

Anexo

Especificación de Requerimientos de Seguridad en los contratos

Versión 5.00

Seguridad de la Información
Telefónica Argentina S.A.

Realizado por	Revisado por	Aprobado por
<i>Diego Arias / Planificación y Tecnología de IT</i>	<i>Malena Digon / Transformación de Seguridad</i>	<i>Paulo Escaño / Jefe Transformación de Seguridad</i>
<i>18/01/2016</i>	<i>14/05/2018</i>	<i>14/05/2018</i>

INDICE

1	CONTROL DE CAMBIOS.....	2
1.1	Control de cambios del Documento:	2
1.2	Control de cambios del template:	2
2	OBJETIVO.....	3
3	ALCANCE.....	3
4	CONSIDERACIONES ESPECIALES.....	3
5	ABREVIATURAS Y DEFINICIONES.....	3
6	REFERENCIAS.....	4
7	ROLES Y RESPONSABILIDADES	4
8	REQUERIMIENTOS	4
8.1	Marco Regulatorio.....	4
8.2	Acceso Lógico y Gestión de Cuentas.....	4
8.3	Trazabilidad y Auditoria	6
8.4	Gestión de la Configuración	7
8.5	Arquitectura de Seguridad.....	8
8.6	Cloud	9
8.7	Mobile	9
8.8	Big Data	9
8.9	Respaldo y recuperación.....	10
8.10	Integración con la Red de la compañía	11

1 CONTROL DE CAMBIOS

1.1 Control de cambios del Documento:

Versión	Fecha entrada en vigencia	Fecha fin de vigencia	Cambios realizados en versión	Responsable de definición de cambios
01.00	15/04/2013	19/02/2015	Versión Inicial	Nestor Perelman
02.00	19/02/2015	22/01/2016	Actualización de versión de NCSI y se suprimen los epígrafes que mencionan a la NCSI por el detalle de los requisitos	Nestor Perelman
03.00	22/01/2016	20/04/2018	Agregado de requisitos de servicios Cloud y Mobile	Diego Arias
04.00	20/04/2018	14/05/2018	Revisión y corrección completa del documento.	Malena Digon
05.00	14/05/2018	-	Se modificó texto bajo los títulos de: "Arquitectura de Seguridad" y "Auditoria y Trazabilidad"	Malena Digon

1.2 Control de cambios del template:

Versión	Fecha entrada en vigencia	Fecha fin de vigencia	Cambios realizados en versión	Responsable de definición de cambios
01.00	15/07/2013	21/11/2014	Versión Inicial	Paula Trotta, Procesos y Calidad TI
01.01	21/11/2014	-	Agregado de tabla de roles y responsabilidades en Inciso 6. Agregado del control de cambios del template	Gabriela Moroz, Procesos y Calidad TI

2 OBJETIVO

El objetivo de este documento es realizar una descripción general de los requerimientos de seguridad que deberán ser tenidos en cuenta por el oferente al ser contratado el servicio y/o comprado, y que serán de cumplimiento obligatorio.

Dichos requerimientos se encuentran alineados con el Marco Normativo Corporativo de Seguridad de la Información de Telefónica Global. Siendo el cumplimiento de este marco obligatorio para todas las operadoras del grupo.

3 ALCANCE

La definición del alcance y forma de cumplimiento de los requerimientos aquí indicados, se realizará mediante el criterio que Telefónica considere, luego del análisis de riesgos correspondiente que definirá los niveles de acuerdo de servicio (SLA) indicados en estos requerimientos.

4 CONSIDERACIONES ESPECIALES

Telefónica se reserva el derecho de realizar auditorías y revisiones a los sistemas involucrados en el presente contrato, en los intervalos que considere.

Todos los desvíos a los requerimientos de este anexo se deberán corregir en un plazo definido (SLA), sin costo adicional para Telefónica y todo lo no consultado por fuera de este documento se define que será cumplido por el proveedor.

