CONTENIDO

HOJA DE CONTROL DE DOCUMENTOS

LISTA DE CAMBIOS

Versión	Fecha	Autor	DESCRIPCIÓN
1	15/03/2010	Planificación Ingeniería y Control	Unificación de requerimientos de Seguridad de la Información y Seguridad Física
2	13/12/2011	Seguridad de la Información	Revisión de alineamiento a Normativa Corporativa de Seguridad de la Información Versión 3
3	01/06/2015	Seguridad de la Información	Actualización del documento, inclusión y exclusión de requisitos, revisión y alineación a la Normativa Corporativa de Seguridad de la Información Versión 4
4	04/08/2016	Seguridad de la Información	Actualización del documento, inclusión en al apartado de Autenticación, la designación de un responsable para envío de contraseñas temporales.
5	12/01/2021	Cristhian Angueta	Actualización de responsables y codificación del documento a PR.SI.SD.04.01
6	21/03/2022	Jose Javier Escobar	Actualización del documento inclusión de requisitos.

FLUJO DE APROBACIÓN

Elaborado	Revisado	Aprobado
Jose Javier Escobar (Especialista Seguridad de la Información)	Blanca Egas (Gerente Legal) Ramiro Pérez Jefe de Seguridad Digital Angel Molina Especialista de Procesos Cristian Moreno (Jefe de Compras)	Dean Torres (Gerente de Seguridad) Cristian Moreno (Jefe de Compras) German Saona (Gerente Compras) Diego Calderón (Director B2B) Gerardo Suárez (Director B2C)

	Andrés Reinoso (Gerente Atención canal online y Telefónico) _____ Carlos Almeida. (Gerente Micro y Soho Ecuador Micro y Soho) _____ Fernando Castellanos. (Gerente Ventas y Canal Presencial) _____ Fernando Cabrera. (Gerente Atención B2B) _____ Hugo Vidal (Gerente Ingeniería y Procesos Ecuador Soporte TI) _____ Richarth Laguna (Jefe Infraestructura TI) _____ Juan Andres Obregon (Gerente Gestion de Red y Data Centers Ecuador OYM Gestion de Red) _____	Guillermo Herrera. (Gerente OYM Red) _____ Soraya Salazar (Gerente TI) _____

OBJETO

Formalizar la inclusión en los contratos con Proveedores y Distribuidores Autorizados los requerimientos de Seguridad de la Información especificados en la Norma de Seguridad Corporativa del Grupo Telefónica.

1. DETALLE DE REQUISITOS

Ámbito/ Actividad	Requerimientos
General	• El proveedor y distribuidor se compromete a definir un responsable en materia de seguridad, quien será el interlocutor para estos temas con OTECEL y el encargado de hacer cumplir los requisitos de seguridad del Contrato. • El proveedor y distribuidor se compromete a informar los cambios de personal que presta servicios para OTECEL. La notificación se realizará formalmente mediante correo electrónico al administrador del contrato definido por OTECEL, dentro de 24 horas calendario de realizado el suceso. • El proveedor y distribuidor se compromete a mantener actualizada los usuarios a su cargo, gestionar y confirmar la eliminación de los accesos del personal que sea dado de baja, la gestión deberá ser realizada dentro de las 24 horas de haber sucedido la salida del personal. • Es responsabilidad de cada Proveedor y distribuidor, hacer negocios con OTECEL de una manera legal, ética cumpliendo los requisitos de seguridad establecidos. • Los Recursos de Información de OTECEL deben ser usados únicamente para los fines aprobados por OTECEL. • Los Recursos de Información de OTECEL deben ser protegidos contra el uso no autorizado, robo, uso inadecuado, modificación accidental o no autorizada, revelación, transferencia o destrucción. • La confiabilidad, disponibilidad e integridad de los recursos de Información de OTECEL y las actividades de procesamiento de información deben ser protegidas. • Cada Proveedor y distribuidor, y cada Empleado del Proveedor y Distribuidor debe permitir a personal de OTECEL autorizado a realizar inspecciones de seguridad periódicas en sitio, además se deberá solicitar reportes de auditoria extraordinarios del equipo de computación utilizado en el manejo de negocios o información de OTECEL; ya sea este equipo propiedad de OTECEL, arrendado o controlado por el Proveedor y distribuidor, r o Empleados del Proveedor y/o Distribuidor. • Los equipos deben ser proporcionados y autorizados por las áreas de TI de cada proveedor, distribuidor y/o cumplimiento con los lineamientos de seguridad (No se autoriza equipos personales) Los equipos tanto de proveedores y distribuidores deben ser declarados a OTECEL. • Procedimientos que presentar por el proveedor o distribuidor: – Procedimiento de devolución o destrucción de la información a la

