LINEAMIENTOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN
PARA PROVEEDORES

1. INTRODUCCIÓN

La información de TELEFÓNICA, así como las personas, procesos, sistemas y redes que la soportan son activos importantes de la empresa. Su confidencialidad, integridad, disponibilidad y auditabilidad son esenciales para mantener la seguridad de dicha información y para cumplir los requerimientos legales y regulatorios, así como mantener la buena imagen de la organización.

Para garantizar la seguridad de la información es importante que la gestión de la misma se realice sobre la base de lineamientos, normativas y procedimientos que deberán ser cumplidos por los colaboradores, proveedores y terceros en general con los que TELEFÓNICA se relacione.

2. OBJETIVO

Regular las obligaciones acerca de la seguridad de la información que deben cumplir los proveedores de TELEFÓNICA.

3. 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 o 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 (SSL): Protocolo creado por Netscape para permitir la transmisión cifrada y segura de información a través de la red.
- 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.
- IDM: Gestión de identidades.

4. LINEAMIENTOS Y DIRECTRICES DE SEGURIDAD

4.1. Controles previos

- Previamente al inicio de cualquier servicio que implique acceder, procesar, comunicar o gestionar la información de TELEFÓNICA o a la prestación de servicios de procesado de información, el PROVEEDOR deberá cumplir los controles de seguridad requeridos por TELEFÓNICA.

4.2. Gestión de Activos y Clasificación de la Información

- Cualquier nueva información generada por el PROVEEDOR o los terceros de los que éste se valga, relacionada con las actividades de TELEFÓNICA se considera Restringida. Caso contrario mantiene el nivel de clasificación indicado por TELEFÓNICA.
- TELEFÓNICA clasifica su información en Reservada, Restringida, Uso Interno y Pública.
- El PROVEEDOR y los terceros de los que éste se valga, de ser el caso, deberán tratar la información de acuerdo al criterio de clasificación establecido.
- La información será etiquetada de forma tal que indique su nivel de clasificación.
- La información “Reservada” y “Restringida”, en formato electrónico, se almacenará con los respectivos mecanismos de seguridad que amerite el documento tanto en los sistemas de información como en los soportes informáticos para que pueda ser accesible solo por las personas autorizadas para su uso.
- La información “Reservada” y “Restringida” en soporte impreso se almacenará bajo llave o cualquier otro mecanismo que garantice su custodia con total confidencialidad.
- La destrucción de la información “Reservada” o “Restringida” (en formato electrónico o físico) se realizará de forma que no se pueda recuperar total o parcialmente por ningún medio físico o electrónico.
- Dado que el PROVEEDOR tendrá acceso a información y recursos confidenciales y críticos de TELEFÓNICA, debe garantizar que dicha información no será divulgada o compartida a terceros tomando las precauciones razonables para la protección de dicha información confidencial.
- La protección de toda información confidencial deberá permanecer vigente indefinidamente y de manera independiente a la finalización de cualquier contrato de prestación de servicios con el PROVEEDOR.

4.3. 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 TELEFÓNICA. 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 TELEFÓNICA no representen riesgos de seguridad para la misma y ante solicitud de TELEFÓNICA 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.

4.4. Áreas seguras

- Se utilizarán correctamente los controles físicos de entrada establecidos para asegurar que únicamente accede el personal autorizado a los espacios de los que dispone TELEFÓNICA.
- El PROVEEDOR y los terceros de los que se valga, de ser el caso, deberán llevar su identificación, en un lugar visible, mientras permanezcan en instalaciones de TELEFÓNICA.
- Salvo en aquellos casos en que se reciba autorización expresa de TELEFÓNICA, se prohíbe sacar de las instalaciones de ésta cualquier infraestructura TIC o software propiedad de TELEFÓNICA.
- Durante su permanencia en las instalaciones de TELEFÓNICA, el personal del PROVEEDOR no podrá dejar fuera de custodia información confidencial de la organización comprometiendo su confidencialidad.

4.5. Gestión de las Comunicaciones y Operaciones

- Se prohíben los cambios sobre las infraestructuras y los recursos de propiedad de TELEFÓNICA, salvo autorización expresa de ésta.

