información, gestión de accesos, segregación de funciones, continuidad del negocio y ciberseguridad.

Cuando corresponda, INTEGRATEL podrá requerir al PROVEEDOR la acreditación de dichos estándares mediante certificaciones, auditorías externas, reportes de

[1] Sin carácter limitativo, algunos de estos estándares requeridos son: ISO/IEC 27001 (seguridad de la información), ISO 37001 (anticorrupción), NIST Cybersecurity Framework, PCI-DSS, TL9000 para operaciones Telco, estándares de auditoría de accesos y segregación de funciones (SoD).

cumplimiento u otros mecanismos equivalentes, los cuales deberán ser proporcionados dentro de los plazos que se establezcan.

El PROVEEDOR se obliga a mantener actualizadas sus prácticas y controles conforme a la evolución de la normativa aplicable, los riesgos tecnológicos y las exigencias razonables de INTEGRATEL durante la vigencia del Contrato.

5.3. Control de accesos

El PROVEEDOR será plenamente responsable de la administración segura de los accesos que INTEGRATEL le otorgue, asegurando que estos se utilicen únicamente para la ejecución de los servicios contratados y conforme a los lineamientos de seguridad establecidos.

El PROVEEDOR deberá designar formalmente un responsable de seguridad, quien actuará como único punto de contacto autorizado para la coordinación con el Oficial de Seguridad de INTEGRATEL de cada área involucrada y con el área de Seguridad de Redes de la Compañía.

El PROVEEDOR deberá informar oportunamente al Oficial de Seguridad del área usuaria de INTEGRATEL cualquier cambio relacionado con su personal, incluyendo las altas, modificaciones, reemplazo o modificaciones de roles y funciones que puedan afectar los accesos que fueron otorgados por la Compañía.

Previamente al inicio del servicio, así como durante su ejecución y al momento de su finalización, el PROVEEDOR y, cuando corresponda, los terceros que este subcontrate deberán solicitar la creación, modificación y revocación de usuarios conforme a los procedimientos definidos por INTEGRATEL, los cuales regulan el otorgamiento y retiro de accesos a los sistemas de información.

Asimismo, al término de la relación contractual o cuando sea requerido, el PROVEEDOR deberá garantizar la eliminación segura o devolución de toda la información de INTEGRATEL bajo su custodia, la devolución de los activos físicos y lógicos proporcionados para la prestación del servicio, y la generación y entrega de evidencia documentada que acredite la correcta ejecución de dichas actividades.

Todos los usuarios del PROVEEDOR y de los terceros que participen en la prestación del servicio deberán contar con un identificador único, personal e intransferible, quedando expresamente prohibido el uso de cuentas compartidas o genéricas.

Se prohíbe estrictamente la utilización de aplicaciones, herramientas o utilidades que puedan eludir, deshabilitar o debilitar los controles de acceso, seguridad o monitoreo, así como aquellas que no estén directamente relacionadas con la prestación del servicio contratado.

El acceso a la información de INTEGRATEL se limitará estrictamente bajo el principio de necesidad de conocer y mínimo privilegio, en función de las actividades autorizadas y del alcance del servicio contratado.

El PROVEEDOR deberá definir, documentar e implementar lineamientos que aseguren el uso de contraseñas robustas, incluyendo requisitos de complejidad, longitud mínima, no reutilización y cambios periódicos, conforme a las políticas de seguridad de INTEGRATEL.

El personal del PROVEEDOR cuyas funciones incluyan la implementación, configuración, modificación o baja de activos, así como el tratamiento de la información contenida en estos, deberá realizar dichas actividades exclusivamente mediante las cuentas personales asignadas, previa solicitud y autorización del propietario del activo. Toda gestión de cambios deberá ser documentada y registrada, y la evidencia correspondiente deberá ser entregada al finalizar las tareas.

El personal del PROVEEDOR no podrá modificar, restablecer o eliminar contraseñas de activos o sistemas sin contar con la autorización previa y expresa del propietario del activo.

Todo acceso a plataformas, sistemas o infraestructura de red de INTEGRATEL deberá realizarse utilizando protocolos de comunicación seguros, conforme a lo definido por el propietario del activo, tales como SSH, SFTP, HTTPS u otros protocolos cifrados debidamente autorizados según el tipo de conexión establecida.

En caso de que el personal del PROVEEDOR utilice equipos propios para acceder a las redes, sistemas o plataformas de INTEGRATEL, dichos equipos deberán cumplir, como mínimo, con los siguientes requisitos de seguridad:

- El equipo deberá encontrarse hardenizado, conforme a las mejores prácticas de seguridad recomendadas por el fabricante del sistema operativo y estándares de la industria.
- El equipo deberá someterse a un análisis de vulnerabilidades previo a su acceso a la red. El PROVEEDOR estará obligado a corregir todas las vulnerabilidades clasificadas como críticas o altas, debiendo aprobar un análisis posterior que valide su remediación antes de permitir el acceso.
- El acceso remoto deberá realizarse mediante mecanismos seguros adicionales, tales como VPN corporativa o soluciones equivalentes autorizadas.
- El PROVEEDOR deberá aplicar una política de gestión de parches y actualizaciones para los equipos utilizados por su personal, la cual podrá ser verificada o auditada por INTEGRATEL.
- Cada miembro del personal del PROVEEDOR deberá contar con una cuenta de usuario única y personal para el acceso al equipo utilizado en la red de INTEGRATEL.
- Queda prohibido el almacenamiento, transmisión o manipulación de contraseñas en texto plano.
- El equipo deberá contar con software antivirus/antimalware instalado, activo y actualizado.
- El equipo deberá tener habilitado cifrado completo de disco, utilizando algoritmos criptográficos robustos, tales como AES de 128 bits o superior o RSA-3072 o superior.
- En el caso de equipos móviles, como laptops, estos únicamente podrán conectarse a las redes expresamente habilitadas por INTEGRATEL para la ejecución de las tareas asignadas.