Ámbito/ Actividad	Requerimientos
	finalización del acuerdo. – Procedimiento de concienciación y formación en lo referente a normas de seguridad de la información. – Procedimiento de gestión de cambios del proveedor o distribuidor. – Procedimiento de notificación gestión y escalamiento de los incidentes de seguridad que detalle las plataformas: o Accesos no autorizados a la información, o Falta de integridad, o Indisponibilidad, o Fuga de Información. o Uso inapropiado de las plataformas de Otecel etc. – Procedimiento de escalado en la resolución de problemas – Procedimiento de actualización de antivirus o antimalware. – Procedimiento de gestión de parches y actualizaciones de seguridad. – Procedimiento de Hardening de Workstation que contemple el bloqueo de almacenamiento de información en USB, discos externos, asignación privilegios mínimos de acceso en los equipos de los ejecutivos. Todos los usuarios deberán tener permisos de acuerdo con su rol y perfil. (No usuarios de administradores). El dispositivo de cómputo Workstation/ Laptop debe contar con dos particiones, la partición C: únicamente de sistema, y la partición del disco dos (D:) para guardar la información. – La unidad de datos disco (D:) debe estar cifrada – Plan de Continuidad del negocio que incluya: o Planes de emergencia o Planes de contingencia o Recuperación de desastres o Plan de pruebas
Expectativas de Privacidad	• Los Recursos de Información de OTECEL, incluidos, pero no limitados a, redes de voz, correo electrónico, y mensajes de voz son propiedad de OTECEL y, como tales, deben ser usados únicamente con el propósito de negocios de OTECEL. • Por ello OTECEL puede solicitar monitorear ocasionalmente por causa justificada, y/o revisar el uso de sus Recursos de Información asignados al proyecto específico del contrato (servidores, o equipos). • La información clasificada como personal cumplirá con lineamientos establecidos en las leyes vigentes.
Informe de Infracciones	• En caso de que cualquier empleado del Proveedor y distribuidor, prestando servicios para OTECEL, sea testigo de una infracción contra los estándares y regulaciones, leyes locales o permisos de licencias, debe reportar inmediatamente al área de Seguridad de la Información de OTECEL. • No se tomarán medidas independientes para corregir un problema de seguridad a menos que la falta de una respuesta inmediata resulte en daños irreparables para OTECEL. Si se toma una medida para prevenir daños irreparables, reporte la medida junto con un informe del problema al Departamento de Seguridad Digital lo más pronto posible.
Virus y Código	

