FLUJO DE APROBACIÓN

Cargo	Rol
Gerente de Seguridad Integral	Dueño de Proceso N2
Gerente de Seguridad Digital	Dueño del Proceso N2
Jefe Arquitectura & Gobierno Seguridad	Dueño del Proceso N3
Gerente Legal	Participante
Gerente Atención y Desarrollo Comercial	Participante
Gerente Ventas y Canal Presencial	Participante
Gerente Nacional Negocios y Emprendedores	Participante
Gerente de Atención	Participante
Gerente Ingeniería Preventa e Implantación	Participante
Gerente TI	Participante
Jefe de Área Contact Center	Participante
Jefe de Compras	Participante
Jefe Infraestructura TI	Participante
Especialista de Procesos	Participante
Especialista Sr Seguridad de la Información	Participante

1. INTRODUCCION

El enfoque de OTECEL sobre la seguridad en la cadena de suministro se basa en el adecuado conocimiento de los proveedores y su importancia para el negocio, garantizando la adecuada prestación del servicio de éstos, se minimiza el riesgo de indisponibilidad y acceso no autorizado. Para alcanzar un nivel de seguridad homogéneo y adecuado a las necesidades del negocio. A continuación, se describen los objetivos de control asociados a la seguridad en la cadena de suministro:

- Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.
- Mantener un nivel de seguridad en la provisión de productos y servicios por parte de los proveedores.
- Mantener la seguridad en la información que se transfiere dentro de la organización y con cualquier entidad externa.

Para asegurar el cumplimiento de estos objetivos, se establecen en este documento los requerimientos de seguridad de la información para Proveedores y/o Distribuidores autorizados externos.

2. OBJETO

Establecer y formalizar los requerimientos y obligaciones de seguridad de la información que deben cumplir los Proveedores y/o Distribuidores autorizados de OTECEL.

3. RESPONSABILIDADES

3.1. Administrador del Contrato – OTECEL:

- Asegurar y garantizar que el Proveedor y/o Distribuidor cumpla con los requerimientos de seguridad de la información establecidos en el presente documento.
- Validar periódicamente el cumplimiento de los requerimientos de seguridad de la información.
- Supervisar que el nivel de seguridad del producto o servicio contratado sea adecuado y cumpla con lo establecido en el contrato con el Proveedor y/o Distribuidor
- Ser el interlocutor entre el Proveedor y/o Distribuidor y el Área de Seguridad.
- Garantizar que los requisitos de seguridad se mantengan en toda la cadena de suministro del Proveedor y/o Distribuidor.

3.2. Proveedor y/o Distribuidor:

- Cumplir con los requerimientos de seguridad de la información especificados en este documento.
- Implementar y mantener las medidas necesarias para el cumplimiento de los requerimientos de seguridad de la información.
- Facilitar las auditorías de seguridad realizadas por el Área de Seguridad o por terceros designados.
- Informar de inmediato los incidentes de seguridad que pueda afectar la información o los

servicios proporcionados, objeto del contrato.

3.3. Área de Seguridad:

- Llevar a cabo auditorías de seguridad para verificar el cumplimiento de las normas establecidas.
- Coordinar la respuesta a incidentes de seguridad y asegurar que se tomen las medidas correctivas necesarias.
- Mantener actualizadas los lineamientos de seguridad de la información y comunicar cualquier cambio relevante a los Proveedores y/o Distribuidores.
- Proveer apoyo y asesoramiento en materia de seguridad de la información cuando sea requerido.

4. POLÍTICAS

Generales
El Proveedor y/o Distribuidor se compromete a gestionar el cumplimiento de los requisitos de seguridad detallados en el presente documento, mientras que el administrador del contrato debe garantizar que el Proveedor y/o Distribuidor cumpla con los requisitos de seguridad.
El Proveedor y/o Distribuidor deberá informar formalmente cualquier cambio en el personal y mantener actualizados los usuarios a su cargo, además deberá gestionar la eliminación de accesos para el personal desvinculado que presta servicios a OTECEL. Esta notificación debe enviarse al administrador del contrato designado por OTECEL dentro de las 24 horas calendario de haber sucedido la salida del personal.
El Proveedor y/o Distribuidor debe operar de forma ética y legal, cumpliendo con los requisitos de seguridad estipulados por OTECEL
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/o Distribuidor, así como sus empleados, deberán permitir que el personal autorizado de OTECEL realice inspecciones de seguridad periódicas en las instalaciones correspondientes. Además, se deberán proporcionar reportes de auditoría extraordinarios relacionados con los equipos de cómputo utilizados para gestionar negocios o información de OTECEL, independientemente de si dichos equipos son propiedad de OTECEL, arrendados o están bajo el control del Proveedor, distribuidor o sus Empleados
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.