- Se deberá mantener registro y monitoreo de accesos, actividades privilegiadas y eventos relevantes de seguridad.

El PROVEEDOR deberá notificar de forma inmediata cualquier incidente de seguridad relacionado con accesos, credenciales o equipos utilizados para la prestación del servicio.

INTEGRATEL se reserva el derecho de suspender accesos de manera inmediata ante la detección de incumplimientos o riesgos de seguridad.

5.4. Seguridad Física

Se deberán respetar y utilizar adecuadamente los controles de acceso físico definidos por INTEGRATEL, con el fin de garantizar que únicamente el personal debidamente autorizado pueda ingresar y permanecer en las áreas, instalaciones y espacios bajo su administración.

El personal del PROVEEDOR y, cuando corresponda, los terceros subcontratados por este deberán portar en todo momento una identificación visible y válida, emitida o reconocida por INTEGRATEL, mientras se encuentren dentro de las instalaciones de la Compañía.

Salvo que exista una autorización previa, expresa y documentada por parte de INTEGRATEL, queda estrictamente prohibido retirar de las instalaciones cualquier infraestructura de tecnologías de la información y comunicaciones (TIC), equipos, dispositivos, soportes de almacenamiento o software que sea propiedad de INTEGRATEL.

Durante su permanencia en las instalaciones de INTEGRATEL, el personal del PROVEEDOR deberá garantizar la custodia permanente de la información confidencial, evitando dejarla expuesta, desatendida o accesible a personas no autorizadas, ya sea en formato físico o electrónico.

El acceso del personal del PROVEEDOR a instalaciones de INTEGRATEL deberá realizarse únicamente por zonas autorizadas, quedando restringido el ingreso a áreas críticas o sensibles salvo autorización expresa.

El personal del PROVEEDOR deberá estar acompañado o supervisado, cuando así lo determine INTEGRATEL, especialmente en áreas técnicas, centros de datos o salas de equipos.

Se prohíbe el ingreso de dispositivos de almacenamiento externos (USB, discos duros, etc.) y equipos no autorizados a las instalaciones de INTEGRATEL.

El PROVEEDOR deberá respetar los procedimientos de registro de ingreso y salida, incluyendo controles de visitantes, cuando estos sean aplicables.

Cualquier pérdida, robo o daño de activos físicos o información dentro de las instalaciones de INTEGRATEL deberá ser notificado de forma inmediata al área de seguridad correspondiente.

INTEGRATEL se reserva el derecho de realizar inspecciones o verificaciones razonables para asegurar el cumplimiento de los controles de seguridad física establecidos.

5.5. Gestión de las Comunicaciones y Operaciones

Queda estrictamente prohibida la realización de cambios, modificaciones o intervenciones sobre la infraestructura, sistemas, plataformas, redes o recursos que sean propiedad de INTEGRATEL, salvo que exista una autorización previa, expresa y documentada otorgada por la Compañía, conforme a los procedimientos de gestión de cambios establecidos.

El PROVEEDOR y, cuando corresponda, los terceros subcontratados por este deberán definir, documentar y mantener actualizados los procedimientos operativos y de comunicaciones asociados al servicio o producto brindado a INTEGRATEL, los cuales podrán ser solicitados por la Compañía para su revisión, validación o auditoría en cualquier momento.

Los equipos del PROVEEDOR y de los terceros que participen en la prestación del servicio y que se utilicen para conectarse a la red de INTEGRATEL no deberán contar con software de origen no confiable, incluyendo aplicaciones de procedencia desconocida, freeware, shareware o herramientas no autorizadas. INTEGRATEL podrá implementar controles preventivos y de detección para verificar el cumplimiento de este requisito.

Toda información transmitida a través de medios electrónicos, tales como correo electrónico, mensajería instantánea o transferencia de archivos, deberá contar con mecanismos de protección adecuados, acordes a su nivel de clasificación, que garanticen la confidencialidad, integridad y disponibilidad de la información durante su transmisión.

El PROVEEDOR deberá asegurar la generación, conservación y protección de registros de auditoría (logs) en los sistemas operativos, bases de datos y sistemas de información vinculados al servicio o producto prestado a INTEGRATEL. Los registros deberán contener información suficiente, íntegra y trazable que permita la investigación de eventos, incidentes de seguridad y actividades no autorizadas.

El PROVEEDOR deberá aplicar procedimientos formales de gestión de cambios, incluyendo análisis de impacto, autorización previa, pruebas y registro de cada cambio realizado.

Se deberá garantizar la segregación de funciones en las actividades operativas y administrativas, evitando que una misma persona tenga control total sobre procesos críticos.

El acceso a redes y sistemas de INTEGRATEL deberá realizarse a través de canales de comunicación seguros, tales como VPN corporativa o mecanismos equivalentes autorizados.

Los sistemas utilizados para la prestación del servicio deberán mantenerse actualizados, con parches y configuraciones de seguridad acordes a las políticas de INTEGRATEL.

El PROVEEDOR deberá implementar controles para prevenir la introducción de malware, incluyendo mecanismos de detección y respuesta.

Los registros de auditoría deberán estar protegidos contra alteración, eliminación o acceso no autorizado, y conservarse por un período acorde a los requerimientos legales, contractuales y de seguridad.

Cualquier interrupción, degradación del servicio o evento relevante en las comunicaciones u operaciones deberá ser notificado oportunamente a INTEGRATEL, conforme a los procedimientos establecidos.

INTEGRATEL se reserva el derecho de monitorear las comunicaciones y operaciones relacionadas con los servicios prestados, en cumplimiento de la normativa aplicable.

5.6. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

Previo a la aceptación, puesta en producción o conformidad formal por parte de INTEGRATEL de cualquier sistema de información desarrollado por el PROVEEDOR o por terceros bajo su responsabilidad, deberá realizarse un análisis de vulnerabilidades. Dicho sistema no podrá presentar vulnerabilidades clasificadas como críticas o altas, debiendo estas ser corregidas y validadas antes de su liberación.