Ámbito/ Actividad	Requerimientos
Dañino de Computadores	• Todo equipo del Proveedor y distribuidor, conectado a la red de OTECEL debe mantenerse libre de virus y otros códigos dañinos de computadores, debiendo los usuarios de estos sistemas adoptar las medidas necesarias para el efecto. • Todo equipo del Proveedor y distribuidor, conectado a la red de OTECEL, deberá usar un software para protección de virus debidamente licenciado. • El proveedor, distribuidor deberá implementar soluciones de antivirus o antimalware de seguridad con características de EPP + EDR y posea gestión y monitoreo de las Estaciones de trabajo, con control de aplicaciones
Restricciones del Uso de Software	• Todo software instalado en el equipo del proveedor y distribuidor que se conecte a la red de OTECEL, deberá ser previamente autorizado por OTECEL. • Software personal de los Empleados del Proveedor y distribuidor, no debe ser instalado ni utilizado en los computadores que se conecten o usen recurso de la red de OTECEL. • Se prohíbe la instalación y uso de software gratuito en equipos empleados por el proveedor y distribuidor para dar el servicio, excepto ante autorizaciones explicitas dadas por OTECEL. • La licencia y derechos de autor y restricciones de software siempre deben ser acatados. • Medidas preventivas: Ej. gabinetes con llave: Deben ser usados para prevenir el uso no autorizado, copia o robo de hardware y software.
Gestión de Cambios	• Todo cambio relacionado al ambiente de Producción o pruebas en las plataformas instaladas, accedidas y manejadas local o remotamente, deben regirse al proceso de gestión de cambios de OTECEL • El Proveedor y distribuidor, que realizan cambios a sistemas, software, hardware; llámese cambios Emergentes, Funcionales, Técnicos y Express que afecten al software, hardware, configuraciones, arquitectura, componentes etc.; relacionados al servicio brindado, deben cumplir con todos los requisitos del proceso de Gestión de Cambios que se lleva en OTECEL
Gestión de Incidentes	• El Proveedor y distribuidor, debe contar con una herramienta, mecanismo o procedimiento para gestionar incidentes que ocurriesen en sus plataformas, sistemas o servicios tecnológicos que esté brindando a OTECEL.S. A, adicional el proveedor y distribuidor deberá evaluar soluciones de monitoreo y correlación de logs, para detección de comportamiento anómalo de usuarios y que en la medida sea integrable con las plataformas de OTECEL S.A para fortalecer la trazabilidad de los incidentes. • El Proveedor y distribuidor debe tener la capacidad de entregar en un tiempo mutuamente acordado entre las partes informes detalladas de los incidentes gestionados en los que debe constar tiempos de respuesta, penalidades, cumplimiento de Acuerdo de Nivel de Servicio (ANS). • El Proveedor y distribuidor, debe acogerse a los ANS para la gestión de incidentes especificados en el contrato.
Desarrollo de Software	• El Código de computación creado, modificado, o de otra manera provisto para OTECEL debe cumplir con los siguientes requisitos:

Ámbito/ Actividad	Requerimientos
	○ Debe ser documentado de acuerdo a su función y requerimientos de uso, para OTECEL, ○ No debe contener ningún código de acceso maestro (identificación, contraseña, puerta de atrape, caballo de Troya, puerta trasera, etc.) al sistema, y no debe contener ningún virus u otro código dañino, accesorio o fecha de expiración. ○ No debe degradar la seguridad al interferir o modificar las funciones normales del sistema operativo en el que residirá el software. • El Proveedor y distribuidor que realizan el desarrollo del sistema o de software bajo la dirección de OTECEL, deben cumplir con todos los requisitos de desarrollo y seguridad de las Políticas de Seguridad Corporativa de OTECEL. • Por temas de auditoría y control, es requisito que en los sistemas o soluciones desarrolladas o accedidas por OTECEL, el Proveedor y distribuidor, cuente con módulos de gestión para administración de cuentas de usuarios, además deberán contar con un control de auditoria para chequeos permanente. • El Proveedor y distribuidor, que realizan el desarrollo del sistema o de software bajo la dirección de OTECEL, y el Proveedor y distribuidor, que presten sus servicios como parte de un acuerdo de consultoría externa, deberán seguir los requisitos de desarrollo de software en las Políticas de Seguridad Corporativa de OTECEL y en las Políticas de otras compañías afiliadas. El Proveedor y distribuidor, deben seguir las Políticas de Desarrollo de Software establecidas en los Requerimientos de Seguridad para Acuerdos Contractuales. • No se deberá modificar el sistema operativo, código de aplicaciones u otro software que pueda impactar negativamente la actual o futura seguridad del ambiente del sistema computarizado. • Se debe tomar en cuenta que al requerir la implementación de un Web Services, se debe considerar las siguientes recomendaciones de seguridad: ○ En lo posible el Web Services debe correr solo en el servidor y no con otra aplicación, que este no tenga una lectura accesible del lenguaje script, y que no soporte login remoto
Computadores Portátiles	• Computadores portátiles del Proveedor y distribuidor, empleados para dar el servicio contratado por OTECEL, deben ser protegidos contra robo, el proveedor y distribuidor está en la obligación de implementar los controles necesarios para este efecto. • Cuando el personal del proveedor y distribuidor maneje en sus computadoras información, clasificada como Reservada, Restringida o Interna por parte de OTECEL, el proveedor y distribuidor estará en la obligación de contar con una solución de encriptación aprobada por OTECEL, que asegure la confidencialidad de la misma en caso de robo de estos equipos. • Los equipos deben ser proporcionados y autorizados por las áreas de TI de cada proveedor y distribuidor y/o cumplimiento con los lineamientos de seguridad. (No se autoriza equipos personales) Los equipos tanto de proveedores y distribuidores deben ser declarados a OTECEL.
Respaldo de Información	• El Proveedor y distribuidor, se debe establecer un proceso formal de respaldo de información el cual sea validado y aceptado por OTECEL
Información	

