Santander Global Technology, S.L.

Reporte de los controles de la Organización de Servicios relacionados con los principios de Seguridad, Disponibilidad, Integridad y Confidencialidad (SOC 2) para los Controles Generales de Tecnología de Información relacionados con el servicio de gestión de infraestructura tecnológica de Banco Santander Perú y Edpyme Santander Consumo Perú por el período comprendido del 1 de enero de 2019 al 31 de diciembre de 2019 e Informe de los auditores de servicio independientes.

Índice

Resumen Ejecutivo

Resumen Ejecutivo

Santander Global Technology	
Alcance	Seguridad, Disponibilidad y Confidencialidad de la Información
Periodo de revisión	Del 01 de Enero al 31 de Diciembre del 2019
Principios aplicables	Trust Services de Seguridad, Disponibilidad, Integridad y Confidencialidad
Localidades	Banco Santander Perú y Banco Consumer Perú
SubOrganización de Servicio	No existen suborganizaciones de servicio
Opinión	No Calificada
Excepciones Identificadas	SS5.1.10: Identificamos un usuario de proceso el cual no se encontraba en la GreenList. Indagamos sobre el usuario y detectamos que este es un usuario que fue eliminado de la GreenList debido a que el aplicativo que lo usa, Bladelogic, está en proceso de ser removido por la entidad, por lo cual el usuario se eliminó en preparación al decomiso de la aplicación mencionada, sin embargo, se identificó que el acceso de administrador de este usuario es adecuado. Adicionalmente, en caso de que un usuario con permisos de administrador no se encontrara en la GreenList, esto sería detectado por medio del control de User Access Review. Para remediar este punto, la compañía agregó al usuario a la GreenList, mientras la aplicación Bladelogic es eliminada.
Controles Complementarios	Las entidades usuarias proveen • Configuración y resguardo de los respaldos. • Autorización para implementar los cambios • Autorización para el ABC de usuarios (físicos y lógicos) • Vo.Bo. antes del cierre de los tickets de soporte

Sección I:
Informe de los Auditores de Servicio Independientes

Deloitte Asesoría en Riesgos, S.C.

Paseo de la Reforma 505, piso 28,
col. Cuauhtémoc, 06500,
Cuauhtémoc, CDMX.

Sección I: Informe de los Auditores de Servicio Independientes

A la administración de Santander Global Technology, S.L:

Alcance

Hemos examinado la descripción adjunta de los controles generales de TI de la organización de servicios Santander Global Technology, S.L. ("SGT") relacionado con la seguridad, disponibilidad y confidencialidad del servicio de gestión de infraestructura tecnológica para procesar las transacciones de Banco Santander Perú y Edpyme Santander Consumo Perú para el período comprendido entre el 1 de enero al 31 de diciembre de 2019 (la "Descripción") basada en los criterios para una descripción del sistema de una organización de servicios establecidos en DC, por sus siglas en inglés, sección 200, 2018 Criterios de Descripción para una Descripción del Sistema de una Organización de Servicios en un Informe SOC 2® ("criterios de descripción) y la idoneidad del diseño y efectividad operativa de los controles establecidos en la Descripción a lo largo del periodo del 1 de enero al 31 de diciembre de 2019 para proporcionar certeza razonable de que los compromisos de servicio y los requisitos de controles generales de TI de SGT fueron alcanzados con base en los criterios de los servicios de confianza relevantes para: seguridad, disponibilidad y confidencialidad ("criterios de servicios de confianza aplicables") establecidos en TSP, por sus siglas en inglés, sección 100, 2017 Criterios de servicios de confianza para Seguridad, Disponibilidad, Integridad de procesamiento, Confidencialidad y Privacidad.

La Descripción indica que ciertos objetivos de control definidos en la Descripción pueden lograrse únicamente si los controles complementarios llevados a cabo por las entidades usuarias contemplados en el diseño de los controles de SGT son diseñados adecuadamente y operan efectivamente en conjunto con los controles relacionados de la Organización de Servicio. Nuestra revisión no se extendió a los controles de las entidades usuarias o sus funciones y no hemos evaluado el diseño adecuado y eficacia operativa de dichos controles complementarios.