El contenido expresado en este documento debe ser considerado como confidencial entre las partes, por lo cual no debe ser divulgado a terceros y debe ser mantenido bajo la más estricta confidencialidad.

5 ABREVIATURAS Y DEFINICIONES

- **SLA:** Service Level Agreement. Acuerdo de nivel de servicio
- **SOX:** Ley Sarbanes-Oxley
- **PCI:** Payment Card Industry Data Security Standard. Estándar de Seguridad de Datos para la Industria de Tarjeta de pagos.
- **LDAPS:** Protocol ligero de acceso a directorios (LDAP) sobre SSL.

- **SSL:** Secure Socket Layer. Capa de conexión segura

6 REFERENCIAS

Normativa Global de Seguridad

https://intranet.telefonica.com/docs/normativa_grupo_telefonica/20170510_Normativa_Global_Seguridad.pdf

7 ROLES Y RESPONSABILIDADES

Rol	Responsabilidades	Responsable
Seguridad de la Información	Realizar análisis de riesgo y definir SLA en caso que se requiera	Marcos Jaimovich - Gerente Seguridad de la Información
Oferente	Cumplir los requerimientos definidos en este anexo en su producto o servicio.	<i>Oferente</i>

8 REQUERIMIENTOS

8.1 Marco Regulatorio

- 1) Deberá cumplir con los requerimientos definidos en la Normativa Corporativa de Seguridad de la Información de Telefónica y los procedimientos derivados de ella.
- 2) Deberá cumplir con los requerimientos normativos, legales y regulatorios en función al tipo de información y/o servicios que estén alcanzados por el sistema informático, sea por ejemplo el caso:
 - a) Si maneja información financiera deberá cumplir con la Ley de SOX.
 - b) Si maneja información de tarjetas de crédito o débito deberá ser PCI-DSS o PA.
 - c) Si maneja información personal de empleados y/o clientes, deberá cumplir con la Ley de Protección de Datos Personales.

8.2 Acceso Lógico y Gestión de Cuentas

- 1) El proceso de autenticación y autorización de la solución ofertada debe ser efectuado a través de la integración con los sistemas corporativos (IBM Access Manager) tanto para usuarios internos o clientes, siendo los siguientes métodos disponibles:
 - a) Basic Authentication a través de WebSeal: Reverse Gateway de la solución de Access Manager, brinda una cara de seguridad perimetral a todas las aplicaciones protegidas por Access Manager.
 - b) Web Services para LogIn: En caso que una aplicación necesite un formulario de autenticación diferente al estándar definido, se deberá tratar especialmente aplicando APIs de Access Manager para autenticar y autorizar al usuario usando páginas propias de la aplicación.
 - c) Identity Provider (IDP) mediante Protocolos SAML 2.0/OAuth 2.0 (obligatorio para todas aquellas aplicaciones hospedadas fuera de la compañía o de carácter cloud).
- 2) La aplicación no deberá permitir el acceso simultáneo de un mismo usuario.
- 3) La solución debe cerrar la sesión inactiva del colaborador después de un período parametrizable. De ser requerido por Seguridad de la Información, esta funcionalidad deberá ser parametrizable por tipos y atributos de usuarios, perfiles, módulos de aplicación y/o ambiente en los que se puede acceder a la aplicación.
- 4) La solución debe utilizar el mecanismo de control de acceso basado en perfiles (RBAC): Usuarios > Perfiles > Permisos. Los perfiles de acceso deben cumplir los siguientes criterios:
 - a) La asignación deberá ser posible por medio de la membresía/asignación de grupos LDAP perteneciente a la solución IBM Access Manager o por medio de APIs de aprovisionamiento que resuelvan completamente la asignación.
 - b) Los usuarios deben ver solo lo requerido y necesario por su perfil y no deben ver campos o menús que no puedan ser accedidos por sus niveles de privilegios asignados.
 - c) Los roles deben ser creados bajo la condición de solo poder ver y/o gestionar lo requerido para el puesto.
 - d) Todas las funcionalidades de la aplicación deben ser controladas por perfiles. No deben existir funcionalidades que exijan la configuración de atributos individuales por usuarios.
 - e) El perfil de administración no deberá contener la funcionalidad de ABM de Usuarios y Perfiles. Este permiso debe estar en un perfil separado
- 5) Deberá contar con un módulo de ABM de usuarios y perfiles, con la documentación de los procedimientos adecuados. Además del módulo correspondiente, estas mismas funcionalidades deben estar disponibles para ser consumidas como Web Services o con sus correspondientes APIs para poder invocarlas mediante algún desarrollo o interfaz.
- 6) Deberá permitir obtener reportes de los usuarios, con todos sus campos de información, y perfiles asignados. Además de los perfiles activos en la aplicación.
- 7) Deberá permitir el bloqueo y reactivación de cuentas.
- 8) Deberá permitir la configuración de políticas de usuarios y contraseña, para cuentas no personalizadas incluyendo:
 - a) Identificación del tipo de cuenta y su responsable
 - b) Bloqueo por inactividad