Ámbito/ Actividad	Requerimientos
Clasificada	• Información clasificada como Reservada, Restringida o Interna, (según procedimientos internos) de gobierno u otra información de carácter sensitivo debe ser protegida de acuerdo con las regulaciones y leyes aplicables de OTECEL. • OTECEL tiene la responsabilidad de identificar la información según su clasificación, para que el Proveedor y distribuidor aplique carácter especial en ella.
Información Propietaria	• Todos los Proveedor y distribuidores deben estar cubiertos por un acuerdo de privacidad o intercambio de información entre ellos y OTECEL. • Todos los Empleados del Proveedor y distribuidor, deben estar cubiertos por un acuerdo de privacidad ente su empleador. • La información de OTECEL, así como la información propietaria de los clientes de OTECEL es privada y Reservada, y no debe ser accedida, usada, transferida, modificada, revelada, destruida, o desechada, excepto en conformidad con el acuerdo contractual. Si no se ha logrado un acuerdo entre las partes interesadas, entonces, los Empleados del Proveedor y distribuidor, no podrán acceder la información propietaria de OTECEL y de sus clientes.
Propiedad Intelectual	• En caso de que el Proveedor y distribuidor no esté cubierto por un acuerdo contractual con OTECEL que incluya la posesión de asuntos de propiedad intelectual, el Proveedor y distribuidor que accederá a los Recursos de Información de OTECEL deberá estar cubiertos por un acuerdo separado de propiedad intelectual entre sus empleados y OTECEL, o entre el Proveedor y distribuidor y OTECEL. • El conocimiento que individuos contratados obtengan acerca de OTECEL, sus servicios, equipo, instalaciones, redes, sistemas de computación, planes, procedimientos, etc, no podrán ser utilizados con el fin de ventaja personal o el provecho de otras personas, compañías, organizaciones, o gobiernos, inclusive tras terminar la prestación de servicios contractuales a OTECEL • La propiedad intelectual de OTECEL incluyendo el software desarrollado exclusivamente por/para OTECEL no debe ser usado ni revelado a terceros.
Identificación	• Todos los Empleados del Proveedor y distribuidor, deben tener identificación (usuarios individuales) para computadores, sistema y redes de OTECEL. • OTECEL debe estar provisto del nombre, dirección y número telefónico de cada Empleado del Proveedor y distribuidor, quien tendrá acceso al sistema de OTECEL. • Empleados del Proveedor y distribuidor, deberán proveer su número de cédula de identidad cuando se requiera. El número de cédula de identidad será usado para identificación del usuario en el proceso de acceso en los Recursos de Información.
Autenticación	• Las contraseñas deberán ser manualmente ingresadas con el fin de conectarse a cualquier computador o sistema de OTECEL. • Las contraseñas u otros mecanismos de autenticidad no deberán ser programados en un instrumento o paquete de software con el fin de evitar el