Responsabilidades de la Organización de Servicio

Santander Global Technology S.L. es responsable de sus compromisos de servicio y requisitos del sistema y de diseñar, implementar y operar controles efectivos dentro del sistema para proporcionar una garantía razonable de que se cumplieron los compromisos de servicio y los requisitos del sistema de Santander Global Technology S.L.

En la sección II: Aseveración de la Administración, SGT ha proporcionado la aseveración acerca de la razonabilidad de la presentación de la descripción y, el adecuado diseño y eficacia operativa de los controles para lograr los objetivos de control indicados en la descripción. SGT es responsable de preparar la descripción y de la aseveración, incluyendo su integridad, exactitud y el método de presentación de estas, proporcionar los servicios cubiertos en la descripción, especificar los objetivos de control e indicarlos en la descripción, identificar los riesgos que amenazan el logro de los objetivos de control, seleccionar los criterios y diseñar, implementar y documentar los controles que están diseñados adecuadamente y operan efectivamente para lograr los objetivos de control relacionados indicados en la Descripción.

Responsabilidades del Auditor de Servicio

Nuestra responsabilidad consiste en expresar una opinión sobre la Descripción y sobre el adecuado diseño y eficacia operativa de los controles para lograr los objetivos de control relacionados e indicados en la Descripción, basados en nuestro examen. Nuestro examen ha sido realizado de acuerdo con las normas para atestiguar establecidas por el Instituto Americano de Contadores Públicos Certificados ("AICPA" por sus siglas en inglés). Dichas normas requieren que planifiquemos y realicemos el examen para obtener una seguridad razonable de que, en todos los aspectos materiales, la Descripción esta presentada razonablemente y los controles fueron diseñados adecuadamente y operaran efectivamente para alcanzar los objetivos de control relacionados e indicados en la Descripción durante el periodo comprendido del 1 de enero al 31 de diciembre del 2019. Consideramos que la evidencia obtenida es suficiente y apropiada para proporcionar una base razonable para nuestra opinión.

El examen de la Descripción del sistema de la Organización de Servicio y la idoneidad del diseño e implementación de los controles implica:

- Obtener una comprensión del sistema y los compromisos de servicio y los requisitos del sistema de la organización de servicios.
- Evaluar los riesgos de que la descripción no sea razonablemente presentada y de que los controles no sean diseñados adecuadamente o no operen efectivamente para lograr los objetivos de control relacionados establecidos en la Descripción.
- Realizar procedimientos para obtener evidencia sobre si la descripción se presenta de acuerdo con los criterios de descripción.
- Realizar procedimientos para obtener evidencia sobre si los controles establecidos en la descripción fueron diseñados adecuadamente para proporcionar una seguridad razonable de que la organización de servicio cumplió con sus compromisos de servicio y los requisitos del sistema con base en los criterios de servicios de confianza aplicables.
- Probar la eficacia operativa de esos controles establecidos en la descripción para proporcionar una seguridad razonable de que la organización de servicio cumplió con sus compromisos de servicio y los requisitos del sistema con base en los criterios de servicios de confianza aplicables.
- Evaluar la presentación general de la Descripción, lo adecuado de los objetivos de control indicados en ella y lo adecuado de los criterios especificados por la organización de servicios en su aseveración.

Nuestro examen también incluyó la realización de otros procedimientos que consideramos necesarios de acuerdo a las circunstancias.