El Proveedor y/o Distribuidor deberá tener al menos la siguiente documentación como marco normativo interno de seguridad:

- Procedimiento de concienciación y formación en lo referente a normas de seguridad de la información.
- Procedimiento de gestión de cambios del Proveedor y/o Distribuidor.
- Procedimiento de notificación gestión y escalamiento de los incidentes de seguridad que detalle:
  - Accesos no autorizados a la información,
  - Falta de integridad,
  - Indisponibilidad,
  - Fuga de Información.
  - 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.
- 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:
  - Planes de emergencia
  - Planes de contingencia
  - Recuperación de desastres
  - Plan de pruebas

Los Recursos de Información de OTECEL, como redes, correos electrónicos y mensajes de voz, son propiedad exclusiva de OTECEL y deben ser utilizados únicamente para fines relacionados con el objeto del contrato

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). Permitiendo auditorías justificadas y cumpliendo con las leyes vigentes.

Los datos personales cumplirán con lineamientos establecidos en las leyes vigentes.

Informe de Infracciones

En caso de que cualquier empleado del Proveedor y/o 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, se deberá reportar la medida junto con un informe del problema al Área de Seguridad Digital lo más pronto posible.

Todo equipo del Proveedor y/o 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/o Distribuidor, conectado a la red de OTECEL, deberá usar un software para protección de virus /antimalware debidamente licenciado.

Restricciones del Uso de Software

Todo software instalado en los equipos del Proveedor y/o Distribuidor que se conecte a la red de OTECEL, deberá ser previamente autorizado por OTECEL.
Software personal de los Empleados del Proveedor y/o Distribuidor no está autorizado por lo que, no debe ser instalado ni utilizado en los computadores que se conecten o usen recurso para los servicios que se prestan a OTECEL.
Se prohíbe la instalación y uso de software gratuito en equipos empleados por el Proveedor y/o 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
El Proveedor y/o Distribuidor, que realice cambios en el ambiente de producción, preproducción o testing en las plataformas, a las que acceda y maneje local o remotamente, 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 de OTECEL.**
Gestión de Incidentes
El Proveedor y/o Distribuidor debe contar con una herramienta, mecanismo o procedimiento para gestionar incidentes que ocurran en sus plataformas, sistemas o servicios tecnológicos brindados a OTECEL S.A. Además, el Proveedor y/o Distribuidor deberá evaluar soluciones de monitoreo y correlación de logs (SIEM) para la detección de comportamientos anómalos de usuarios, y que sean integrables con las plataformas de OTECEL S.A. para fortalecer la trazabilidad de los incidentes.
El Proveedor y/o Distribuidor debe tener la capacidad de entregar en un tiempo mutuamente acordado entre los partes informes detallados de los incidentes gestionados en los que debe constar tiempos de respuesta, penalidades, cumplimiento de Acuerdo de Nivel de Servicio (ANS).
El Proveedor y/o Distribuidor, debe acogerse a los ANS para la gestión de incidentes especificados en el contrato.
Desarrollo de Software
El código fuente creado, modificado, o de otra manera provisto para OTECEL debe cumplir con los siguientes requisitos: - Debe ser documentado de acuerdo con su función y requerimientos de uso, para OTECEL - No debe contener ningún código de acceso maestro (identificación, contraseña, backdoor, caballo de Troya, etc.) al sistema, y no debe contener ningún virus u otro código dañino, fecha de expiración. - En el código fuente se debe garantizar librerías actualizadas y seguras que garantice la calidad y confiabilidad de este. - No debe degradar la seguridad al interferir o modificar las funciones normales del sistema operativo en el que residirá el software.
El Proveedor y/o Distribuidor que realiza el desarrollo del sistema o de software bajo la dirección de OTECEL, debe cumplir con todos los requisitos de desarrollo y seguridad de la **Política de Seguridad de OTECEL** y la **Instrucción global de desarrollo seguro de software** y las políticas establecidas en los requerimientos de Seguridad para Acuerdos Contractuales.
Es requisito que en los sistemas o soluciones desarrolladas o accedidas por el Proveedor y /o Distribuidor, cuente con módulos de gestión para administración de cuentas de usuarios, además deberán contar con un control de auditoria para chequeos permanentes.
No se deberá modificar el sistema operativo, código de aplicaciones u otro software que pueda impactar negativamente la actual o futura seguridad del ambiente de los sistemas.
Computadores Portátiles