Ámbito/ Actividad	Requerimientos
	ingreso manual del mecanismo de autenticación en el momento de conexión. Cualquier excepción debe ser aprobada por el Equipo de Control de Seguridad de OTECEL. • Ninguna contraseña puede ser utilizada por más de 60 días debiendo el dueño de la misma cambiarla de forma obligatoria. • Al definir una nueva contraseña no se podrá reutilizar una las 12 últimas contraseñas. • Las credenciales del usuario son de uso personal e intransferible • A nivel de Proveedores y Distribuidores que prestan servicios de Call Center: Si por la naturaleza propia del servicio, se requiere que una contraseña sea entregada a un usuario diferente al dueño de la misma, es decir al usuario quién crea y para quien se generó la contraseña en base al identificador único, el proveedor y distribuidor se compromete en definir un representante en materia de seguridad, que para este caso y en base a las políticas de OTECEL será un funcionario con nivel de jefatura o superior el cual custodiará de forma temporal esa contraseña y será el responsable de entregarla al usuario final dueño del identificador de acceso, a su vez exigirá de manera inmediata el cambio de la misma. Si se identifica que la contraseña no ha sido cambiada, la responsabilidad por cualquier daño, fallo, mal manejo o acción indebida que se presente, recaerá sobre el funcionario que el proveedor y distribuidor haya designado y estará sujeto a las sanciones contractuales establecidas por OTECEL. • Una contraseña comprometida, (contraseña que es conocida) por terceros nunca debe ser reutilizada. • Las contraseñas deben tener un mínimo de doce caracteres. Administradores de sistemas y otras contraseñas de usuarios, especiales o privilegiados deben tener un mínimo de doce caracteres. • La contraseña debe incluir al menos una letra mayúscula, minúsculas número y carácter especial • Las contraseñas no deben incluir nombres propios comunes, palabras del idioma inglés, o ninguna cadena mayor a tres caracteres de la identificación del usuario. • Las contraseñas no pueden contener una cadena de tres o más caracteres numéricos o alfabéticos ascendentes o descendentes como 123, XYZ. • Las contraseñas no deben contener la totalidad o parte de un número de teléfono, cédula de identidad, dirección, fecha de nacimiento, siglas de la compañía o el nombre de un grupo de trabajo.
Conexiones con redes	• La transmisión de datos que contengan información reservada, restringida o interna, no puede ser transferida por medios que no tengan encriptación en la transmisión y autenticación, tanto de sesión como de usuario. • El tráfico de autenticación como el de gestión de los dispositivos de control de acceso de red, además de servidores remotos, deberá ser cifrado (ssh, ssl, o mediante aquellos mecanismos soportados por el tipo de red, etc.), Por lo que no se deben usar servicios como FTP, Telnet, rlogin, rexec, rsh, vnc. • Mediante la segregación de tareas y responsabilidades se debe evitar que una misma persona pueda acceder, modificar o usar una red sin autorización ni posibilidad de detección. • La conexión de la red interna de la empresa OTECEL con una red externa deberá ser autorizada previamente.