Limitaciones Inherentes

La Descripción está preparada para satisfacer las necesidades comunes de una amplia gama de usuarios de informes y, por lo tanto, puede no incluir todos los aspectos del sistema que los usuarios de manera individual consideren importantes para satisfacer sus necesidades de información. Existen limitaciones inherentes en la efectividad de cualquier sistema de control interno, incluida la posibilidad de error humano y la elusión de los controles. Debido a su naturaleza, es posible que los controles no siempre funcionen de manera efectiva para proporcionar una seguridad razonable de que los compromisos de servicio y los requisitos del sistema de la Organización de Servicio se cumplan de acuerdo con los criterios de servicios de confianza aplicables. Además, la proyección hacia el futuro de cualquier conclusión sobre la idoneidad del diseño o la efectividad operativa de los controles está sujeta al riesgo de que los controles puedan volverse inadecuados debido a cambios en las condiciones o que el grado de cumplimiento de las políticas o procedimientos puede deteriorarse.

Descripción de las pruebas de controles

Los controles específicos que probamos y la naturaleza, oportunidad y resultados de nuestras pruebas se presentan en la Sección IV de nuestro informe titulada "Descripción de la prueba de controles y sus resultados".

Opinión

En nuestra opinión, en todos los aspectos importantes, basados en los criterios descritos en la Aseveración de SGT en la Sección II.

a. La descripción presenta razonablemente los controles generales de TI de la organización de servicios relacionados con el servicio de gestión de infraestructura tecnológica como fueron diseñados e implementados, durante el período del 1° de enero de 2019 al 31 de diciembre del 2019.

b. Los controles indicados en la descripción se diseñaron adecuadamente durante todo el periodo del del 1° de enero de 2019 al 31 de diciembre del 2019 para proporcionar una seguridad razonable de que los compromisos de servicio y los requisitos del sistema de Santander Global Technology S.L. se cumplirían según los criterios de servicios de confianza aplicables. Nuestra revisión no se extendió a los controles de las entidades usuarias o sus funciones y no hemos evaluado el diseño adecuado y eficacia operativa de dichos controles complementarios.

c. Los controles establecidos en la descripción funcionaron de manera efectiva durante todo el período del 1° de enero de 2019 al 31 de diciembre del 2019, para proporcionar una seguridad razonable de que los compromisos de servicio y los requisitos del sistema de Santander Global Technology S.L. se lograron con base en los criterios de servicios de confianza aplicables. Nuestra revisión no se extendió a los controles de las entidades usuarias o sus funciones y no hemos evaluado el diseño adecuado y eficacia operativa de dichos controles complementarios.

Uso Restringido

Este informe, incluyendo la descripción de las pruebas de los controles y los resultados de los mismos en la Sección IV, está destinado únicamente a la información y el uso de la Organización de Servicio, las entidades usuarias del sistema de la Organización de Servicio durante parte o la totalidad del periodo del 1 de enero al 31 de diciembre de 2019, los socios comerciales de la Organización de Servicio que están sujetos a los riesgos derivados de las interacciones con el sistema de la Organización de Servicio, los profesionales que prestan servicios a dichas entidades usuarias y socios comerciales , posibles entidades usuarias y socios comerciales, y reguladores que tienen suficiente conocimiento y comprensión de lo siguiente:

- La naturaleza del servicio prestado por la Organización de Servicio.
- Cómo interactúa el sistema de la Organización de Servicio con entidades usuarias, socios comerciales y otras partes.
- El control interno y sus limitaciones.
- Responsabilidades de la entidad usuaria y cómo pueden afectar la capacidad de la entidad usuaria de emplear de manera efectiva los servicios de la Organización de Servicio.
- Los criterios aplicables de los servicios de confianza.
- Los riesgos que pueden amenazar el cumplimiento de los compromisos de servicio y los requisitos del sistema de la Organización de Servicio y cómo los controles abordan esos riesgos.

Este informe no está destinado a ser, y no debe ser, utilizado por nadie más que estas partes especificadas.

