Estándar para el centro de llamadas

Términos generales

(A) Estos Requerimientos deben acompañar a la Matriz de Implementación del Apéndice 1 de este documento, la cual brinda más detalles sobre las conductas y los resultados que BT considerará aceptables a la hora de considerar el cumplimiento del Proveedor con los Requerimientos.

(B) BT podrá realizar evaluaciones de riesgos en el centro de contacto tal como se establece en 3.10 de los Requerimientos de Seguridad para Proveedores de BT ("Requerimientos de Seguridad") en cualquier momento, ya sea mientras presta los servicios y después de ello. Sin perjuicio de otras soluciones que pudiera utilizar BT, BT podrá estipular acciones de remediación, controles de compensación y medidas defensivas para atender riesgos identificados y/o incumplimiento o cumplimiento parcial de estos Requerimientos, las cuales deberá implementar el Proveedor y documentarse como apéndice de este estándar; todos los costos asociados con la implementación de requerimientos de seguridad nuevos deberán acordarse entre las partes.

(C) BT podrá, a partir de una solicitud, revisar las políticas y los procedimientos del Proveedor que plasmen los requerimientos de esta guía en el curso de las evaluaciones de riesgo en el centro de contacto. Tales políticas podrán incluir, pero no se limitan a, lo siguiente: Política de uso de computadoras, eliminación de TI, autenticación de clientes, verificaciones de antecedentes previas al empleo, evaluación de riesgos y proceso de gestión, etc.

1. Seguridad física

1.1 El Proveedor debe asegurar que las áreas del centro de contacto (ver Glosario) utilizadas para la explotación de la cuenta BT/EE estén físicamente separadas de todas las demás áreas de negocios con Controles de Acceso Físicos.

1.2 El Proveedor debe contar con un proceso de acceso auditable para la solicitud y aprobación de nuevos accesos físicos o la remoción de otros existentes en el área del centro de contacto.[1]

1.3 El Proveedor debe garantizar que para evaluar los derechos de acceso físico a las áreas del centro de contacto (incluidos los movimientos y cambios internos) y como parte del proceso aplicable cuando un empleado deja la empresa del proveedor, el proceso auditable de acceso se revea cada tres (3) meses y la fecha de cada revisión queda registrada.

1.4 El Proveedor debe garantizar que no existe trabajo sin supervisión directa en el área del centro de contacto. Este requerimiento incluye al personal de limpieza y otros empleados de terceros.

1.5 El Proveedor debe tener un proceso auditable que asegure que no hay amontonamientos en las barreras y/o puertas de acceso controlado. El proceso debe ser observado por todos y su incumplimiento repetido será sujeto a medidas disciplinarias.

[1] Ver ejemplos de procesos de acceso auditable en la Matriz de Implementación.

2. Pases de seguridad y para visitantes

2.1 El Proveedor debe garantizar que los empleados que pueden (como parte de su trabajo) llevar y usar teléfonos celulares, laptops, iPads y/o tablets en las áreas del centro de contacto son fáciles de reconocer para otros empleados y supervisores.[2]

2.2 El Proveedor debe contar con un proceso auditable para emitir y gestionar los Pases de Seguridad y los Pases de Seguridad Temporarios para los empleados del centro de contacto cuando sea necesario, que incluya la cancelación automática de los derechos de acceso cuando expira el periodo para el cual se requirió el pase.

2.3 El Proveedor debe garantizar que los pases de seguridad y los cordones no identifiquen el lugar de trabajo del empleado.

2.4 El Proveedor debe garantizar la existencia de un proceso auditable para el tratamiento de visitantes y que este esté publicado para todos los empleados. Debe mantenerse un registro de visitantes como prueba.[3]

2.5 Los pases de seguridad que se emitan a un visitante deben distinguirlo de los empleados, y deben recuperarse cuando este abandona el centro de contacto; todos los pases de seguridad que no se hayan devuelto deben deshabilitarse el próximo día hábil.

2.6 El Proveedor debe asegurar que los visitantes al área del centro de contacto están acompañados en todo momento y usan los pases o distintivos de visitantes en lugares visibles.

3. Empleados

3.1 El Proveedor debe garantizar que todos los Efectos Personales (incluidos los dispositivos móviles) se guardan en Casilleros Designados fuera del área del centro de contacto.

3.2 El Proveedor debe permitir el ingreso al área del centro de contacto con medicamentos personales o equipo médico básico necesarios, tal como inhaladores, insulina o medicamentos para la tos.