Ámbito/ Actividad	Requerimientos
	• Cualquier conexión de la red interna con otras redes externas estará protegida con un cortafuego como mínimo. • No se permitirá el uso de módems ni otros mecanismos similares (ADSL, etc.) de conexión a redes externas en sistemas que estén conectados a la red interna. • Los cortafuegos y dispositivos de encaminamiento de red del proveedor y distribuidor deberán establecer mecanismos para evitar el "spoofing".
Control de Acceso	• Los controles de acceso deben ser cumplidos y no evadidos fraudulentamente. • La exploración no autorizada o uso del comando “ping” u otros similares, en sistemas y redes es estrictamente prohibido. Cualquier intento de acceso no autorizado a Recursos de Información de OTECEL, o de otros sistemas, está prohibido. Esto incluye cualquier forma de ingreso a cualquier sistema o penetración de seguridad como “probing, sniffing, browsing, o looping” u otras variaciones. • No se deberá conectar ningún accesorio o equipo diferente al provisto por OTECEL a la red interna, sin previo análisis y autorización de Seguridad de Información. • No se deberá dejar desatendidos los sistemas que están conectados a la red. Individuos bajo contrato son responsables por el uso del sistema y serán asociados a su identificación de usuario. • El acceso a Recursos de Información de OTECEL deberá ser autorizado por el auspiciante (Administrador de contrato) o su delegado. • El acceso podrá ser revelado a personas que tengan la necesidad de saber y estén autorizados a recibir dicha información. • Empleados del Proveedor y distribuidor, no deberán ser permitidos de acceder a ningún bien de OTECEL y cambiar cualquier código de computador de manera remota, a menos que exista una cláusula escrita y aprobada en la descripción de su trabajo. • Empleados del Proveedor y distribuidor, podrán tener acceso únicamente a los bienes necesarios para cumplir su labor. • Debido a la naturaleza crítica de ciertos Recursos de Información, los responsables de aprobar dichos accesos a los sistemas de OTECEL serán los dueños de los activos, solicitud que deberá ser gestionada por el administrador de contrato de OTECEL, para los Empleados del Proveedor y distribuidor, • Los acuerdos de privacidad, intercambio de información, y propiedad intelectual deben estar establecidos entre OTECEL y el Proveedor o distribuidor, u OTECEL y el Proveedor o Distribuidor, y en caso de ser necesario, el respectivo empleado del proveedor y/o Distribuidor, antes de que se permita el acceso a un Recurso de Información de OTECEL. • Empleados del Proveedor y distribuidor, no pueden tener acceso remoto directo a la red de Otecel, por ejemplo, (VPN), únicamente se permitirá la conexión directa (punto a punto), enlace directo, o la tecnología definida por Otecel, desde las instalaciones (oficinas) del proveedor, distribuidor a la red de Otecel. El Distribuidor / Proveedor deberá proporcionar a sus colaboradores la conexión remota hacia su red local, con mecanismos de seguridad por ejemplo VPN (MFA). • Cualquier acceso por medio de un bien de computación no estandarizado por parte de Empleados del Proveedor y distribuidor, deberá estar documentado por escrito y aprobado por el administrador del contrato y área de seguridad de

Ámbito/ Actividad	Requerimientos
	la información. • Cualquier dispositivo de acceso, por ejemplo, una tarjeta SecureID, debe ser devuelta a OTECEL cuando el Proveedor y Distribuidor haya terminado sus actividades.
Plan de Contingencia	• El Proveedor y distribuidor, debe contar con soluciones redundantes tanto en su Infraestructura de Hardware como de Software, que asegure la continuidad del servicio que presta para OTECEL, de acuerdo a lo señalado en la definición de Redundancia en el ANS (Acuerdo de Nivel de Servicio). • Minimizar el grado de exposición del negocio frente a las amenazas que puedan afectar a la continuidad de este. Es decir, minimizar la probabilidad de que una amenaza explote una vulnerabilidad (se produzca un incidente) mediante la identificación y establecimiento de los controles de prevención necesarios • Mitigar el impacto que se derivaría de la ocurrencia de un incidente mediante el establecimiento de los controles de detección y recuperación oportunos.
Responsabilidad	• Cualquier equipo de OTECEL usado por los Empleados del Proveedor y distribuidor, deberá ser inmediatamente devuelto a OTECEL apenas su trabajo sea completado o haya terminado. • Cualquier equipo del Proveedor y Distribuidor usado por OTECEL y/o sus empleados deberá ser inmediatamente devuelto al Proveedor y Distribuidor apenas su trabajo sea completado o haya terminado. • Los términos del presente documento deben interpretarse en su sentido literal, en el contexto de este y cuyo objeto revela claramente la intención de los Proveedores y distribuidores. En todo caso su interpretación se sujetará a lo dispuesto por el Departamento de Seguridad Digital de OTECEL.
Administración de Seguridad	• Empleados del Proveedor y distribuidor, no están permitidos para realizar funciones de seguridad administrativa, excepto cuando sean aprobados explícitamente por OTECEL, de acuerdo con los Estándares de Seguridad Corporativa
Obligaciones relativas al personal	Con carácter general, el personal que trabaja en la empresa (empleados, proveedores / Distribuidores y terceras partes) está obligado a: • Cumplir con los consejos, recomendaciones, criterios, normativas y procedimientos de seguridad de OTECEL ***"ES.SI.SD.04.01 Obligaciones, Recomendaciones y Consejos de Seguridad"*** • Identificarse en el control de acceso a los edificios siempre que le sea requerido ***"PR.SI.SF.02.01 Control de Acceso a instalaciones de telefónica Ecuador"*** • Seguir las indicaciones del área de seguridad de OTECEL, especialmente en situaciones de emergencia o incidentes de seguridad **"**PR.SI.SD.01.01 Procedimiento Gestión de Incidentes para proveedores (Externos)**"** • Cumplir con los siguientes criterios en la gestión de las credenciales de acceso:

Ámbito/ Actividad	Requerimientos
	○ Responsabilizarse de las acciones que se realicen con su identificador ○ Mantener la confidencialidad de las credenciales de acceso y no compartirlas con nadie, así como comunicar cualquier anomalía o incidente (robo, pérdida, extravió, etc.) que tenga con las mismas al Departamento de Seguridad de OTECEL ○ Evitar la escritura, copia o reproducción de las mismas en papel o almacenarlas en un fichero sin protección ○ Cambiar las contraseñas siempre que sospechen que pudieran haber sido comprometidas ○ Cambiar las contraseñas frecuentemente, al menos cada 90 días ○ Seleccionar contraseñas fáciles de recordar pero que cumplan con la sintaxis establecida en norma de caracteres y longitud ○ No utilizar las mismas contraseñas en servicios externos (por ejemplo, en cuentas de correo gratuitas de Internet, etc.) u otros propósitos ajenos a la empresa ○ Cumplir con el procedimiento de eliminación de accesos del personal que tenga a su cargo, que no preste servicio para OTECEL o el proveedor , distribuidor asociado. ○ Preservar los activos de la organización, incluyendo sistemas, equipos, información, mobiliario y material de oficina. Estos activos deberán ser utilizados para propósitos relacionados con el negocio de la empresa. Cualquier uso de los recursos o instalaciones de la empresa con fines ilegales y/o lucrativos, así como comerciales o profesionales distintos a los permitidos, se encuentra estrictamente prohibido. ○ Utilizar los sistemas de información y redes de comunicaciones autorizados estrictamente para el cumplimiento de sus funciones dentro de la empresa. ○ Concretamente, los empleados podrán utilizar el correo electrónico y los servicios de Internet con libertad y responsabilidad, en el sentido más amplio posible para el desempeño de las actividades de su puesto de trabajo. No deben usar estos servicios de forma que pongan en riesgo la seguridad y reputación de la empresa (evitar navegar por sitios no confiables, que puedan facilitar la propagación de virus o spam, no realizar descargas de material protegido por copyright, entre otros). ○ Finalizar las sesiones que tenga abiertas cuando no las necesite ○ Usar un protector de pantalla con un periodo de inactividad máximo de 5 minutos y que necesite ser desbloqueado por contraseña ○ No desactivar ni desconfigurar los mecanismos de protección instalados en los sistemas (cortafuegos personales, antivirus etc.) ○ Sólo utilizar software homologado y licenciado por la empresa ○ No intentar aumentar el nivel de privilegios de su usuario en los sistemas ○ Borrar cualquier programa o fichero que impida o dificulte el normal funcionamiento del sistema ○ Velar por las actualizaciones de seguridad del sistema y actualización de los antivirus, de acuerdo a los mecanismos establecidos en la empresa ○ Cumplir con una política de "mesa limpia": ▪ Guardar bajo llave la información sensible impresa en papel o almacenada en soportes