Deloitte Asesoría en Riesgos, S.C.
Miembro de Deloitte and Touche Tohmatsu Limited

C.P.C. José González Saravia Calderón
10 de junio de 2020

Sección II:
Aseveración de la Administración

Sección II: Aseveración de la Administración Santander Global Technology, S.L

27 de Abril de 2020

Deloitte

Deloitte Asesoría en Riesgos, S.C.
Avenida Paseo de la Reforma 505,
Cuauhtémoc, Cuauhtémoc, 06500 CDMX

Hemos preparado la descripción de los Controles Generales de TI de la organización de servicios Santander Global Technology, S.L. ("**SGT**") durante todo el período del 1 de enero al 31 de diciembre de 2019, el "período", relacionado con el hospedaje del sistema y los servicios de soporte en los centros de datos, basado en los criterios de los puntos (1) (a) - (b) a continuación, que son los criterios para una descripción del sistema de una organización de servicios en DC, por sus siglas en inglés, Sección 200, 2018 Criterios de Descripción para la Descripción del Sistema de una Organización de Servicio en un informe SOC 2® ("criterios de descripción"). La Descripción está destinada a proporcionar a los usuarios información sobre nuestro sistema que pueda ser útil al evaluar los riesgos derivados de las interacciones con el sistema de la Organización de Servicio, particularmente información sobre los controles del sistema que la Organización de servicio ha diseñado, implementado y operado para proporcionar un aseguramiento razonable de que sus compromisos de servicio y los requisitos de los Controles Generales de TI se lograron con base en los criterios de servicios de confianza relevantes para el alcance: seguridad, disponibilidad y confidencialidad, ("criterios de servicios de confianza aplicables"), establecidos en la Sección 100 del TSP, por sus siglas en inglés, 2017 Criterios de Servicios de Confianza para Seguridad, Disponibilidad, Integridad de Procesamiento, Confidencialidad y Privacidad.

Confirmamos a nuestro leal saber y entender, que:

a. La Descripción presenta el sistema de la Organización de Servicio que fue diseñado e implementado durante todo el período del 1 de enero al 31 de diciembre de 2019 de acuerdo con los criterios de descripción.

b. Los controles establecidos en la Descripción se diseñaron adecuadamente durante todo el período del 1 de enero al 31 de diciembre de 2019, para proporcionar una seguridad razonable de que los compromisos de servicio y los requisitos del sistema de la Organización de Servicio se cumplirían en función de los criterios de servicios de confianza aplicables, si los controles funcionaron de manera efectiva durante ese período y si las entidades usuarias aplicaron los controles complementarios asumidos en el diseño de los controles de la Organización de Servicio durante ese período.

c. Los controles establecidos en la Descripción funcionaron de manera efectiva durante todo el período del 1 de enero al 31 de diciembre de 2019, para proporcionar una seguridad razonable de que los compromisos de servicio y los requisitos del sistema de la Organización de Servicio se lograron con base en los criterios de servicios de confianza aplicables, si los controles complementarios de la entidad usuaria asumidos en el diseño de los controles de la Organización de Servicio operaron efectivamente durante ese período.

Sección III:
Descripción del Sistema

Sección III: Descripción proporcionada por Santander Global Technology, S.L.

Antecedentes

Aplicabilidad y propósito del Informe

El propósito de este informe es dar una opinión acerca de los controles relacionados a los principios de Seguridad, Disponibilidad y Confidencialidad de SGT cliente y ("SGT"), relacionados a los servicios de hospedaje y soporte de infraestructura de los datos para el período del 1 de enero al 31 de diciembre de 2019. La descripción del sistema y los controles asociados están destinados a cumplir los criterios para los principios de Seguridad, Disponibilidad y Confidencialidad.

Controles Complementarios de las Entidades Usuarias

Las entidades usuarias son responsables de establecer su propio sistema de control interno y aplicar esos controles dentro de su entorno. No es factible que todos los criterios de los servicios de confianza sean alcanzados únicamente por SGT. Esta sección resalta los controles complementarios de la entidad de usuario que la administración de SGT cree que deberían estar presentes para cada entidad usuaria.

Las entidades usuarias deben revisar los controles de entidad de usuario complementarios y su importancia para cumplir los criterios aplicables de los servicios con los que se relacionan.

Las entidades usuarias son responsables de implementar y mantener controles internos efectivos que se extiendan más allá de los cubiertos en este informe, incluidos, entre otros, los siguientes.