- c) Complejidad de contraseñas
 - d) Historial de contraseñas
 - e) Tiempo mínimo y máximo de vida de las contraseñas
 - f) Bloqueo por accesos incorrectos.
- 9) En caso de prestación de servicios por parte del proveedor, que requiera el acceso a los sistemas de Telefónica, se deberá cumplir con lo siguiente:
- a) El proveedor deberá designar un responsable gerencial y un responsable operativo que informará a Telefónica, por las vías formales definidas, los cambios de nómina que impacten en la asignación de privilegios en los sistemas de Telefónica, según el SLA definido.
 - b) El proveedor deberá segregar sus roles según los criterios y matrices de incompatibilidad de Telefónica. Por ejemplo: desarrollo, certificación, administración y soporte.
 - c) El proveedor se hará responsable por todas las acciones realizadas con los usuarios asociados a su contrato.
 - d) Todos los usuarios del proveedor deberán ser personalizados. No se permitirá el uso de usuarios genéricos.
 - e) El acceso remoto para la gestión de los sistemas deberá alinearse con los procedimientos definidos por Telefónica.

8.3 Trazabilidad y Auditoria

- 1) La solución debe proporcionar información que permita la investigación de los registros de auditoría (trazabilidad fin-a-fin) de los procesos. La trazabilidad comprende desde los elementos más altos de la aplicación (Módulos), intermediarios (Actividades/Tareas) y bajos (cambios en campos), asociando siempre el detalle de fecha/hora, IP, grupo e identificación de usuario. La seguridad de acceso a dicho módulo, así como la facilidad operativa debe ser análoga a la proporcionada para funciones disponibles para el usuario final.
- 2) Mantener el historial de operaciones por usuario del sistema. La herramienta debe disponibilizar registro y pantallas de búsquedas que permitan rastrear operaciones realizadas por los usuarios.
- 3) Además de registrar las operaciones de los usuarios dentro del sistema, deberá registrar los siguientes eventos, como mínimo, relacionados al acceso a la aplicación y gestión de cuentas:
 - a) Intentos de accesos no válidos.
 - b) Inicio de sesión y cierre de sesión de usuarios.
 - c) Eventos del sistema.
 - d) Gestión de cuentas de usuario.
 - e) Cambios en las configuraciones de la aplicación.
 - f) Uso de privilegios de usuarios.
 - g) Acciones administrativas
 - h) Eventos relacionados con la seguridad de la aplicación
 - i) Errores de conexiones SSL