El cifrado de la información deberá cumplir con los requisitos técnicos, legales y de negocio definidos por INTEGRATEL, utilizando algoritmos criptográficos robustos, vigentes y sin vulnerabilidades conocidas, tanto para la información en reposo como en tránsito.

Para la protección de la información en tránsito, se deberán emplear protocolos de comunicación seguros, tales como TLS en su versión 1.2 o superior (preferentemente TLS 1.3), quedando expresamente prohibido el uso de protocolos obsoletos o vulnerables, como SSL y versiones inseguras de TLS.

El uso de datos reales en ambientes de prueba, desarrollo o preproducción deberá evitarse. En caso de que su utilización resulte estrictamente necesaria, el PROVEEDOR y/o terceros deberán contar con la autorización previa y expresa de INTEGRATEL. Asimismo, deberá contar con procedimientos documentados de enmascaramiento, anonimización o mezcla de datos que garanticen la disociación de la información. En todo momento, la información utilizada para pruebas deberá mantenerse protegida y bajo control.

Las vulnerabilidades técnicas identificadas en los sistemas de información, ya sea durante el desarrollo, mantenimiento u operación, deberán ser notificadas de manera inmediata a INTEGRATEL, indicando su nivel de criticidad, impacto potencial y plan de remediación correspondiente.

El PROVEEDOR deberá aplicar principios de seguridad desde el diseño y por defecto (security by design & by default) en la adquisición y desarrollo de sistemas.

Se deberán definir y mantener entornos separados para desarrollo, pruebas y producción, evitando el acceso cruzado no autorizado.

Todo cambio en los sistemas deberá gestionarse mediante un proceso formal de gestión de cambios, que incluya evaluación de riesgos, aprobación, pruebas y documentación.

El código fuente deberá ser protegido contra accesos no autorizados y, cuando aplique, someterse a revisiones de código y análisis estático/dinámico.

Se deberá mantener un inventario de componentes de software, incluyendo bibliotecas y dependencias de terceros, y gestionar oportunamente sus vulnerabilidades.

El PROVEEDOR deberá asegurar que los sistemas cuenten con mecanismos de registro y monitoreo que permitan la detección de eventos de seguridad.

Las actualizaciones, parches y correcciones de seguridad deberán aplicarse de forma oportuna, conforme a los lineamientos de INTEGRATEL.

En caso de uso de servicios en la nube o componentes externos, el PROVEEDOR deberá garantizar que estos cumplan con los requisitos de seguridad definidos por INTEGRATEL.

5.7. Gestión de incidentes de Seguridad de la Información

El PROVEEDOR y, cuando corresponda, los terceros subcontratados por este estarán obligados a reportar en el plazo ≤ 1 hora a INTEGRATEL cualquier incidente de seguridad de la información que ocurra o sea detectado durante la prestación del servicio, independientemente de su origen, impacto o nivel de criticidad.

La notificación del incidente deberá realizarse a la brevedad posible al correo gestionincidencias.pe@integratel.com.pe, e incluir, como mínimo, una descripción preliminar del evento, los sistemas o información afectados, la fecha y hora de detección, así como las acciones iniciales de contención adoptadas.

Todos los incidentes de seguridad de la información serán gestionados, coordinados y liderados por INTEGRATEL, quien podrá requerir la colaboración activa del PROVEEDOR y/o terceros involucrados para la investigación, análisis, contención, erradicación y recuperación del incidente.

El PROVEEDOR deberá implementar las acciones correctivas y preventivas que se deriven del análisis del incidente, dentro de los plazos que ha establecido INTEGRATEL.

5.8. Gestión de Continuidad de Negocio

El PROVEEDOR y, cuando corresponda, los terceros subcontratados por este deberán definir, documentar, implementar y mantener un Plan de Continuidad del Negocio (PCN) que asegure la continuidad, disponibilidad y recuperación de los servicios o productos brindados a INTEGRATEL, en concordancia con los acuerdos contractuales, niveles de servicio (SLA) y requerimientos operativos establecidos.

El Plan de Continuidad del Negocio deberá contemplar los escenarios de interrupción relevantes, incluyendo fallas tecnológicas, incidentes de ciberseguridad, indisponibilidad de personal clave, desastres naturales y otros eventos que puedan afectar la prestación del servicio.

5.9. Cumplimiento de los Requerimientos Legales

El PROVEEDOR y, cuando corresponda, los terceros subcontratados por este deberán asegurar la protección adecuada de los activos de INTEGRATEL frente a amenazas de origen interno o externo, durante toda la vigencia y bajo las condiciones establecidas en la relación contractual, en estricto cumplimiento de los requerimientos legales, regulatorios, contractuales y corporativos aplicables.

El PROVEEDOR será responsable de identificar, conocer y cumplir con la normativa vigente que resulte aplicable a los servicios o productos prestados a INTEGRATEL, incluyendo, pero no limitándose a, leyes de protección de datos personales, regulaciones del sector telecomunicaciones, normas de propiedad intelectual y disposiciones sobre ciberseguridad.

El PROVEEDOR deberá garantizar que su personal y subcontratistas conozcan y cumplan los requisitos legales y contractuales relacionados con la seguridad de la información.

5.10. Seguridad de Recursos Humanos

El PROVEEDOR y los terceros de los que se valga, de ser el caso, deberá verificar los antecedentes de las personas que designan para la ejecución del contrato celebrado con INTEGRATEL. En ese sentido deberán contar con:

- Antecedentes policiales y penales.
- Copias de los certificados de educación superior, cursos y certificados laborales.
- Evaluación psicológica.
- El PROVEEDOR y los terceros de los que se valga, de ser el caso, entrenará a su personal en temas de seguridad de la información necesarios para asegurar que cumpla el esquema de seguridad debido-
- El PROVEEDOR es responsable de garantizar que los empleados que participen en la ejecución del servicio a INTEGRATEL no representen riesgos de seguridad para la misma y ante solicitud de INTEGRATEL proveerán información necesaria para evaluar los riesgos relacionados a su personal. Asimismo, el PROVEEDOR deberá firmar un Acuerdo de Confidencialidad de la Información establecido entre las partes.