Panorama General de Operaciones

SGT, antes Produban, se dedica a proporcionar servicios para la gestión de la infraestructura tecnológica para los bancos del Grupo Santander en todo el mundo desde 2009.

SGT es una empresa orientada a la operación de las distintas plataformas tecnológicas del Grupo Santander a nivel global, logrando su estabilidad y confianza, mediante el compromiso de ofrecer el máximo nivel de calidad en el servicio para responder satisfactoriamente a las necesidades de sus clientes.

SGT proporciona el servicio de *Hosting* en cuanto a la operación, apoyándose en su infraestructura tecnológica como *Hardware* y *Software*, así como del grupo de especialistas dedicados a dar soporte a los requerimientos del cliente, previniendo cualquier situación de emergencia que se llegue a presentar a través del establecimiento de planes de contingencia operativa.

Misión

Prestar servicios tecnológicos competitivos a las entidades del Grupo Santander.

Para ello SGT desarrollará un catálogo de servicios que permitan benchmarks con el mercado.
Estos servicios se construirán sobre una plataforma tecnológica moderna que deberá garantizar eficiencias, altos estándares de calidad y gestión excelente del riesgo operacional, todo ello en partnership con las principales compañías tecnológicas del mundo y bajo la estrategia tecnológica marcada por el Grupo Santander a través de su división corporativa de T&O.

SGT deberá ser global para aprovechar sinergias que garanticen el modelo operativo más eficiente y deberá tener presencia local en las geografías en las que presta servicio para asegurar la calidad y responder a las necesidades locales.

SGT se instrumentaliza en la forma jurídica de sociedad mercantil propiedad de la matriz del Grupo con vehículos societarios locales de SGT matriz.

Valores

- Dinamismo;
- Fortaleza;
- Liderazgo;
- Innovación;
- Orientación al cliente y calidad de servicio;
- Ética profesional y sostenibilidad.

Cambios durante el periodo

No existieron cambios relevantes en el ambiente de control, durante el periodo del 1 de enero al 31 de diciembre de 2019.

Sección IV:
Descripciones, pruebas y resultados del sistema

Sección IV: Descripciones, pruebas y resultados del sistema

Introducción

Este informe sobre los controles puestos en operación y las pruebas de efectividad operativa tiene como objetivo brindar a las partes interesadas la información suficiente para comprender los aspectos de los controles de SGT relacionados con los principios de Seguridad, Disponibilidad y Confidencialidad de los servicios de Hospedaje y de soporte en los centros de datos que puede ser relevante para los controles de una organización de usuario. Este informe, junto con una comprensión del control interno existente en las organizaciones de usuarios, tiene como objetivo ayudar en la evaluación del control interno que rodea el sistema relacionado con la seguridad, la disponibilidad y la confidencialidad de los servicios de hospedaje y soporte del sistema.

Nuestro examen estuvo restringido a los criterios aplicables de los servicios de hospedaje y soporte de centros de datos relacionados a los principios de Seguridad, Disponibilidad y Confiabilidad de la información, tomando en cuenta, las operaciones de procesamiento de datos asociadas y los controles relacionados especificados por SGT y específicamente identificados como controles y procedimientos de prueba en la Sección IV, y no se extendieron a los procedimientos vigentes en las entidades usuarias.

Es responsabilidad de cada usuario evaluar la información incluida en este informe en relación con el control interno implementado en las entidades usuarias individuales para obtener un entendimiento y evaluar el riesgo de control en las entidades usuarias. Los controles de las entidades usuarias y los controles de SGT deben ser evaluados conjuntamente. Si no existen controles eficaces de la entidad usuaria, los controles de SGT no pueden compensar tales debilidades.

Nuestra revisión se llevó a cabo conforme a lo establecido en la sección 100 del TSP, Principios, Criterios e Ilustraciones de Servicios de Confianza para Seguridad, Disponibilidad, Integridad de Procesamiento, Confidencialidad y Privacidad (AICPA, Ayudas de Práctica Técnica) (aplicable criterios de los servicios de confianza), Los controles de SGT se restringieron a los objetivos de control y actividades de control relacionados enumerados en esta Sección IV y no se extendieron a los controles descritos en la Sección III, pero no incluidos en la Sección IV, o a controles que pudieran estar en vigor en las organizaciones de usuarios.