- j) Fallas del sistema/aplicación
 - k) Cambios en la activación/desactivación de auditoria de logs
 - l) Mensajes de errores generados por la aplicación (sin incluir información sensible).
- 4) En ningún momento los registros de auditoría (log) creados por la aplicación deberán contener datos considerados confidenciales.
 - 5) Los archivos de registro deben almacenarse de forma segura y tener restricción de acceso, principalmente en los casos de permiso de cambio y eliminación. El acceso y la lectura de los archivos de registro deben restringirse a los usuarios autorizados.
 - 6) El tiempo de retención de los registros de auditoria serán definidos por el área de Seguridad de la Información.
 - 7) La solución debe generar los registros y almacenarlos en una tabla (o múltiples tablas) de base de datos de forma que la solución de SIEM (Security Information and Event Manager) de Telefónica pueda acceder a ellas a través de consultas SQL estándar.
 - 8) Los registros de auditoría de los diferentes componentes de la solución deberán ser inequívocamente relacionados para asegurar la trazabilidad de las acciones realizadas.
 - 9) Todos los componentes de la solución deberán estar sincronizados con el reloj definido por Telefónica.

8.4 Gestión de la Configuración

- 1) Se deberá cumplir, para cada componente del sistema informático, con los requerimientos de seguridad en la configuración de los mismos, definido por Telefónica en los procedimientos de seguridad correspondientes.
- 2) Toda la infraestructura involucrada deberá contar con las plantillas de seguridad aplicadas y actualizadas tanto como para Sistemas Operativos y Base de Datos.
- 3) Deberá permitir la integración de los sistemas de control de configuración de Telefónica.
- 4) Deberá, en caso de ambientes que Telefónica defina, implementar la solución homologada de Antivirus de Telefónica.
- 5) Deberán los equipos que den soporte a la aplicación estar actualizados en su última versión, tanto de sistema operativo como de parches de seguridad.
- 6) Deberá integrarse con los requerimientos y políticas de respaldo y recuperación de Telefónica, definido en el documento en referencia, y detalladas en procedimientos particulares.
- 7) Se deberá cumplir con un SLA definido por Telefónica, en función de la criticidad de la información y/o los servicios afectados, para la disponibilidad de parches propios de la solución u homologación de parches de terceros
- 8) Ningún componente y/o servicio de la solución debe requerir privilegios administrativos y/o de superusuario para su ejecución

8.5 Arquitectura de Seguridad

- 1) Se deberán separar los ambientes de Desarrollo, Certificación y Producción.
- 2) Se deberá asegurar que las vulnerabilidades que se encuentren en los elementos del sistema sean debidamente solucionadas dentro de la ventana de riesgo definida por Telefónica, en función de la criticidad de la información o los servicios asociados.
- 3) Deberá permitir la segregación de los componentes de la solución según el análisis de riesgos que realizará Telefónica, y en el que definirá el nivel de seguridad requerido para cada uno de ellos.
- 4) Toda interface web, sea aplicación o web service, deberá cumplir con los requerimientos definidos en OWASP (Comunidad Abierta sobre Seguridad en Aplicaciones), como buenas prácticas para el desarrollo seguro.
- 5) Se deberá asegurar el correcto procesamiento de la información en las aplicaciones, cumpliendo con los siguientes requerimientos:
 - a) Validación de datos de entrada: las entradas de datos en las aplicaciones deben ser validados previo a su procesamiento para asegurar que son correctos y apropiados.
 - b) Control de procesamiento interno: Se deben incorporar las verificaciones de validación a las aplicaciones para detectar cualquier caso de corrupción de la información a través del procesamiento de errores o actos deliberados.
 - c) Integridad del mensaje: Se deben identificar los requerimientos para asegurar la autenticidad y para proteger la integridad del mensaje de las aplicaciones, y se deben identificar e implementar controles apropiados.
 - d) Validación de datos de salida: Se debe validar la salida de datos de una aplicación para garantizar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias.
- 6) El sistema deberá proveer mecanismos para la protección de la información crítica que maneje en todas las etapas de su ciclo de vida (generación, tratamiento, transporte, almacenamiento y destrucción).
- 7) Deberá soportar protocolos de acceso y transporte de información seguros, y no se utilizarán protocolos que no permitan el cifrado o que presenten debilidades de seguridad.
- 8) Deberá proveer autenticación en las API o WS, si los hubiere.
- 9) Toda API o WS debe interactuar con elementos externos al producto pasando siempre, y sin excepciones a través del APIGW corporativo.
- 10) Todos los componentes usados como soporte para brindar funcionalidad a la aplicación (ej.: librerías de terceros) deben estar actualizadas a su última versión. De lanzarse una nueva versión el proveedor deberá confirmar la compatibilidad de la misma con la aplicación.
- 11) Deberá permitir segregar la interfaz de gestión de la de servicio y aplicar listas de control de acceso para restringir el origen de las conexiones, únicamente a los orígenes definidos por Telefónica como válidos.