5.11. Auditoría

A solicitud de INTEGRATEL, podrán realizarse auditorías, evaluaciones o revisiones de cumplimiento sobre el presente documento, con el objetivo de verificar el grado de conformidad, identificar brechas y, cuando corresponda, definir e implementar acciones correctivas.

Las auditorías podrán ser ejecutadas directamente por INTEGRATEL o por terceros designados por esta, y podrán abarcar aspectos organizativos, técnicos, operativos y documentales relacionados con los servicios o productos prestados por el PROV Las auditorías podrán ser ejecutadas directamente por INTEGRATEL o por terceros designados por esta, y podrán abarcar aspectos organizativos, técnicos, operativos y documentales relacionados con los servicios o productos prestados por el PROVEEDOR.

El PROVEEDOR deberá facilitar oportunamente toda la información, accesos, recursos y evidencias que le sean requeridos durante la ejecución de auditorías internas o externas, así como brindar las facilidades necesarias para su adecuado desarrollo.

6. Requerimientos de Seguridad

Se establecen a continuación los requerimientos mínimos de seguridad que deberán cumplirse obligatoriamente durante la implementación, configuración, operación y mantenimiento de equipos, sistemas y dispositivos que se integren o conecten a las redes y plataformas de INTEGRATEL ya sea que estos sean provistos por la Compañía, por el PROVEEDOR o por terceros bajo su responsabilidad.

El cumplimiento de estos requerimientos tiene como finalidad proteger la confidencialidad, integridad y disponibilidad de la información, así como garantizar la seguridad, estabilidad y continuidad de las operaciones de INTEGRATEL, conforme a los lineamientos internos, acuerdos contractuales y normativa aplicable.

6.1. Identificación y autenticación

Los sistemas, plataformas y equipos de comunicaciones deberán ser compatibles con la solución de gestión de accesos que tenga implementado INTEGRATEL.

Los sistemas, plataformas y equipos de comunicaciones deberán ser capaces de integrarse con un sistema de autenticación centralizado como por ejemplo sistemas basados en LDAP, SAML, OIC, RADIUS o TACACS.

Los sistemas, plataformas y equipos de comunicaciones no deberán permitir a ningún usuario tener más de 02 sesiones simultáneas abiertas desde diferentes IP de origen salvo por necesidades de servicios que se manejarán como excepciones.

Los sistemas, plataformas y equipos de comunicaciones deberán soportar la configuración de por lo menos un método alternativo de autenticación (por ejemplo, autenticación local) en caso de que la autenticación centralizada no esté disponible.

Se establece el uso obligatorio de autenticación multifactor (MFA) para todos los accesos remotos, así como para cuentas con privilegios elevados o que accedan a sistemas críticos, a fin de fortalecer la seguridad en los procesos de autenticación y reducir el riesgo de accesos no autorizados.

Los sistemas, plataformas y equipos de comunicaciones deberán ser capaces de crear y trabajar con ID de usuarios de por lo menos 8 caracteres alfanuméricos y deberá tener la siguiente estructura: primera letra de su primer nombre seguido de su apellido completo. Ejemplo Carlos Bueno Perez: cbueno o cbuenop en caso de duplicidad.

Se deberá permitir la deshabilitación y/o eliminación de usuarios (User ID).

Se deberán cambiar los identificadores que están definidos por defecto, tales como Administrador, Director, Auditor, Invitado, SysAdmin, etc., así como también las contraseñas por defecto de todos los usuarios.

Los sistemas, plataformas y equipos de comunicaciones no deberán mostrar información (banner) relacionada al servidor como el sistema operativo, aplicaciones o versiones usadas.

Las contraseñas no serán visibles en pantalla cuando se inicie el proceso de autenticación para todos los tipos de acceso permitido.

Frente a una autenticación fallida se deberá entregar un mensaje genérico (por ejemplo “Autenticación Fallida, ingrese nuevamente”), sin incluir mensajes específicos que puedan indicar cuál ha sido la secuencia del proceso que ha fallado, como, por ejemplo, “Password Errónea”, “Usuario no existe”, etc.

Los sistemas, plataformas y equipos de comunicaciones deberán soportar que el ID del usuario sea automáticamente bloqueado después de un numero predeterminado consecutivo de intentos fallidos (típicamente 5) dentro del intervalo de tiempo pre-configurado (típicamente 60 minutos). Estableciéndose un tiempo mínimo automático de reactivación (típicamente 15 minutos).

La solución deberá permitir la configuración del parámetro del plazo de días para el cambio de contraseña, y dicho parámetro se deberá configurar para forzar el cambio de las contraseñas cuyo periodo de tiempo es definido por INTEGRATEL (típicamente 30 días).

Los sistemas, plataformas y equipos de comunicaciones deberán soportar ser configurada para forzar a un usuario el cambio de su contraseña en su primer inicio de sesión.

Los sistemas, plataformas y equipos de comunicaciones deberán permitir que el usuario modifique su contraseña cuando éste lo requiera.

Los sistemas, plataformas y equipos de comunicaciones deberán solicitar la confirmación de la nueva contraseña para permitir el cambio de contraseña.