- El PROVEEDOR y los terceros de los que se valga, de ser el caso, deberán documentar sus procedimientos de operaciones y comunicaciones relacionados al servicio o producto que brinda a TELEFÓNICA, el cual ésta puede requerir para revisión.
- Los equipos del PROVEEDOR y los terceros de los que se valga, de ser el caso, usados para conectarse a la red de TELEFÓNICA no deberán tener instalado software de procedencia dudosa, de freeware, shareware o similares. TELEFÓNICA establecerá controles preventivos y detectivos orientados hacia dicho fin.
- La información que sea transmitida mediante mensajería electrónica debe ser protegida apropiadamente.
- El PROVEEDOR y los terceros de los que se valga, de ser el caso, deberán garantizar que existan los registros de auditoría en los sistemas operativos, en las bases de datos y en los sistemas de información relacionados al servicio o producto que brinda a TELEFÓNICA. La información que se almacene en estos registros debe permitir investigaciones futuras.

4.6. Control de Accesos

- El PROVEEDOR será responsable de gestionar de manera segura los accesos otorgados por TELEFÓNICA.
- El PROVEEDOR deberá reportar al Oficial de Seguridad del área usuaria de TELEFÓNICA, cambios de personal y de sus roles y/o funciones.
- El PROVEEDOR deberá designar a un responsable, el cual será el único autorizado para coordinar con el Oficial de Seguridad de TELEFÓNICA de cada área y con el área de Seguridad de Redes.
- El PROVEEDOR y los terceros de los que se valga, de ser el caso, previa a la prestación y a la finalización del servicio en TELEFÓNICA, deberá solicitar el alta y baja de usuarios en base a los procedimientos establecidos que concede y revoca el acceso a los sistemas de información.
- Todos los usuarios del PROVEEDOR y los terceros de los que se valga, de ser el caso, dispondrán de identificador único de usuario para su uso personal y exclusivo.
- Se prohíbe el uso de aplicaciones y/o utilidades que pudieran invalidar los controles de acceso y/o aplicación y las no asociadas a la prestación del servicio contratado.
- El acceso a la información de TELEFÓNICA será restringida en función a la necesidad de conocer, para los servicios contratados al PROVEEDOR.
- El PROVEEDOR y los terceros de los que se valga, de ser el caso, deberán definir lineamientos e implementar medidas para asegurar el uso de contraseñas fuertes y cambio periódico de las mismas.
- El personal del PROVEEDOR, cuyas tareas impliquen la implementación, configuración, modificaciones o baja de activos así como el tratamiento de la información contenida en ellos, deberá ejecutar dichas tareas haciendo uso de las cuentas personales asignadas, así como previa solicitud y autorización del propietario del activo, documentando en todo momento la gestión de cambios realizada; la cual debe ser entregada al finalizar dichas tareas.
- El personal del PROVEEDOR no podrá modificar o eliminar cualquier contraseña sin la autorización previa del propietario del activo.
- Todo acceso a plataforma o infraestructura de red deberá ser ejecutado utilizando protocolos seguros, de acuerdo a lo establecido por el propietario del activo. Dichos protocolos serán ssh, sftp, https, entre otros; dependiendo el tipo de conexión establecida y autorizada contra el activo.
- En el caso de que el personal del PROVEEDOR utilice equipo propio para acceder a las redes y plataformas de TELEFÓNICA, éste debe cumplir todos los requerimientos de seguridad mínimos listados a continuación:
  - ✓ Equipo hardenizado según las mejores prácticas de seguridad establecidas por el fabricante del sistema operativo
  - ✓ El equipo deberá ser sometido a un análisis de vulnerabilidades antes de su acceso a las redes y/o plataformas. El PROVEEDOR deberá subsanar todas las vulnerabilidades críticas y altas halladas en el equipo antes de su ingreso a red, para lo cual será sometido a un segundo análisis que certifique el levantamiento de dicha vulnerabilidades.
  - ✓ El PROVEEDOR deberá seguir una política de parchado a los equipos asignados a su personal, el cual podrá ser auditado por TELEFÓNICA.
  - ✓ El PROVEEDOR le asignará a su personal una cuenta de usuario única para su acceso al equipo a utilizar en la red de TELEFÓNICA.
  - ✓ Las contraseñas no podrán ser manipuladas en texto plano.
  - ✓ El equipo deberá tener instalado y ejecutándose un antivirus.