Computadores portátiles del Proveedor y/o Distribuidor, empleados para dar el servicio contratado por OTECEL, deben ser protegidos contra robo, el Proveedor y/o Distribuidor está en la obligación de implementar los controles necesarios para este efecto.
Cuando el personal del Proveedor y/o Distribuidor maneje en sus computadoras información, clasificada como Reservada, Restringida o Interna por parte de OTECEL, el Proveedor y/o Distribuidor estará en la obligación de contar con una solución de encriptación aprobada por OTECEL, que asegure la confidencialidad de esta en caso de robo de estos equipos.
Los equipos deben ser proporcionados y autorizados por las áreas de TI de cada Proveedor y/o Distribuidor, cumpliendo con los lineamientos de seguridad de OTECEL.
Respaldo de Información
El Proveedor y/o Distribuidor debe establecer un proceso formal de respaldo de información, el cual debe ser validado y aceptado por OTECEL
Información Clasificada como Reservada, Restringida o Interna, (según procedimientos internos) de gobierno u otra información de carácter sensible debe ser protegida y respaldada de acuerdo con las regulaciones y leyes aplicables de OTECEL.
Información 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.
Es responsabilidad del administrador de contrato por parte de OTECEL identificar la información según su clasificación, para que el Proveedor y/o Distribuidor apliquen el carácter especial correspondiente.
Información Propietaria
Todos los Proveedores y/o Distribuidores deben estar cubiertos por un acuerdo de privacidad o de intercambio de información entre ellos y OTECEL.
Todos los Empleados del Proveedor y/o Distribuidor, deben estar cubiertos por un acuerdo de privacidad con su empleador.
La información referente a 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 no podrán acceder la información propietaria de OTECEL y de sus clientes.
Propiedad Intelectual
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/o 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/o Distribuidor que tendrá acceso a los sistemas de OTECEL.
Empleados del Proveedor y/o Distribuidor, deberán proveer su número de cédula de identidad o pasaporte 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

Para conectarse a cualquier computadora o sistema de OTECEL, las contraseñas deben ser ingresadas manualmente.
Las contraseñas y otros mecanismos de autenticación no deben ser programados en ningún dispositivo o software para evitar el ingreso manual en el momento de conexión. Cualquier excepción debe ser aprobada por el equipo de Seguridad Digital de OTECEL
Ninguna contraseña puede ser utilizada por más de 60 días debiendo el dueño de esta, cambiarla de forma obligatoria.
Al definir una nueva contraseña no se podrá reutilizar las 12 últimas contraseñas.
Las credenciales del usuario son de uso personal e intransferible
Una contraseña comprometida, (contraseña que es conocida) por terceros nunca debe ser reutilizada.
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.
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/o 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 está prohibido. Cualquier intento de acceso no autorizado a recursos de información de OTECEL, 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 Digital
No se deberá dejar desatendidos los sistemas que están conectados a la red. El Proveedor y/o Distribuidor es responsable por el uso del sistema