Los mecanismos de accesos a las aplicaciones deberán estar alineadas a los lineamientos de seguridad de contraseñas que ha definido INTEGRATEL. Las cuales deberán contemplar lo siguiente

- Se debe validar la correcta longitud, la cual debe ser no menor a 12 caracteres.
- Al menos debe contener una letra mayúscula, un número y un carácter especial.
- No debe comenzar por el identificador del usuario o el identificador escrito al revés (usuario administrador o cualquier otro identificador del personal).
- No debe utilizar palabras que estén relacionadas con el usuario como fecha nacimiento, DNI, nombre, apellido, área, o palabras comunes como “password”, “Integratel”, “admin”, “root”, “1234”, “redintel”.
- No debe ser deducible con técnicas basadas en diccionario o reglas, por ejemplo, del tipo caracteres consecutivos idénticos (abcdefg), todos numéricos (12345678) o todos alfanuméricos (¡”#$%&/).

Se recomienda implementar el uso de teclados virtuales para el ingreso de credenciales en todos los aplicativos que gestionen datos personales o información sujeta al secreto de las telecomunicaciones, con el fin de mitigar riesgos de captura de datos (*keylogging*).

Se debe implementar el uso de mecanismos de verificación tipo CAPTCHA en cada transacción realizada dentro de los aplicativos que involucren el tratamiento de datos personales e información protegida por el secreto de las telecomunicaciones, garantizando la legitimidad del origen de la petición.

Las contraseñas no deberán ser reusadas después de un periodo de tiempo definido por la empresa (típicamente 90 días).

6.2. Control de accesos

Los sistemas, plataformas y equipos de comunicaciones deberán tener tantos perfiles o roles de acceso basados en la criticidad de los privilegios, por ejemplo, perfil operación (quienes tienen habilidad de cambio de configuración), administración (quienes pueden hacer cambios o upgrade de software) y monitoreo (quienes pueden realizar seguimiento de transacciones y con acceso de lectura).

Los privilegios de acceso a la información y uso de recursos no deben ser otorgados a usuarios individuales, en su lugar deberá ser sobre perfiles o roles.

Los sistemas, plataformas y equipos de comunicaciones deberán tener la posibilidad de parametrizar el límite de acceso de los usuarios a los días de la semana y horas del día no laborables o fuera de su turno de trabajo. Los sistemas y programas que se adquieran por otra vía deberán contar con esta posibilidad identificando los posibles riesgos evaluados por las áreas de Seguridad de Red.

Los sistemas, plataformas y equipos de comunicaciones deberán ser configurables para sólo presentar al usuario comandos autorizados.

Los sistemas, plataformas y equipos de comunicaciones deberán configurar timeouts para la administración de conexiones, para evitar sesiones abiertas, las cuales deberán ser configurables. Típicamente en entornos de producción son 15 minutos.

Los sistemas, plataformas y equipos de comunicaciones deberán soportar listas de control de accesos ACL o filtros para limitar la administración y acceso, sólo desde la IP origen o rangos requeridos.

Los equipos de comunicaciones deberán soportar la configuración de puertos físicos, deshabilitando aquellos que no se usen. Los puertos físicos en los sistemas en producción desplegados deberán ser explícitamente deshabilitados.

Si hay límite máximo de sesiones remotas para administración de acceso, los sistemas, plataformas y equipos de comunicaciones deberán soportar la configuración de administración de acceso dedicado (terminal virtual vty) sólo accesible desde un IP o rango especifico. La razón es mantener uno o de ser posible libre los puertos vty para emergencias de acceso.

Los administradores deben configurar dentro de lo posible o renombrar usuarios “administrator” o “root”, para restringir el acceso remoto como super administrador y registrar cambios por aumento de privilegios.

6.3. Sistema Operativos

La lista de requisitos de seguridad indicados a continuación aplica a sistemas operativos diversos, no obstante, algunos están enfocados a sistemas UNIX/Linux:

El sistema operativo y aplicaciones deberán tener instaladas las últimas actualizaciones de seguridad.

Se deberá realizar un proceso de hardening para poder asegurar el sistema operativo y aplicaciones de todos los elementos que forman parte de la solución. De esta forma se eliminará software, servicios y usuarios innecesarios o por defecto.

Los usuarios genéricos que sea necesario utilizar (dueño de aplicación o transferencia) no deben tener acceso directo al intérprete de comandos del sistema, y deben tener un entorno restringido, adecuado a sus funciones.

Las aplicaciones no deben utilizar scripts con permisos SUID- SGID. Para el caso de binarios de la aplicación que requieran la utilización de dicha funcionalidad, la aplicación no debe requerir que el propietario sea root y los grupos no deben ser los de sistema (bin, adm, sys, etc).

Todo directorio de escritura común (/tmp) para todos los usuarios del sistema operativo deben tener sus permisos el flag de “sticky bit”.

6.4. Auditoria y Monitoreo de Logs

Los registros de auditoría deberán estar accesibles on-line como mínimo durante un 1 mes. A partir de este tiempo deberán estar disponibles off-line durante el límite temporal de conservación definido por los requerimientos del negocio y regulatorios.

Como norma general, los registros de auditoría se conservarán por un periodo mínimo de dos (2) años para aquellos sistemas que involucren el tratamiento de datos personales, en cumplimiento con el Reglamento de la Ley de Protección de Datos Personales. Para otros eventos de seguridad o auditoría interna, el tiempo de retención estándar será de cinco (5) años, salvo que exista una disposición legal o contractual superior.

La generación de logs o eventos de seguridad de los equipos deberá ser habilitado, para conocer las acciones tomadas sobre el equipo, así como quienes realizaron el acceso sobre la plataforma, y de esta forma obtener mayor nivel de auditoría e inclusive facilitar un análisis forense (de ser el caso) después algún incidente de seguridad.

Intentos de autenticaciones fallidas deberán ser registrados.

El inicio y fin de la conexión del usuario deberán ser registradas.

El sistema debe registrar todas las acciones de los administradores y personal que realiza configuraciones (usuarios con máximos privilegios).

Los logs de auditoría y transaccional, deberán estar protegidos de modificaciones no autorizadas, y deberán existir controles para detectar manipulaciones y/o accesos no autorizados.

El equipo debe ser configurado para generar logs de denegación de tráfico en filtros IP o ACL's.