3.3 A menos que esté autorizado después de una evaluación de riesgos, el personal que trabaja en el área del centro de contacto no tiene permitido llevar teléfonos celulares o dispositivos móviles a menos que estén autorizados. El Proveedor debe implementar inspecciones oculares sorpresa del personal regularmente para garantizar que no se ingresen teléfonos celulares ni dispositivos móviles al área del centro de contacto; también se debe instalar cartelería que prohíba el uso de tales dispositivos. Además, los programas de capacitación en concientización sobre la seguridad deben referirse con claridad a este requerimiento y deberá existir un proceso disciplinario que sancione su incumplimiento.

3.4 El Proveedor debe garantizar un proceso que habilite la comunicación de terceros externos con los empleados en caso de una emergencia personal.[4]

3.5 Deberá existir un proceso auditable para la autorización y el uso de lapiceras, lápices y papel dentro del área del centro de contacto. Estos elementos no están permitidos a menos que los empleados estén autorizados por sus gerentes a hacerlo como parte de sus trabajos.

[2] Ver qué constituye fácil reconocimiento en la Matriz de Implementación.
[3] Ver qué información ha de quedar en el registro de Visitantes en la Matriz de Implementación.
[4] Ver ejemplos de procesos para tratar la comunicación en emergencias personales en la Matriz de Implementación.

3.6 El Proveedor debe garantizar que, si se produjeran notas manuscritas como parte del trabajo de un empleado, estas no deben quedar desatendidas y deben guardarse en forma segura (según se indica para el tratamiento de la clasificación y la información), o bien se deben eliminar[5] al final del día laboral para demostrar una 'Política de Escritorio Limpio'[6].

http://www.selling2bt.bt.com/working/ThirdPartySecuritystandards/index.htm

3.7 El Proveedor debe procurar la existencia de pizarras y anotadores borrables (incluidos marcadores y borradores) como alternativa a lapiceras, lápices y papel, para que sea posible tomar notas durante las llamadas. El Proveedor debe garantizar que esas notas se borran tan pronto como concluye la consulta con el cliente, y todas las notas deben eliminarse de las pizarras al final del turno de cada asesor. Los gerentes y supervisores deben recorrer el piso y realizar inspecciones sorpresa para garantizar que se cumpla este requerimiento.

3.8 El Proveedor debe garantizar que todas las notas temporarias que se guarden en línea o en herramientas electrónicas (como soporte de llamadas a clientes) se borran automáticamente al final del turno de cada asesor o al final del día laboral. Eso debe suceder o bien en forma automática o bien se debe guardar un registro diario que garantice el cumplimiento de este requerimiento.

3.9 El Proveedor debe garantizar que existe un proceso auditable para el uso de pizarras y papel que asegure lo siguiente:

- Los papeles están guardados en forma segura o se han retirado y eliminado al final del día laboral.
- Las pizarras están limpias al final de cada turno y al final del día laboral.[7]

3.10 El Proveedor debe procurar que todas las interacciones con los clientes queden registradas en la cuenta (memo o anotador según el sistema que se use).

3.11 El Proveedor debe garantizar que ninguna interacción con los clientes queda registrada en las aplicaciones de Microsoft Office a menos que los empleados estén autorizados por medio de una evaluación de riesgos como parte de sus trabajos.

3.12 El Proveedor debe garantizar que se evalúan los riesgos de todos los puestos autorizados a realizar cualquiera de las siguientes actividades dentro del área del centro de contacto según los requerimientos establecidos en la sección 11. Tales actividades incluyen, pero no se limitan a, lo siguiente:

- Uso de aplicaciones de Microsoft Office
- Uso de dispositivos móviles para negocios
- Uso de laptops de la empresa
- Uso de efectos personales (tal como se definen en el Glosario)
- Impresión o copia de información de los clientes
- Descarga de grabaciones de llamadas desde todos los servidores
- Acceso a herramientas de correo electrónico internas o externas, u otras herramientas de comunicaciones; por ejemplo, de mensajería instantánea
- Uso de lapiceras o lápices y papel para tomar notas

[5] Ver ejemplos de almacenamiento o eliminación seguros en la Matriz de Implementación.
[6] Ver ejemplo de lo que debería incluir la Política de Escritorio Limpio en la Matriz de Implementación.
[7] Ver ejemplos de lo que debe incorporar un control de pizarras y papel en la Matriz de Implementación.

- Envío de múltiples mensajes de textos a clientes
- Acceso remoto al equipo de un cliente

3.13 El Proveedor debe garantizar que no es posible enviar múltiples mensajes de texto (un mensaje de texto a varios clientes), a menos que los empleados estén autorizados a hacerlo como parte de sus trabajos. Si se envían tales textos, debe quedar registro que demuestre cuándo sucedió, quiénes fueron los destinatarios y las razones para el envío.