- ✓ El equipo deberá contar con cifrado de disco duro basada en algoritmos AES de 128 bits o mayor, o RSA-3072 o mayor.
- ✓ En caso de tratarse de un equipo móvil como una laptop, ésta no podrá conectarse a una red fuera de las habilitadas por TELEFÓNICA para las tareas asignadas.

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

- Previo a la conformidad, por parte de TELEFÓNICA, de un sistema desarrollado por el PROVEEDOR o externo, se realizará un análisis de vulnerabilidades. Este sistema no deberá tener vulnerabilidades críticas y altas.
- El cifrado de información seguirá los requerimientos establecidos por TELEFÓNICA para el cumplimiento de requisitos legales y de negocio, empleando algoritmo de cifrado fuerte que no padezca vulnerabilidades ni debilidades conocidas.
- Se evitará el uso de datos reales en el entorno de pruebas. En caso de recurrir a datos de este tipo, el PROVEEDOR y/o tercero deberá ser autorizado por TELEFÓNICA y deberá contar con un procedimiento de mezcla de la información y garantice su disociación. En todo caso la información utilizada para pruebas estará en todo momento protegida y controlada.
- Las vulnerabilidades técnicas identificadas en los sistemas de información, por parte del proveedor y/o externo, deberá ser notificada a la brevedad a TELEFÓNICA.

4.8. Gestión de Incidentes de Seguridad de la Información

- El PROVEEDOR y los terceros de los que se valga, de ser el caso, estarán obligados a notificar cualquier incidente de seguridad que se produzca en la prestación del servicio. Esta notificación deberá realizarse a la brevedad.
- Todos los incidentes de seguridad serán gestionados por TELEFÓNICA y podrán requerir la colaboración del PROVEEDOR y/o tercero para su resolución.

4.9. Gestión de Continuidad del Negocio

- El PROVEEDOR y los terceros de los que se valga, de ser el caso, deben desarrollar y mantener un Plan de Continuidad del Negocio (PCN) que garantice la continuidad de los servicios o productos prestados a TELEFÓNICA en concordancia con los acuerdos contractuales.

4.10. Cumplimiento de los Requerimientos Legales

- El PROVEEDOR y los terceros de los que se valga, de ser el caso, velarán por la protección de los activos de TELEFÓNICA frente a distintas amenazas, durante el tiempo y forma que se establezca en la relación contractual, en base a los requerimientos legales, reglamentarios y empresariales.

4.11. Auditoría

- A requerimiento de TELEFÓNICA, se podrán realizar auditorías de cumplimiento sobre la presente Política, con el fin de determinar el grado de cumplimiento de la misma y establecer acciones correctivas en su caso.

5. REQUERIMIENTOS DE SEGURIDAD

A continuación los requerimientos mínimos de seguridad que se deben cumplir en la implementación de equipos en las redes y plataformas de TELEFÓNICA.

5.1. Identificación y Autenticación

1. Los sistemas, plataformas y equipos de comunicaciones deberán ser compatibles con la solución de gestión de identidades (Oracle Identity Manager) y con la solución de control de accesos (Nakina), de ser necesario realizar las adecuaciones para su correcta integración.
2. 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, RADIUS o TACACS.
3. 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.