El registro de auditoria debe contener por lo menos la siguiente información (cuando sea relevante):

- Sistema, aplicación o elemento que ha generado el registro.
- ID de usuario, programa, o elemento que causa el evento (ejemplo user login, procesos ID, dirección IP, terminal, local, etc)
- Fecha y hora de ocurrencia del evento.
- Descripción del evento que está siendo registrado (ejemplo acceso, sistema shutdown, crash, error, etc)
- Tipo de Acción: Autorizado, Rechazado.

Un evento de seguridad será generado si hay intentos no autorizados de querer modificar el contenido de los registros de auditoría.

La solución deberá ser capaz de enviar registros generados a un sistema centralizado en la red SIEM (Security Information and Event Management), que almacene y centralice los eventos de seguridad. La colección de eventos de seguridad será hecha a través de agentes instalados sobre el elemento o usando los protocolos de auditoría de logs: netflow, ODBC, Syslog, snmp y SDEE. La solución deberá ser compatible con SIEM corporativo.

La solución debe soportar el configurar múltiples servidores a quienes se les va a enviar mensajes de registros de auditoría.

El sistema que almacena registros de auditoria debe permitir monitoreo de capacidad del sistema vía traps snmp hacia el recolector corporativo.

La solución deberá soportar NTP y de preferencia deberá usar NTPv4 (más estable y soporte 64bits en timestamps)

6.5. Comunicaciones y Redes

La solución debe incluir agentes SNMP que permite monitoreo en tiempo real de parámetros para operación y usabilidad. Se deberá implementar el protocolo SNMPv3 de forma mandatoria, salvo excepciones sustentadas.

Requerimientos SNMPv3

- El agente deberá soportar ambos niveles de seguridad AuthNoPriv (sin encripción) y AuthPriv(autenticados y encriptados).
- El sistema deberá soportar una interface IP específica y físicamente independiente, el cual permite un direccionamiento exclusivo, independiente desde las interfaces usadas para la entrega del servicio, sólo para la administración de red.

Elementos de comunicaciones que soportan filtrado de tráfico IP deben implementar los siguientes tipos de filtros:

- Lista de control de accesos (estándar y extended) por interfaces físicas y lógicas como 802.1q.
- Lista de control de accesos de nivel 3 (IP origen y destino) y nivel 4 (ICMP code, para TCP o UDP origen o destino) aun en condiciones complejas como rangos de puertos.
- Teniendo la habilidad para definir y aplicar filtros a nivel IP VLAN (VLAN ACL's)
- Aplicando ACL's de tráfico sobre interfaces físicas y lógicas tanto en sentido incoming como outgoing aún con interfaces VRF.
- Filtros aplicados enviados dinámicamente vía atributos Radius en autenticaciones de usuarios.
- Filtros anti-spoofing para prevenir cambios de IP de usuarios.
- Filtro de tráfico IPv6 debe ser soportado.

Los elementos de red presentados en la solución con protocolos de ruteo dinámico deberán incluir la habilidad de filtrar información de enrutamiento, y soportar autenticación en protocolos de enrutamiento para evitar la inserción de rutas inválidas de fuentes no autorizadas. La configuración de enrutamiento debe ser soportado sobre interfaces físicas y lógicas.

La solución deberá ser capaz de restringir el uso de brocadcast directos.

La configuración "ignore gratuitous" ARP deberá ser soportado.

Los elementos de red deberán ser configurados para no permitir enrutamiento de tráfico entre sus diferentes interfaces.

Los elementos de red deberán ser capaces de evitar pasar paquetes IP peligrosos o fuente de redirección de enrutamiento.

La solución debe ser capaz de deshabilitar envío de mensaje "ICMP unreachable" cuando un paquete es denegado por lista de acceso.

Los sistemas TCP con acceso a servicios de internet deberán soportar un mecanismo de protección contra SYN Flood attacks.

Los sistemas de comunicaciones deberán ser capaces de cifrar si estos pasan de un acceso de usuario remoto a red corporativa interna (vía telefónica, wireless, internet, etc.)

Si la solución soporta interfaces Wifi deberá soportar encriptación WPA y WPA2.

Requerimientos de protocolo SCP

- El sistema debe implementar protocolo SCP con soporte SSH para encriptación de data en la transferencia de información.
- El sistema trabajara en entorno cliente – servidor

Requerimientos para Fibra Óptica

- Para las redes de fibra redundada es necesario garantizar la alta disponibilidad mediante una configuración de QuadPath con Failover sin Failback de ser el caso.

- Para garantizar la alta disponibilidad cada servidor debe disponer de al menos dos puertos físicos en HBAs (Host Bus Adapter) independientes. Se recomienda utilizar cuatro puertos físicos en dos tarjetas DualFB (dos puertos físicos en tarjetas diferentes es válida).
- Si se utilizan 2 puertos físicos de fibra por servidor (2 SingleFB) siempre deben configurarse dos puertos lógicos sobre cada puerto físico. Conectando los puertos físicos a switches de fibra diferentes.
- Para las redes de fibra de backup se requerirá la configuración mínima de un camino desde cada servidor a cada switch de fibra, que interconecta con el robot (sistema centralizado backup) y el administrador de backup.
- Los robots poseen una interfaz de fibra por cada tape (o cabina de discos redundante), por lo que siempre que sea posible se conectaran la mitad a un switch y la otra mitad a otro switch.