3.14 El Proveedor debe garantizar que no esté permitida -o no sea posible- la descarga de las grabaciones de llamadas desde los servidores de grabaciones a los escritorios o las laptops a menos que el individuo esté autorizado a hacerlo como parte de su trabajo. Si este fuera el caso, debe quedar registro de quién está aprobado para hacerlo y, si las llamadas fueron descargadas, debe registrarse por qué se hizo, cuál fue la llamada que se descargó y las razones de la descarga. Se debe revisar la validez de los incumplimientos y de los asesores autorizados en forma regular.

4. Equipo

4.1 El Proveedor debe garantizar que todos los asesores tengan protegidas las pantallas de sus computadoras de manera que el contenido no sea visible desde fuera del área separada del centro de contacto.[8]

4.2 El Proveedor debe garantizar que las impresoras y las máquinas de fax están ubicadas en zonas seguras, y su uso limitado solo a individuos autorizados y estricta necesidad. La lista de usuarios autorizados y el uso de las máquinas debe revisarse en forma regular para garantizar su vigencia. Todas las copias en papel deben guardarse seguras según el estándar de tratamiento y clasificación de la información, y no debe retirarse del centro de contacto a menos que lo autorice BT.

4.3 El Proveedor debe garantizar que toda actividad de impresión y copia exija la identificación del usuario y el código de seguridad de manera que todas las impresiones sean monitoreadas y registradas con fines de auditoría.

4.4 El Proveedor debe garantizar la existencia de trituradores de papel de corte cruzado y cesto de papeles confidenciales en las áreas donde están las impresoras y las máquinas de fax. Los trituradores y los cestos deben vaciarse regularmente y el contenido eliminarse en forma segura.

4.5 El Proveedor debe garantizar que toda copia de información en papel se elimina en forma segura, ya sea triturándola o colocándola en los cestos de residuos confidenciales según lo establece la sección 4.4.

4.6 El Proveedor debe garantizar que los Activos Físicos asignados a individuos al principio de su empleo en el área del centro de datos se recuperan o se eliminan antes de que deje su puesto allí o rescinda su contrato con BT/EE. Debe mantenerse un inventario de Activos Físicos.[9]

4.7 El Proveedor debe garantizar que los Activos Físicos que se han recuperado o retirado sean eliminados en forma segura y de acuerdo con los requerimientos correspondientes.[10]

[8] Vea ejemplos de "pantallas protegidas" en la Matriz de Implementación.
[9] Vea ejemplos de lo que debería incluir el inventario de Activos Físicos en la Matriz de Implementación.
[10] Vea ejemplos de lo que deben incorporar los requerimientos de eliminación segura en la Matriz de Implementación.

5. Acceso a sistemas

5.1 Para proteger los datos de los clientes, todos los asesores deben registrar su Identificación de Usuario cuando accede a la cuenta o el registro de un cliente así como el motivo del acceso. Solo se deberá dar acceso después de la aprobación del Propietario del Sistema o un gerente de línea. Además, solo se permitirá el acceso a las cuentas de los clientes si se lo requiere el puesto de asesor; este acceso se debe establecer al mínimo necesario para que el asesor cumpla con su trabajo. No debe permitirse el acceso de ninguna persona que no necesite acceso a un sistema de BT y/o EE para ver los registros de los clientes por ningún motivo.

5.2 Se debe evitar el acceso con visualización solamente a menos que lo requieran las operaciones. Si se autorizara este tipo de acceso, se debe registrar y monitorear para evitar el uso inapropiado.

5.3 El Proveedor debe asegurar que los empleados no tienen permitido acceder a Internet, el correo electrónico personal o externo, los medios sociales (como Facebook) u otra herramienta de comunicación, como Messenger o Communicator, a menos que esté autorizado por BT y se requiera como parte de un trabajo.

5.4 El Proveedor debe asegurar que todos los mensajes de texto enviados desde los sistemas de los proveedores son registrados y monitoreados. Si se envían textos, debe quedar registro que demuestre cuándo sucedió, quiénes fueron los destinatarios y las razones para el envío.

5.5 El Proveedor debe asegurar que solo se permita el uso de herramientas de acceso remoto que hayan sido aprobadas previamente para acceder a los dispositivos de los clientes con fines de soporte, y que su uso queda restringido al personal que las necesite para realizar su trabajo. El acceso debe revisarse cada 3 meses y será revocado si ya no se necesita para realizar la tarea. Se deben implementar soluciones que identifiquen el uso de herramientas de acceso remoto no aprobadas.[11]

5.6 El Proveedor no debe permitir el acceso remoto al correo electrónico laboral de los empleados del centro de contacto ni a ningún sistema para acceder a los registros de los clientes.