4. 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.
5. 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 Cesar Beltran Perez: cbeltran o cbeltranp en caso de duplicidad.
6. Se deberá permitir la des-habilitación y/o eliminación de usuarios (User ID).
7. 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.
8. Los sistemas, plataformas y equipos de comunicaciones no deberán mostrar información (banner) relacionada al servidor como el sistema operativo, aplicaciones o versiones usadas.
9. Las contraseñas no serán visibles en pantalla cuando se inicie el proceso de autenticación para todos los tipos de acceso permitido.
10. 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.
11. 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).
12. 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 TELEFÓNICA (típicamente 45 días).
13. 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.
14. Los sistemas, plataformas y equipos de comunicaciones deberán permitir que el usuario modifique su contraseña cuando éste lo requiera.
15. Los sistemas, plataformas y equipos de comunicaciones deberán solicitar la confirmación de la nueva contraseña para permitir el cambio de contraseña.
16. La sintaxis de las contraseñas deben contemplar los siguientes puntos:
    - Se debe validar la correcta longitud, la cual debe ser no menor a 8 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", "telefónica", "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 (¡"#$%&/).
17. Considerar registro de contraseña mediante teclados virtuales para aplicativos inmersos en la protección de datos de clientes y el secreto de las telecomunicaciones.
18. Implementar controles captcha por transacción realizada para aplicativos requieran protección de datos de clientes y el secreto de las telecomunicaciones.
19. Las contraseñas no deberán ser reusadas después de un periodo de tiempo definido por la empresa (típicamente 90 días).

5.2. Control de Accesos

1. 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).
2. 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.

3. 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.
4. Los sistemas, plataformas y equipos de comunicaciones deberán ser configurables para sólo presentar al usuario comandos autorizados.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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 ejem: uso de su.

5.3. Sistemas Operativos

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

1. El sistema operativo y aplicaciones deberán tener instaladas las últimas actualizaciones de seguridad.
2. 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.
3. 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.
4. 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).
5. Todo directorio de escritura común (/tmp) para todos los usuarios del sistema operativo deben tener sus permisos el flag de “sticky bit”.
6. Todos los archivos que contengan información de configuración de la aplicación o del sistema operativo deberán ser protegidos, mediante un esquema restrictivo de mínimos privilegios de acceso sólo para los usuarios que deben acceder a dichos archivos.
7. No se debe utilizar para el funcionamiento de las aplicaciones, implementaciones y/o interfaces, servicios (rcp, rsh, rlogin) basados en relaciones de confianza (.rhosts, hosts.equiv). La funcionalidad que estos servicios brindan, deberá remplazarse por servicios seguros con autenticación basada en claves pública y privada.
8. No se deberá utilizar ftp basado en archivo .netrc para automatizar la autenticación de dichas transferencias, en su reemplazo deberá ser utilizado el servicio sftp.
9. No deberán ser montados recursos que no sean propios de la administración del sistema operativo sobre el file system “/ ” del servidor.

5.4. Auditoria y Monitoreo de Logs

1. 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.
2. Como norma general se conservarán los Registros de Auditoría por un tiempo mínimo de 1 año y un tiempo máximo de 5 años.
3. 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 auditoria e inclusive facilitar un análisis forense (de ser el caso) después algún incidente de seguridad.

4. Intentos de autenticaciones fallidas deberán ser registrados.
5. El inicio y fin de la conexión del usuario deberán ser registradas.
6. El sistema debe registrar todas las acciones de los administradores y personal que realiza configuraciones (usuarios con máximos privilegios).
7. 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.
8. El equipo debe ser configurado para generar logs de denegación de tráfico en filtros IP o ACL's.
9. 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.
10. Un evento de seguridad será generado si hay intentos no autorizados de querer modificar el contenido de los registros de auditoría.
11. 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 serán hechos 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.
12. La solución debe soportar el configurar múltiples servidores a quienes se les va a enviar mensajes de registros de auditoria.
13. El sistema que almacena registros de auditoria debe permitir monitoreo de capacidad del sistema vía traps snmp hacia el recolector corporativo TIVOLI.
14. La solución deberá soportar NTP y de preferencia deberá usar NTPv4 (más estable y soporte 64bits en timestamps)

5.5. Comunicaciones y Redes

1. 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.
2. 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.
3. 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 trafico IPv6 debe ser soportado.
4. 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.

5. La solución deberá ser capaz de restringir el uso de brocadcast directos.
6. La configuración "ignore gratuitous" ARP deberá ser soportado.
7. Los elementos de red deberán ser configurados para no permitir enrutamiento de tráfico entre sus diferentes interfaces.
8. Los elementos de red deberán ser capaces de evitar pasar paquetes IP peligrosos o fuente de redirección de enrutamiento.
9. La solución debe ser capaz de deshabilitar envío de mensaje "ICMP unreachable" cuando un paquete es denegado por lista de acceso.
10. Los sistemas TCP con acceso a servicios de internet deberán soportar un mecanismo de protección contra SYN Flood attacks.
11. 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.)
12. Si la solución soporta interfaces Wifi deberá soportar encriptación WPA y WPA2.
13. 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
14. 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 físico 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.