6.6. Control de Software

Las aplicaciones no deberán ser dependientes de servicios y configuraciones de sistema operativo, en caso contrario el flujo del funcionamiento de la aplicación deberá estar debidamente documentado:

- Validación de entradas. Todas las entradas deben ser validadas en el sentido de verificar que el dato entregado se encuentra dentro de lo esperado. Este concepto incluye, los argumentos de una línea de comando, las interfaces de red, las variables de ambiente de cualquier tipo, los datos recibidos por medio de interfaces con otros componentes y sistemas y las entradas por parte de los usuarios.
- Principio de Mínimos Privilegios. Adoptar este principio en el diseño y en la codificación, garantizando que un proceso siempre se ejecutará con el conjunto mínimo de privilegios que necesita para ejecutar la acción.
- Sanidad de los datos. Como contrapartida a la Validación de Entradas, toda la información enviada entre procesos o subsistemas de la plataforma, ó enviados a sistemas externos, deben ser sometidos a controles de “sanidad” para garantizar que los mismos están bien formados y son consistentes.
- Para el caso específico de aplicaciones WEB se debe considerar las recomendaciones de OWASP Top 10 2013, CWE/SANS Top 25 Most Dangerous Software Errors y Web Application Security Consortium (WASC).

En el diseño de la arquitectura del software se deberá considerar y documentar:

- Escalabilidad horizontal y vertical.
- Portabilidad, con la finalidad evitar la necesidad de modificar el código ante distintas situaciones.
- Composición de servicios de infraestructura, como, por ejemplo, Servicios de log, pool de conexiones, sistema de configuración, gestor de accesos, permisos y roles de usuarios, etc.
- Descripción funcional del sistema.
- Colaboración entre aplicaciones, con la finalidad de evitar el acceso directo al repositorio de información:

- Componentes frontales: Invocación de servicios de negocio de una aplicación desde otra mediante un componente, usado para transacciones distribuidas.
- Servicios web: invocaciones remotas en formato xml sobre protocolo http. Publicar un “Servicio Web” por cada servicio de negocios que se desea compartir con otras aplicaciones.

La solución debe ser capaz de deshabilitar servicios no requeridos.

Los desarrolladores deberán utilizar, siempre que se pueda, las facilidades de seguridad integrada con el Sistema Operativo o la Base de Datos y no deberán construir otros mecanismos para almacenar contraseñas o autenticar usuarios. De ser necesario implementar algún otro mecanismo, se deberá solicitar validación de su uso a las áreas de Seguridad.

La solución deberá permitir monitoreo en tiempo real de parámetros de operación y capacidad.

La solución deberá tener mecanismos que aseguren la integridad de archivos, parches del sistema operativo y actualizaciones de software antes de su pase a producción.

La solución deberá ser capaz de generar alarmas y detectar alguna configuración inconsistente. Esta verificación deberá ser completada antes de que la configuración este activa o antes de su pase a producción.

La solución debe ser capaz de detectar cuando tiene insuficiente memoria para cargar nuevas configuraciones o software y previamente notar la ocurrencia de un evento, deshabilitándola y manteniendo la configuración previa.

La solución deberá tener mecanismos para detectar y prevenir la instalación o ejecución de código malicioso (virus, troyanos, gusanos, etc.).

Archivos críticos, los cuales incluyen binarios y archivos de configuración deberán ser protegidos por permisos en los archivos de tal forma que solo usuarios autorizados puedan visualizar y modificar su contenido.

El proveedor deberá proporcionar una estrategia de respaldo de la información y apoyar a INTEGRATEL en su implementación. Esta estrategia deberá estar alineada con los estándares y políticas existentes.

La solución deberá proporcionar procesos de respaldo y de paso a histórico.

La solución deberá proporcionar los procedimientos para la recuperación ante fallos habituales.

Las acciones por realizar en caso de fallo (procedimientos de gestión de errores) deberán estar extensamente documentados.

6.7. Bases De Datos

Deberá soportar y ajustarse para su normal funcionamiento, a los siguientes requerimientos y roles de usuarios:

- Cuentas Dueñas de Esquema: Son aquellas con las que se crean todos los objetos que contendrá la aplicación, sus privilegios, roles, etc. Su única función es precisamente el armado del ambiente y su puesta a punto previo a la explotación. Una vez finalizado el mismo, deben permanecer bloqueadas en los ambientes Productivos, y sólo serán usadas para ajustes o creación de nuevos objetos en él.
- Cuentas de Explotación: Son las responsables de la ejecución de procesos específicos de la aplicación. Deben tener asignados los privilegios necesarios de actualización y ejecución correspondientes.
- Cuentas de Consulta: Son aquellas dedicadas a la extracción específica de información.
- Cuentas Personalizadas: Cuenta necesaria para realizar consultas de información o tareas de soporte por parte de los usuarios. Únicamente podría contener un role que involucre privilegios de select sobre los objetos de un esquema. En caso de ser necesarios privilegios de select sobre los objetos de un esquema.

En Oracle sobre sistemas operativos UNIX, no se utilizarán usuarios de UNIX con autenticación externa para validarse en la base de datos.

La forma en que los usuarios de la aplicación autentican con la base de datos debe ser de forma tal que garantice:

- Que todos los usuarios de las bases de datos deberán poseer y cumplir la Lineamientos de gestión de contraseña y restricciones frente a los intentos de acceso fallido.
- Que las contraseñas no están almacenadas de forma plana (texto plano legible) en ninguna parte de la aplicación ni del código.
- Que las contraseñas pueden cambiarse de forma periódica sin tener que tocar el código de la aplicación.
- Que la contraseña no deberá estar escrita en ninguna forma de código de aplicación. De ser necesario, por la funcionalidad propia de la aplicación, se deberán utilizar mecanismos de encriptación de dichos archivos u otras metodologías.
- Se deberá tener las contraseñas de administración resguardadas bajo un procedimiento de custodia.

La aplicación debe conectarse a la base con un esquema de mínimos privilegios que debe ser validado y documentado.

La aplicación deberá proveer la trazabilidad mínima que garantice un adecuado seguimiento de las acciones desarrolladas sobre los objetos que utilice.

El usuario dueño del esquema es responsable de la creación de todos los objetos que estarán contenidos en el esquema. Esta cuenta podrá crear cualquier tipo de objeto y asignar mediante comando grant los privilegios.