5.7 El Proveedor debe asegurar que los empleados tienen acceso para lectura solamente a las unidades de disco compartidas solo provistas y gestionadas por BT y/o EE. No debe usarse ninguna otra unidad de disco dentro del centro de contacto. No están permitidos la descarga, la copia, el retiro o la modificación de la información de los clientes desde cualquiera de los sistemas, aplicaciones o bases de datos de BT y/o EE.

6. Grabaciones de llamadas

6.1 El Proveedor debe asegurar que se graban todas las llamadas de los clientes. El Proveedor debe asegurar que las grabaciones de las llamadas (voz o pantalla) están protegidas durante sus transmisión desde el escritorio de la PC a los servidores de grabaciones de llamadas.[12]

6.2 El Proveedor debe asegurar que las grabaciones de las llamadas se guardan en forma segura, particularmente si incluyen Información de Pago con Tarjeta (PCI), para evitar la pérdida o el

[11] Vea ejemplos de conductas que se deben identificar y herramientas de acceso remoto en la Matriz de Implementación.
[12] Vea ejemplos de cómo deben protegerse las transmisiones de las grabaciones de llamadas en la Matriz de Implementación.

uso inapropiado de estos datos del clientes. La PCI debe estar encriptada y se debe tener implementada una solución de gestión de claves para protegerla usando la mejor práctica de la industria. BT y/o EE podrán revisar las soluciones de almacenamiento protegido y de encriptación periódicamente para asegurar que son adecuadas y apropiadas.

7. Autenticación de clientes

7.1 El Proveedor debe asegurar que existe un proceso definido y aprobado de autenticación de clientes para las llamadas entrantes y salientes.[13]

7.2 El Proveedor debe asegurar que los números de identificación personal (PIN) o las contraseñas utilizados por los clientes para autenticar su identidad no están visibles a otros empleados del centro de contacto, por ejemplo, a través del uso de pantallas de PC protegidas o de separación física.

7.3 El Proveedor debe asegurar que está automatizada la autenticación de clientes de manera tal que no requiera que estos revelen el PIN o la contraseña completos al asesor; por ejemplo, a través de la solicitud generada por el sistema de ciertos dígitos o letras de la contraseña (el primero, el tercero y el quinto). BT y/o EE podrán revisar el proceso de autenticación de clientes periódicamente para garantizar que se cumple con estos Requerimientos.

7.4 El Proveedor debe asegurar que, cuando el cliente haya olvidado su PIN o contraseña y necesite restablecerlos, no podrá hacerlo hasta que haya pasado correctamente otras verificaciones de autenticación.[14]

7.5 El Proveedor debe asegurar que los sistemas para establecer los PIN o contraseñas de los clientes son automáticos y no requieren la intervención de un empleado del centro de contacto.

7.6 El Proveedor debe asegurar que los PIN o las contraseñas son creados por un sistema automatizado y que los PIN o las contraseñas nuevos son enviados directamente a los clientes por texto o correo electrónico sin la necesidad de que intervenga un asesor.

7.7 El Proveedor debe asegurar que los clientes pueden restablecer la contraseña o el PIN de una cuenta online o por medio de un sistema de Respuesta de Voz Interactiva (IVR).

7.8 El Proveedor debe asegurar que existe un recurso de "restablecimiento con asistencia de un empleado" que permita contar con la ayuda de un empleado del centro de contacto para el restablecimiento. La capacidad de restablecer el PIN o la contraseña debe restringirse a un número limitado de empleados.[15]

7.9 El Proveedor debe poder producir, cuando se lo soliciten, una pista de auditoría que muestre los restablecimientos de PIN y contraseñas de los clientes, así como el sistema utilizado para realizarlo (online, IVR o asistencia de un empleado) y qué empleado participó de la acción.

[13] Ver ejemplos de lo que implica el proceso de autenticación de clientes en la Matriz de Implementación.
[14] Ver ejemplos de lo que implican otras verificaciones de autenticación en la Matriz de Implementación.
[15] Ver ejemplos de lo que debe incorporar un recurso de restablecimiento con asistencia de un empleado en la Matriz de Implementación.

8. Privacidad de los datos

Además de la capacitación obligatoria en Protección de Datos y Seguridad de BT (ver Anexo 2) que todos los empleados del Proveedor deben completar y manifestar que han comprendido, se debe cumplir con lo siguiente:

8.1 El Proveedor debe asegurar que los empleados dentro del área del centro de contacto tiene fácil acceso a la información pertinente y aplicable sobre protección de datos y seguridad, en la primera página de la página de inicio de su intranet (o en caso de que no tengan intranet, por capacitaciones y actualizaciones por correo electrónico regulares).