5.6. 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:

1. 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.
2. 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.
3. 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.
4. 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).
5. 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:

i. Componentes frontales: Invocación de servicios de negocio de una aplicación desde otra mediante un componente, usado para transacciones distribuidas.
ii. 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.

6. La solución debe ser capaz de deshabilitar servicios no requeridos.
7. 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.
8. La solución deberá permitir monitoreo en tiempo real de parámetros de operación y capacidad.
9. 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.
10. 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.
11. 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, deshabilitandola y manteniendo la configuración previa.
12. La solución deberá tener mecanismos para detectar y prevenir la instalación o ejecución de código malicioso (virus, troyanos, gusanos, etc).
13. 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.
14. El proveedor deberá proporcionar una estrategia de respaldo de la información y apoyar a Telefónica en su implementación. Esta estrategia deberá estar alineada con los estándares y políticas existentes.
15. La solución deberá proporcionar procesos de respaldo y de paso a histórico.
16. La solución deberá proporcionar los procedimientos para la recuperación ante fallos habituales.
17. Las acciones a llevar a cabo en caso de fallo (procedimientos de gestión de errores) deberán estar extensamente documentados.

5.7. Bases De Datos

1. 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.
2. En Oracle sobre sistemas operativos UNIX, no se utilizarán usuarios de UNIX con autenticación externa para validarse en la base de datos.
3. 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 Política de Contraseñas 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.

4. La aplicación debe conectarse a la base con un esquema de mínimos privilegios que debe ser validado y documentado.
5. La aplicación deberá proveer la trazabilidad mínima que garantice un adecuado seguimiento de las acciones desarrolladas sobre los objetos que utilice.
6. 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.
7. 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.
8. 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.
9. 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.
10. Los usuarios que cumplan con un rol dueño de esquema de una aplicación, deberán tener un entorno restringido adecuado a sus funciones (privilegios).
11. 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).
12. No deberán ser montados recursos de la base de datos sobre el file system de root “/” del sistema operativo.
13. 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.
14. La solución preferentemente no deberá trabajar en sus puertos por defecto.
15. La solución deberá tener un plan de actualizaciones de seguridad alineados con los paquetes que publica el fabricante.
16. La solución deberá tener la capacidad de encriptar tablas acordes con la clasificación de la seguridad de la información corporativa.
17. La solución deberá tener la capacidad de bloquear y/o eliminar usuarios por defecto no usados.
18. La solución deberá proteger al listener cambiando el puerto por defecto y/o asignando contraseña.
19. Definir y documentar las características y Ubicación de Tabla de Auditoría AUD$ para el caso de Oracle.
20. Limitar Excesivos privilegios de objetos públicos (PUBLIC).

5.8. Integración con control de accesos (ACNE)

1. Para SSO de dispositivos (CLI) Integración
   - El dispositivo debe soportar conectividad IP.
   - El dispositivo debe soportar versiones estándar de protocolos de SSH, FTP, SFTP (para uso del telnet se debe tener la autorización de la dirección).
   - 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, Telnet, SFTP.
   - La documentación indicará si las interfaces no comparten la misma lista de credenciales. Por ejemplo diferentes credenciales necesarias para Telnet y SSH.
2. 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.

3. 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.

5.9. IPV6

1. La solución deberá tener filtro de capacidad de enrutamiento IPv6
2. La solución deberá soportar ACL para IPv6 así como IPv4
3. La solución deberá soportar y administrar los protocolos SNMP, NTP, SSH, etc. para IPv6
4. La solución deberá permitir/deshabilitar servicios ejecutándose en IPv6.
5. 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.
6. La solución deberá denegar trafico IPv6 si no hay servicio IPv6 disponible.
7. El proveedor deberá describir cualquier medida de seguridad propuesta para IPv6 y protección DoS así mismo deberá identificar los diferentes registros para actividades maliciosas.