El usuario de explotación es el responsable de la ejecución de los procesos inherentes al esquema. Esta cuenta no es dueña del esquema, pero puede tener los privilegios que le permitan hacer Insert, Update y Delete sobre las tablas necesarias.

El usuario de consulta será el responsable de realizar consultas de información. Este tipo de usuarios solo podrá tener un role que involucre privilegios de select.

El usuario dueño de esquema no podrá ser utilizado para el acceso y la explotación de la base (ni por el software ni por ningún usuario), la misma permanece bloqueada y solo se habilita en el momento en el cual se necesita modificar los objetos del esquema de la base de datos.

Los usuarios que cumplan con un rol dueño de esquema de una aplicación deberán tener un entorno restringido adecuado a sus funciones (privilegios).

Los file systems generados ad_hoc, para los data files, etc, deberán montarse por defecto con las opciones “nosuid” (no permite fijar id de usuario o id de grupo) y “nodev” (no interpreta caracteres o bloques especiales sobre el file system).

No deberán ser montados recursos de la base de datos sobre el file system de root “/” del sistema operativo.

Los recursos necesarios para aplicaciones, logs del sistema y/o aplicaciones, repositorio de procesos, en resumen, todo lo necesario en cuanto a la explotación de la base de datos deberán estar montados en un file system generado únicamente para esta necesidad.

La solución preferentemente no deberá trabajar en sus puertos por defecto.

La solución deberá tener un plan de actualizaciones de seguridad alineados con los paquetes que publica el fabricante.

La solución deberá tener la capacidad de encriptar tablas acordes con la clasificación de la seguridad de la información corporativa.

La solución deberá tener la capacidad de bloquear y/o eliminar usuarios por defecto no usados.

La solución deberá proteger al listener cambiando el puerto por defecto y/o asignando contraseña.

Definir y documentar las características y Ubicación de Tabla de Auditoría AUD$ para el caso de Oracle.

Limitar la asignación de privilegios excesivos sobre objetos públicos (PUBLIC), asegurando que únicamente se otorguen los accesos estrictamente necesarios bajo el principio de mínimo privilegio.

En caso de tratamiento de datos personales, se deberá implementar una gestión segura de claves criptográficas, que incluya su generación, almacenamiento seguro, distribución controlada, rotación periódica y revocación, así como el uso de algoritmos de cifrado robustos y vigentes, conforme a las mejores prácticas de seguridad de la información.

6.8. Inteligencia Artificial (IA)

El proveedor deberá cumplir, en todo momento, con los documentos de INTEGRATEL referente a IA, así como con los lineamientos y controles que la COMPAÑÍA establezca sobre el uso de dichas herramientas.

Se encuentra prohibido el ingreso, carga, uso, procesamiento o tratamiento de información confidencial de INTEGRATEL, datos personales bajo responsabilidad de INTEGRATEL, así como código fuente, configuraciones, arquitectura o diagramas de red, en herramientas de inteligencia artificial de acceso público o no autorizadas por la COMPAÑÍA.

Asimismo, se prohíbe expresamente el uso de información de INTEGRATEL para el entrenamiento, ajuste o mejora de modelos de inteligencia artificial externos.

De manera excepcional, el uso de sistemas basados en IA podrá autorizarse únicamente cuando se encuentre debidamente declarado por el proveedor en el DPA y el sistema haya sido previamente evaluado y aprobado por INTEGRATEL. El incumplimiento de lo dispuesto en el presente acápite será considerado un incumplimiento grave, sin perjuicio de las responsabilidades legales y contractuales que pudieran derivarse.

6.9. Integración con control de accesos (ACNE)

Para SSO de dispositivos (CLI) Integración

- El dispositivo debe soportar conectividad IP.
- El dispositivo debe soportar versiones estándar de protocolos de SSH, SFTP.
- La documentación del dispositivo deberá contener todos los detalles de los comandos y los métodos utilizados para el dispositivo de inicio de sesión y cierre de sesión.
- La documentación incluirá descripción completa de las interfaces por tipo NE (Network Element), por ejemplo, el número de interfaces de SSH, SFTP.
- La documentación indicará si las interfaces no comparten la misma lista de credenciales. Por ejemplo, diferentes credenciales necesarias para SSH.

Para SSO GUI / Integración de Aplicaciones

- La aplicación debe soportar la conectividad IP.
- La aplicación debe instalarse en un entorno Windows Terminal Server o ser accesible desde el servidor de terminal a través de un navegador o conexión a un entorno Citrix.
- Un único conjunto de credenciales por usuario debe ser requerido para inicio de sesión a la aplicación final.
- La aplicación se debe ejecutar en un entorno compartido por varios usuarios. Por ejemplo, varios usuarios conectados a un servidor Windows Terminal.

Para seguridad de la contraseña en la integración de los NE

- El dispositivo/aplicación deben soportar las funciones de administración de usuario y contraseñas, de forma programática, interfaces de línea de comandos, incluyendo la creación de cuentas, supresión, modificación de la contraseña y el nivel de autorización.
- Las cuentas predeterminadas deben enumerarse, poder eliminarse, y como mínimo tener restablecimiento de contraseña.
- Deben existir varios niveles de autorización.

6.10. IPV6

La solución deberá tener filtro de capacidad de enrutamiento IPv6.

La solución deberá soportar ACL para IPv6 así como IPv4.

La solución deberá soportar y administrar los protocolos SNMP, NTP, SSH, etc. para IPv6.

La solución deberá permitir/deshabilitar servicios ejecutándose en IPv6.

La solución deberá permitir el filtrado de tráfico dependiente sobre paquetes ICMPv6; así como, también deberá permitir/rechazar tráfico dependiente sobre opciones de cabecera y sobre un origen/destino IPv6.

La solución deberá denegar tráfico IPv6 si no hay servicio IPv6 disponible.

El proveedor deberá describir cualquier medida de seguridad propuesta para IPv6 y protección DoS así mismo deberá identificar los diferentes registros para actividades maliciosas.