8.2 El Proveedor debe enviar recordatorios regularmente, al menos dos veces al año, a todos los empleados dentro del área del centro de contacto para reforzar las conductas positivas y acompañar las mejores prácticas en seguridad.

9. Monitoreo

9.1 El Proveedor debe procurar que los supervisores o gerentes realicen una 'verificación de calidad' sobre una selección aleatoria de llamadas telefónicas con los clientes (entrantes y salientes) cada semana, con lo que se garantiza -entre otros Requerimientos- que se ha seguido el proceso correcto de autenticación del cliente.[16]

9.2 El Proveedor debe asegurar que las llamadas son consideradas como "fallidas" si no se siguió el proceso correcto de autenticación del cliente. Después de cada llamada fallida, el Proveedor debe comenzar un proceso de feedback para recordar a los asesores del centro de contacto que su responsabilidad es autenticar a los clientes correctamente y/o mantener las contraseñas seguras (según sea el caso).

9.3 El Proveedor debe contar con un proceso auditable en caso de que un empleado del centro de contacto tenga llamadas fallidas en forma repetida y no logre llevar adelante el proceso correcto de autenticación de los clientes. Esto debe incluir las consecuencias de que un asesor no siga el proceso correcto de autenticación de clientes o el mantenimiento correcto de registro en repetidas ocasiones así como la mención de que esto podría utilizarse como prueba en los procedimientos disciplinarios o de gestión del rendimiento de los individuos correspondientes.

10. Cumplimiento

10.1 El Proveedor debe asegurar que cuenta con un proceso auditable documentado para realizar y gestionar verificaciones regulares de cumplimiento con las normas de seguridad del emplazamiento y/o verificaciones sorpresa para verificar que se esté cumpliendo con este estándar y los Requerimientos de Seguridad de BT; por ejemplo, recorrer el piso, escritorio limpio, etc.[17]

10.2 El Proveedor debe implementar un proceso que asegure que se realizan revisiones trimestrales basadas en pruebas (con el 10% del cupo) de los empleados del centro de contacto o de cualquier individuo que trabaja por contracto con BT y/o EE para garantizar que

[16] Ver ejemplos de lo que debe incluir una verificación de calidad como mínimo en la Matriz de Implementación.
[17] Ver ejemplos de lo que debería incluir en las verificaciones sorpresa de cumplimiento en la Matriz de Implementación.

se hayan completado la capacitación en seguridad y el proceso de averiguación de antecedentes previa al empleo (como parte del proceso de inducción) y que funcionan con eficacia. Con esto, se garantiza que se han corroborado adecuadamente los antecedentes de los empleados que trabajan en el área del centro de contacto (en conjunción con la política de averiguación previa al empleo de BT) y de que ellos han recibido capacitación en seguridad para tener la tranquilidad de que la información sensible de los clientes está bien protegida.

10.3 El Proveedor debe implementar un proceso que asegure que se realizan revisiones trimestrales basadas en pruebas (con el 100% del cupo) de los empleados del centro de contacto o de cualquier individuo que trabaja por contracto con BT y/o EE para garantizar que se hayan completado la capacitación anual y obligatoria en Protección de Datos y Seguridad.

10.4 El Proveedor debe asegurar que se realizan sesiones informativas trimestrales de repaso de las obligaciones de los empleados en materia de Protección de Datos y Seguridad; se debe documentar prueba de la participación y comprensión de los empleados.

10.5 El Proveedor debe asegurar que los empleados del centro de contacto tienen a disposición las políticas, los estándares, las guías y los procesos correspondientes para asegurar que se cumple con este estándar y con los Requerimientos de Seguridad de BT.

11. Evaluación de los riesgos

El Proveedor debe asegurar que evalúa los riesgos de incumplimientos, autorizaciones o excepciones específicas de estos requerimientos y los documenta de acuerdo con el proceso de gestión de riesgos. La evaluación de los riesgos debe incluir lo siguiente:

- Motivos por los cuales se requiere la actividad y por qué se justifica el incumplimiento de estos Requerimientos;
- Estado de un incumplimiento; por ejemplo, permanente o temporario;
- si es temporario, la fecha para la cual implementarán los controles y la fecha en que se completará la actividad;
- Función o puesto de los individuos y por qué la actividad es apropiada para tal puesto (y por qué se excluyó del cumplimiento con controles);
- Controles de mitigación vigentes para minimizar los riesgos que surgen de la actividad;
- Justificación de la implementación de ciertos controles y/o la falta de implementación de los controles necesarios;
- Prueba de Aprobación de un Gerente Senior.