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.
Los empleados del Proveedor y/o Distribuidor no deberán tener acceso a ningún bien de OTECEL ni cambiar cualquier código de computadora de manera remota, a menos que exista una cláusula escrita y aprobada en la descripción de su trabajo
Empleados del Proveedor y/o Distribuidor, podrán tener acceso únicamente a los bienes necesarios para cumplir su labor.
Debido a la naturaleza crítica de ciertos recursos de información, los dueños de los activos serán responsables de aprobar el acceso a los sistemas de OTECEL. La solicitud deberá ser gestionada por el administrador de contrato de OTECEL para los empleados del Proveedor y/o Distribuidor.
Los acuerdos de privacidad, intercambio de información, y propiedad intelectual deben estar establecidos entre OTECEL y el Proveedor y/o Distribuidor.
Empleados del Proveedor y/o 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, ZTNA o la tecnología definida por OTECEL, desde las instalaciones (oficinas) del proveedor, distribuidor a la red de OTECEL. El Proveedor y/o Distribuidor deberá proporcionar a sus colaboradores la conexión remota hacia su red local, con mecanismos de seguridad por ejemplo VPN y garantizar el MFA.
Cualquier acceso a equipos informáticos no estandarizados por parte de empleados del Proveedor y/o Distribuidor deberá estar documentado por escrito y aprobado por el administrador del contrato y el área de Seguridad Digital
Cualquier dispositivo de acceso, por ejemplo, una tarjeta SecureID, debe ser devuelta a OTECEL cuando el Proveedor y/o Distribuidor haya terminado sus actividades.
Plan de Contingencia
El Proveedor y/o 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 con lo señalado 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/o Distribuidor, deberá ser inmediatamente devuelto a OTECEL apenas su trabajo sea completado o haya terminado.
Cualquier equipo del Proveedor y/o Distribuidor usado por OTECEL y/o sus empleados deberá ser inmediatamente devuelto al Proveedor y/o Distribuidor apenas su trabajo sea completado o haya terminado.
Obligaciones relativas al personal

Con carácter general, el personal que trabaja en el Proveedor y/o Distribuidor está obligado a:
Cumplir con los lineamientos, recomendaciones, criterios, normativas y procedimientos de seguridad de OTECEL.
Identificarse en el control de acceso a los edificios siempre que le sea requerido de acuerdo con lo establecido en el **Procedimiento Control de accesos a las Instalaciones de Telefónica Ecuador**.
Seguir las indicaciones del área de seguridad de OTECEL, especialmente en situaciones de emergencia o incidentes de seguridad de acuerdo con lo establecido en el **Procedimiento Gestión de Incidentes para Proveedores**.

Cumplir con los siguientes criterios en la gestión de las credenciales de acceso:

- 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 Administrador del Contrato.
- Evitar la escritura, copia o reproducción de las credenciales en papel o almacenarlas en un fichero sin protección
- Cambiar las contraseñas cuando exista sospecha de que pudieran haber sido comprometidas
- Cambiar las contraseñas frecuentemente, al menos cada 60 días
- Seleccionar contraseñas que cumplan con la sintaxis establecida en norma de caracteres y longitud de acuerdo con la **Procedimiento Gobierno de Gestión de Identidades de OTECEL.**
- 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.
- Utilizar los activos, sistemas de información y redes de comunicaciones autorizados estrictamente para el cumplimiento de sus funciones dentro 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.
- 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.
- 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 con 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
    - No desatender la información en impresoras comunes, fax, etc.
    - Destruir la información sensible.
    - Proteger las PC’s con candados de seguridad.
- Acceder sólo a la información y recursos a los que se tiene acceso autorizado.
- Cumplir con las normas de clasificación y tratamiento de la información.
- Cumplir los criterios, recomendaciones y procedimientos de seguridad que se deben seguir en el teletrabajo.

- Cumplir con las restricciones de propiedad intelectual o industrial del software.
- 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.
- Devolver todos los activos de la empresa (ordenadores portátiles, teléfonos móviles, entre otros) una vez terminada la relación laboral con la misma. En caso del Proveedor y/o Distribuidor y personal externo, la empresa subcontratada será la responsable de exigir la devolución de los activos.
- 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.
- 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:

- Sistema de CCTV de seguridad (circuito cerrado de cámaras)
- Sistema electrónico de control de acceso del personal
- Sistema de alarmas, detectores de movimiento.

La infraestructura de comunicaciones deberá cumplir con las normas de cableado estructurado vigentes en la industria.

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
- Proceso de registro y control de accesos a estas zonas.
- Proceso para control de temperatura y humedad.

Al interior de una 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 de OTECEL.
- Cumplir procedimiento de control de acceso definido en OTECEL.
- Deberá respetar las normas de seguridad establecidas por OTECEL.
- 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/o Distribuidores, teniendo que en todos los casos estar presente una persona del área solicitante de los trabajos como responsable.

En instalaciones fuera de las oficinas principales

Cumplir los requerimientos de seguridad de dichos lugares.
No exponer a las personas, instalaciones y activos de información a riesgos de seguridad.