- 12) Todo el tráfico de la solución debe ser protegido por HTTPS/TLS utilizando certificados digitales, siendo posible el uso de certificados generados por CA (Certificate Authority) internos o externos según el origen del acceso.

8.6 Cloud

- 1) Se debe identificar la legislación aplicable al servicio en función de los países desde los que se usa el servicio y desde los que opera el proveedor de modo que el servicio y/o producto contratado cumpla con dichos requisitos, especialmente referentes a:
 - a) La legislación sobre privacidad protección de datos de carácter personal.
 - b) La legislación sobre de protección y retención de registros de auditoría.
 - c) La legislación sobre criptografía.
- 2) El proveedor debe cumplir con los controles del estándar internacional ISO 27002 en el ámbito del servicio (aunque no sea necesaria la certificación) y debe poseer y mantener en el tiempo una certificación de seguridad como ISO 27001 o SAS70 tipo II (SSAE 16) o similar.
- 3) Las sesiones de usuarios clientes de dicho aplicativo se deben realizar por medio de canales seguros.

8.7 Mobile

- 1) El proveedor debe cumplir con los requisitos establecidos por el estándar OWASP (Comunidad Abierta sobre Seguridad en Aplicaciones) y el estándar CAPEC (Clasificación de Patrones de Ataque Común) para los productos ofrecidos.
- 2) No se debe almacenar información sensible en dispositivos móviles.
- 3) Si es necesario almacenar datos en el dispositivo móvil, por ejemplo, en caché, estos datos deben cifrarse con protocolos seguros
- 4) No se deben almacenar claves de cifrado en dispositivos móviles.
- 5) La aplicación no deberá requerir más permisos sobre las distintas funcionalidades del dispositivo móvil de los únicamente necesarios.

8.8 Big Data

- 1) Ante la necesidad de integración contra el entorno de Big data corporativo, el proveedor deberá cumplir con los estándares de la suite de Hortonworks, HDP (Hortonworks Data Platform) en sus

versiones 2.x y futuras versiones. Contemplando además la integración, administración, autenticación, autorización y protección de datos de auditoría.

- 2) Deberá cumplir con los estándares de anonimización y cifrado, tanto de la suite Hortonworks HDP en sus versiones 2.x como sus futuras versiones

8.9 Respaldo y recuperación

- 1) Deberá definir y realizar resguardos de información en base al riesgo asociado al proyecto y lo que defina el Analista de Seguridad de la Información asignado. Se deberán tener en cuenta los siguientes puntos:
 - a) Los responsables de realizar las copias de respaldo y posterior custodia.
 - b) Periodicidad de las copias de respaldo.
 - c) Número de copias.
 - d) Tipo de respaldo (completa o diferencial/incremental).
 - e) Tiempos máximos de almacenamiento (fecha de expiración) y si es necesario eliminar la información una vez alcanzada la fecha de expiración (así como el tipo procedimiento de destrucción exigido)
 - f) Tiempos mínimos aceptables para recuperar de la información.
- 2) Se deberá cifrar la información respaldada en función de los siguientes aspectos:
 - a) La naturaleza de la información (financiera, contratos con clientes, registros de accesos, sistemas operativos, etc.).
 - b) Los requisitos de disponibilidad determinados por el Propietario de la información de acuerdo a las necesidades del negocio.
 - c) Nivel de clasificación de la información.
 - d) Los requisitos legales aplicables en cada país.
 - e) Políticas internas de retención de información y datos.
 - f) Los niveles de servicio acordados.
 - g) Riesgo tecnológico implícito.
 - h) Los planes de continuidad de negocio.
- 3) El proveedor debe generar los procedimientos de recuperación asociados.
- 4) Las copias de respaldo serán rotuladas e inventariadas, considerando la clasificación de la información.
- 5) Las claves de cifrado y programas asociados deberán guardarse de forma separada, de manera que se pueda recuperar la información a partir de la información cifrada en caso de ser necesario.
- 6) Las copias de respaldo se realizarán de manera que se pueda recuperar, de forma separada e independiente, el sistema y la información que procesa.