12. Glosario

Término	Explicación
Centro de Contacto con el Cliente	Un centro de contacto (también llamado "centro de contacto electrónico" o "centro de interacción con el cliente") es un punto central en una empresa desde el cual se gestionan todos los contactos con los clientes. El centro de contacto típico incluye un centro de llamadas online o más, pero también podría incluir otros tipos de contactos con los clientes, como ser boletines informativos por correo electrónico, catálogos por correo postal, consultas y chats por el sitio web, así como la recolección de información de los clientes durante las compras

	en la tienda. Un centro de contacto es generalmente parte de sistema general de gestión de las relaciones con los clientes (CRM) de una empresa.
Casilleros Designados	El personal que trabaja en el área del centro de contacto no tiene permitido tener encima efectos personales que puedan grabar información de los clientes, tales como teléfonos móviles, en sus estaciones de trabajo. Estos deben quedar guardados bajo llave en casilleros designados (identificados como tal) fuera del área del centro de contacto.
Empleado	Se entiende por "empleado" todo individuo que trabaja dentro del área del centro de contacto, incluidos los empleados permanentes y temporarios del Proveedor, el personal de agencia, contratistas y trabajadores.
Acompañado	Debe existir un proceso formal de tratamiento de los visitantes que asegure, como mínimo, que los visitantes a los centros de contacto estén acompañados en todo momento, para evitar que se pierdan o que deambulen en áreas donde les está prohibido estar.
Matriz de Implementación	La matriz adjunta que establece, como mínimo, los resultados y estándares que debe alcanzar el Proveedor a la hora de implementar ciertos procesos, políticas o procedimientos que se mencionan en estos Requerimientos.
Trabajo sin supervisión directa	Debe existir un proceso que asegure que le prohíba a un individuo que trabaja dentro del área del centro de contacto fuera del horario laboral normal permanecer sin autorización de la gerencia. Esto incluye al personal de limpieza y otros individuos ajenos a la empresa, como ser el personal de mantenimiento.
Aplicaciones de Microsoft Office	Esta categoría incluye, pero no se limita a, Word, PowerPoint, Excel, Outlook y OneNote. Para evitar que se filtren datos fuera de la empresa, las interacciones con los clientes que sucedan por sistemas online no deben registrarse en estas aplicaciones (a menos que sea autorizado) ya que es sencillo copiar y extraer información de estas aplicaciones.
Efectos Personales	Todos los efectos personales que puedan utilizarse para captar, registrar o grabar información sobre los clientes; esto incluye, pero no se limita a, teléfonos celulares, teléfonos inteligentes, iPods, iPads, cámaras, unidades flash USB, lapiceras y papel.
Controles de Acceso Físicos	Los controles de acceso físicos utilizados dependerán del área del centro de contacto donde estén localizados. Pueden ser de corte técnico (por ejemplo, tarjeta con cinta magnética, teclado, biometría) o procesal (por ejemplo, claves con un proceso auditable de finalización de sesión o un proceso de inicio de sesión en que la persona que controla el acceso verifica la identificación). Sin embargo, los controles de acceso físicos utilizados deben ser apropiados para la zona.
Activo Físico	A los fines de este documento, será todo activo capaz de procesar o almacenar datos o información sobre los clientes.
Separado físicamente	A los fines de este documento, significará que las conversaciones no pueden ser escuchadas y la información no puede ser vista desde otras áreas de negocios.

	Debe instalarse una barrera física (pared, un edificio separado, etc.) con controles físicos que rijan la entrada al área.
Incidente de Seguridad	Un incidente de seguridad es un cambio en las operaciones de rutina que impacta en la confiabilidad, integridad o disponibilidad de los activos de información, lo cual indica que podría haber ocurrido una violación a la política, la norma o el requerimiento de seguridad, o bien que podría haber fallado una salvaguardia. Estos son algunos ejemplos: mal uso del sistema, acceso no autorizado, equipo perdido o robado e infección con malware.
Aprobación de un Gerente Senior	Siempre que sea necesaria la conformidad sobre una excepción a estos requerimientos, debe analizarse el riesgo que imponen las circunstancias y la persona encargada de la aprobación deberá ser quien tenga la responsabilidad por la gestión del área funcional, con la autoridad requerida.
Propietario del Sistema	Significa el oficial responsable por el proceso general de compra, desarrollo, integración, modificación u operación y mantenimiento de un sistema de información.
Amontonamiento	La acción de seguir a otro o permitir a un individuo no autorizado acceder por un una puerta o barrera controlada o reja a un área; no usar el pase de seguridad propio para acceder a un área autorizada de las instalaciones de los proveedores utilizadas para contratos con BT/EE.
Pases de Seguridad Temporarios	Deben emitirse como parte de un proceso auditable (como ser un cuaderno, registro o planilla). Todas las emisiones de estos pases deben registrarse con la fecha, el nombre, el departamento, el número de contacto y el motivo de la emisión, así como el nombre del invitado y la fecha de devolución del pase temporario. Debe existir un proceso para las tarjetas que no se han devuelto.
Identificación del Usuario	Las impresoras y las máquinas de fax ubicadas dentro del área del centro de contacto deben requerir que el usuario ingrese su identificación única y un código de seguridad para permitir monitorear el uso por parte de los usuarios individuales. Además, los empleados deben ingresar su identificación única al acceder a las cuentas o los registros de los clientes de acuerdo con la sección 5.1.