Ámbito/ Actividad	Requerimientos
	▪ No desatender la información en impresoras comunes, fax, etc. ▪ Destruir la información sensible en destructoras ▪ Proteger las PC's con los candados de seguridad proporcionados o Acceder sólo a la información y recursos a los que se tiene acceso autorizado o Cumplir con las normas de clasificación y tratamiento de la información o Está prohibido sacar provecho de las vulnerabilidades o debilidades que tengan los sistemas. o Cumplir los criterios, recomendaciones y procedimientos de seguridad que se deben seguir en el teletrabajo o Cumplir con las restricciones de propiedad intelectual o industrial del software o Cumplir con la legislación de protección de datos aplicable, en lo que se refiere a su actividad laboral en la entidad, velando que los datos son veraces, exactos y completos o Devolver todos los activos de la empresa (ordenadores portátiles, teléfonos móviles, entre otros) una vez terminada la relación laboral con la misma. En caso de proveedores / distribuidores y personal externo, la empresa subcontratada será la responsable de exigir la devolución de los activos. o Guardar, por tiempo indefinido, la máxima reserva sobre los datos, documentos, metodologías, claves, análisis, programas y demás información, en soporte material electrónico, a la que tengan acceso durante su relación laboral no pudiendo divulgarlos ni utilizarlos directamente o a través de terceras personas o empresas. o Velar por la continuidad y los planes de contingencia de los servicios y recursos que están asociados a sus actividades.
Requisitos de protección física	Toda zona restringida, esto incluye, pero no se limita a: centro de datos, cuartos de comunicaciones y demás áreas que procesen, almacenen o transmitan información clasificada como reservada o restringida deberán contar con: o Sistema de CCTV de seguridad (circuito cerrado de cámaras) o Sistema electrónico de control de acceso del personal o Sistema de alarmas, detectores de movimiento. o La infraestructura de comunicaciones deberá cumplir con las normas de cableado estructurado vigentes en la industria. o Los centros de datos y cuartos de comunicaciones que soporten servicios prestados para OTECEL, deberán contar con: ▪ Techo falso ▪ Piso falso ▪ Dispositivos para control de temperatura y humedad según lo establecido técnicamente o Deberá existir adicionalmente: ▪ Proceso de registro y control de accesos a estas zonas ▪ Proceso para control de temperatura y humedad o Las instalaciones empleadas para dar el servicio deberán contar con el permiso vigente de funcionamiento emitido por los entes regulatorios municipales y estatales.
Al interior de una	

Ámbito/ Actividad	Requerimientos
instalación	• Llevar en un sitio visible la tarjeta de identificación personal asignada por su empresa • Llevar en un sitio visible la tarjeta de identificación personal asignada por parte de OTECEL en los casos en que se les haya designado. • Identificarse previo a acceder a toda instalación • Cumplir procedimiento de control de acceso definido en OTECEL • Está prohibido ingerir bebidas alcohólicas • Deberá respetar las normas de seguridad establecidas por OTECEL • Deberá hacer buen uso de las instalaciones • Cumplir con los procedimientos de Seguridad Física propios y relacionados • Las áreas involucradas serán las responsables de los trabajos a realizarse por parte de sus proveedores y distribuidores, teniendo que en todos los casos estar presente una persona del área solicitante de los trabajos como responsable. • En caso de que los trabajos requieran de la presencia de personal de Seguridad, el área responsable solicitará este servicio y el costo asociado a estos trabajos serán asumidos y pagados dentro de los costos de su presupuesto
En instalaciones fuera de las oficinas principales	• Obedecer los requerimientos de seguridad de dichos lugares • No exponer a las personas, instalaciones y activos de información a riesgos de seguridad innecesarios • Cumplir con el procedimiento de ingreso a instalaciones y radio bases establecido por OTECEL
Excepciones de los Requisitos de Seguridad de información	Si una de las partes considera que existe necesidad de una variación a los requerimientos de seguridad antes manifestados, esta deberá entregar una petición formal de variación para ser analizada.