- 7) Las copias de respaldo realizadas se verificarán periódicamente y de forma rotativa de acuerdo a un plan de pruebas definido, utilizando una herramienta de verificación o restaurando parte del conjunto para garantizar que las copias estarán disponibles cuando sean necesitadas.
- 8) En los casos en los que sea posible, se debe automatizar el procedimiento de realización de copias de respaldo mediante programación periódica de las mismas.
- 9) En el caso de los datos sean de carácter personal sensibles, se deberá conservar una copia de respaldo de la información y copia de los procedimientos de recuperación en un lugar diferente de aquél en que se encuentren los sistemas que tratan la información, que deberá cumplir en todo caso con las medidas de seguridad de la ubicación original, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.
- 10) Se verificará periódicamente la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

8.10 Integración con la Red de la compañía

- 1) En base a los niveles de riesgo, el proveedor deberá tener en cuenta que se segregaran en varios segmentos lógicos y/o físicos la red donde resida la aplicación. Estos segmentos de red se aislarán mediante dispositivos, que controlarán el acceso y el tráfico entre los segmentos de acuerdo a los criterios y políticas definidas. La solución debe soportar la segregación en capas separando las zonas de presentación (DMZ) de las zonas de aplicación con el mínimo de apertura de puertos de comunicación en los firewalls entre las zonas. El proveedor debe cumplir con una mínima segregación de redes de gestión, tráfico y servicios internos o expuestos.
- 2) El proveedor deberá definir y cumplir con los siguientes requerimientos para conectarse con la compañía en base a lo definido por la empresa:
 - a) Las personas responsables de autorizar las solicitudes (deberá estar involucrado el Analista de Seguridad de la Información).
 - b) La forma de acceso de los usuarios a los segmentos de red, así como los posibles mecanismos de identificación, autenticación, control de accesos y registro de acceso de los mismos.
- 3) El proveedor deberá considerar los siguientes puntos que serán requeridos por Telefónica:
 - a) Todo está prohibido a menos que esté expresamente permitido.
 - b) Evitar que los ataques que se produzcan desde el interior de un segmento de red afecten al resto (propagación de gusanos, etc.).
 - c) Evitar los ataques de denegación de servicio en la medida de lo posible.
 - d) Evitar la suplantación de direcciones origen.
 - e) Permitir la gestión remota sólo desde ciertas direcciones autorizadas.
 - f) Registrar los eventos de seguridad (logs) o garantizar los requisitos del negocio.
 - g) Definir los diferentes niveles de riesgo de los segmentos de red de la aplicación.
- 4) El proveedor deberá utilizar la VPN de Proveedores para acceso a recursos de Telefónica. La autenticación de la VPN deberá ser conforma los estándares establecidos por compañía.

- 5) No se permitirá la conexión a redes externas directas en sistemas que estén conectados a la red interna.
- 6) Los pasos para solicitar, autorizar o anular la interconexión de la red interna de la empresa con redes externas, se indicarán en un procedimiento definido en el cual se identificará el responsable de otorgar las autorizaciones.