PROYECTO KITE: Matriz de Implementación de los Requerimientos del Centro de Contacto con los Clientes

Ref. de progr.	Descripción general	Resultados mínimos para considerarse en conformidad.
1.2	Proceso auditable de acceso	Una planilla o un registro de nombres, que incluya detalles sobre cuándo se dio acceso, la lógica que llevó a ese permiso, la fecha en que se retiró el acceso y los motivos para hacerlo.
2.1	Reconocimiento fácil	El personal con permiso para usar teléfonos celulares, laptops, iPads, tablets, etc. debido a su trabajo debe ser fácil de reconocer con métodos como un cordón de diferente color u otro método que distinga la identificación.
2.4	Registros de visitantes	Se debe registrar la siguiente información: i) nombre del individuo, ii) la organización de la que provienen, iii) fecha y hora de entrada y salida, iv) el motivo de la visita, v) el nombre de la persona que están visitando, vi) número de placa de todo vehículo que ingresa al emplazamiento, vii) número de teléfono celular de contacto, viii) el número de identificación del pase del visitante.
3.5	Emergencia personal	Debe existir un sistema que permita a la familia y los amigos de un empleado contactarlo en caso de una emergencia personal. Este sistema de contacto podría ser el uso de un número de conmutador exclusivo o el número del supervisor que pudiera usarse como punto de contacto central.
3.7	Guardado o eliminado en forma segura	A continuación se incluyen algunos ejemplos de métodos seguros de almacenamiento o eliminación para casos en que se produzcan notas como parte del trabajo de un empleado, pero la lista no se limita a estos: el uso de trituradores de papel, cesto de residuos confidenciales (y potencialmente guardados bajo llave) y/o almacenamiento en instalaciones permitidas que pudieran ser cerradas con llave por los empleados.
3.7	Política de Escritorio Limpio	Todos los materiales deben guardarse o eliminarse en forma segura inmediatamente después de su uso y no debe quedar ningún material sobre el escritorio al final de la jornada laboral. Se deben realizar verificaciones oculares sorpresa en forma regular de los empleados y deberá haber un proceso disciplinario que sancione los incumplimientos.
3.10	Auditoría de pizarras y papel	Con respecto a los procesos mencionados en la sección 3, se debe mantener un registro (en un formulario como ser una planilla de cálculo) que dé cuenta de que se están realizando tales verificaciones y de que se están cumplimiento los requerimientos.

4.1	Pantallas de PC protegidas	No debe ser posible visualizar las pantallas de los asesores dentro del entorno del centro de contacto, ni tampoco que personas que están en el centro de contacto y no tengan los privilegios para leer la información puedan hacerlo (tales como el personal de limpieza y de mantenimiento). Los datos de los clientes que están en las computadoras deben mantenerse ocultos colocando el monitor de manera que no se vean o usando pantallas de privacidad.
4.6	Inventario de Activos Físicos	Debe mantenerse un inventario de todos los Activos Físicos y otros elementos asignados a individuos, como ser pases de seguridad, claves para casilleros, laptops, escritorios o tokens para acceso remoto con fines de auditoría. Cuando un asesor deja el empleo o se transfiere del centro de contacto, debe haber procesos que garanticen que se toman medidas inmediatas para retirar todos los accesos lógicos y físicos, y recuperar los Activos Físicos, claves y pases de seguridad. Esto debe estar ser parte de una Lista de Verificación que utilizar cuando culmina el empleo de algún empleado.
4.7	Requerimientos de eliminación segura	Cuando se eliminan los Activos Físicos al final de su vida útil, debe usarse un software de propiedad como 'Tabernus' o 'Blanco', para garantizar que se ha borrado toda información confidencial o de los clientes del equipo en forma permanente (donde corresponda), y a un nivel aprobado por BT y/o EE. Si no se logra la eliminación segura de los datos usando este software, el equipo deberá pasar un proceso de destrucción segura siguiendo un procedimiento aprobado por BT y/o EE. El contacto de seguridad de BT y/o EE puede asistir en esta área. Una vez que la información confidencial o del cliente ha sido eliminada, los Activos Físicos pueden volver a utilizarse en otra parte, o bien pasarse a retiro, según corresponda.
5.5	Herramientas de acceso remoto	Para evitar el acceso no autorizado a los datos de los clientes, deben implementarse procesos formales que garanticen que solo las herramientas de acceso remoto que han sido aprobadas previamente por BT y/o EE sean capaces de acceder a los dispositivos del cliente. Deben implantarse soluciones que identifiquen herramientas de acceso remoto no aprobadas y deben revisarse regularmente para asegurar que no se puedan usar o que no se han usado herramientas no aprobadas. Por otro lado, el uso de herramientas de acceso remoto aprobadas debe limitarse a individuos autorizados; esas personas solo obtendrán autorización a través de un proceso formal, que incorpora una evaluación de los riesgos de necesitar acceso remoto.
6.1	Transmisión de grabaciones de llamadas	Es esencial encriptar las grabaciones de las llamadas con los clientes que se transfieren desde las PC hacia los servidores de grabaciones; tal encriptación debe

		incluir tanto las grabaciones de voz como los detalles en la pantalla.
7.1	Autenticación de clientes	Todos los asesores deben seguir el proceso de autenticación de clientes tal como fue aprobado por BT/EE para asegurar que los clientes son quienes dicen ser. Ese proceso debe estar claro para los Proveedores y los asesores, y podría diferir según las funciones que brinda el centro de contacto.
7.4	Otras verificaciones de autenticación	Los asesores deben asegurar que, antes de proceder al cambio del PIN o la contraseña de los clientes, deben además confirmar suficiente información del cliente hasta que tengan la tranquilidad de que quien llama es la persona que dice ser por medio de preguntas de seguridad sobre su identidad más allá de su nombre y dirección: por ejemplo, alguna actividad reciente que se registre en la cuenta, la suma de la última cuenta o el tiempo que lleva siendo clientes de BT o EE. No obstante, estos son solo ejemplos y esta lista no es exhaustiva.
7.8	Restablecimiento con asistencia de un empleado	Para los clientes que no pueden restablecer su PIN o contraseña online o por IVR, debe ser posible hacerlo con la asistencia de un empleado del centro de llamadas. Sin embargo, debe haber un proceso formal que asegure que el recurso de restablecimiento con asistencia de un empleado esté limitado a un cierto número de individuos, y que existen las salvaguardias para que los empleados con la facultad de restablecer PIN o contraseñas de clientes estén físicamente separados de los demás en el control de contacto con los controles apropiados. La lista de quienes pueden aprobar esta acción debe revisarse en forma regular para asegurar que tal aprobación todavía se requiere y se utiliza con la discreción que corresponde.
9.1	Verificación de calidad en monitoreo de las llamadas	Los gerentes deben realizar verificaciones de calidad, que incluyen el monitoreo semanal de una selección aleatoria de llamadas telefónicas con clientes (entrantes y salientes) que atienden los asesores, y una revisión mensual de todos los registros y procesos implementados por el Proveedor. Esto debe servir para que el Proveedor cumpla con estos Requerimientos y, en particular, que los empleados estén usando el proceso correcto de autenticación de clientes y manteniendo los registros correctos.
10.1	Verificaciones sorpresa de cumplimento	Debe implantarse un proceso auditable para realizar y gestionar comprobaciones locales de cumplimiento con las normas de seguridad en el emplazamiento y otras verificaciones sorpresa de cumplimiento de todos los Requerimientos. Así como es obligatorio para el Proveedor realizar tales verificaciones, BT y/o EE podrá también realizar verificaciones sorpresa de cumplimiento en cualquier momento.

		Las verificaciones sorpresa deben incluir, pero no limitarse a, lo siguiente: • Identificación de seguridad o pases de seguridad • Escritorio o pantalla limpios • Uso de casilleros personales • Dispositivos móviles personales • Uso de pizarras • Retiro y eliminación de información confidencial impresa o transmitida por fax • Autenticación de clientes • Verificaciones de calidad en monitoreo de las llamadas • Pistas de auditoría sobre restablecimiento de contraseñas • Uso de mensajes de texto • Cumplimiento de lo establecido en materia de capacitación en protección de datos y seguridad Todas las auditorías de las verificaciones sorpresa deben incluir detalles de las medidas que se van a tomar donde se detecten discrepancias o incumplimientos. Se debe realizar el seguimiento de todos los planes de remediación solicitados por BT y/o EE hasta que estén completos.