Las descripciones de los controles son responsabilidad de la administración de SGT. Nuestra responsabilidad es expresar una opinión sobre si:

(1) La descripción presenta de manera justa, en todos los aspectos materiales, los aspectos de los controles de la Compañía A que pueden ser relevantes para el control interno de una organización usuaria.

(2) Los controles incluidos en la descripción fueron diseñados adecuadamente para cumplir con los criterios aplicables de los servicios establecidos en la descripción de la administración.

(3) Los controles incluidos en la descripción estaban funcionando efectivamente para cumplir con los criterios aplicables de los servicios.

Elementos del Entorno del Control

El entorno de control establece el tono de una organización, influyendo en la conciencia de control de su gente. Es la base para otros componentes del control interno, proporcionando disciplina y estructura. Además de las pruebas de diseño e implementación de los controles identificados por SGT, nuestros procedimientos incluyeron pruebas de los siguientes elementos relevantes del entorno de control de SGT:

a. Comunicación y aplicación de la integridad y los valores éticos
b. Compromiso con la competencia
c. Participación de los responsables de la gobernanza
d. Filosofía de la administración y estilo de operación
e. Estructura organizacional
f. Asignación de autoridad y responsabilidad
g. Políticas y prácticas de recursos humanos
h. Evaluación de riesgos
i. Información y comunicación
j. Monitoreo

Dichas pruebas incluyeron la indagación del personal de gestión, supervisión y personal apropiado; la observación de las actividades y operaciones de SGT, la inspección de los documentos y registros de SGT, y la reevaluación de la aplicación de los controles de SGT. Los resultados de estas pruebas se consideraron en la planificación de la naturaleza, el momento y el alcance de nuestras pruebas de las actividades de control descritas en esta sección.

Responsabilidad por las actividades de control

Las actividades de control enumeradas y correlacionadas con los criterios del principio de confianza AICPA para Seguridad, Disponibilidad y Confidencialidad Sección IV de este informe fueron proporcionadas por la administración de SGT. Las pruebas de diseño e implementación para los procedimientos de control son responsabilidad de Deloitte.

Descripción de los Procedimientos de Prueba Realizados

Nuestras pruebas de los controles se diseñaron para cubrir un número representativo de transacciones durante el período comprendido entre el 1 de enero al 31 de diciembre de 2019. Al determinar la naturaleza y alcance de las pruebas consideramos, (a) la naturaleza y la frecuencia de los controles que se prueban, (b) los tipos de evidencias disponibles, (c) la naturaleza de los objetivos de control a alcanzar, (d) el nivel evaluado de riesgo de control, (e) la efectividad esperada de la prueba, y (f) los resultados de nuestras pruebas del ambiente de control.

La prueba de la exactitud e integridad de la información provista por SGT, también es un componente de los procedimientos de prueba realizados. La información que utilizamos como evidencia puede haber incluido, pero no se limita a:

- Informes estándar configurados dentro del sistema
- Informes parametrizados generados por los sistemas de SGT
- Informes personalizados desarrollados que no son estándar para la aplicación
- Hojas de cálculo, que incluyen información relevante utilizada para la prueba de un control
- SGT preparó análisis, programaciones u otra evidencia preparada y utilizada manualmente por ellos.

Si bien estos procedimientos no se mencionaron específicamente en los procedimientos de prueba enumerados en esta sección, se completaron como un componente de nuestras pruebas para respaldar la evaluación de si la información es o no suficientemente precisa y detallada para los fines de probar completamente los controles identificados por SGT.

Prueba	Descripción
Indagación Corroborativa	Entrevistas detalladas con el personal pertinente para obtener evidencia de que el control estuvo en funcionamiento durante el período del informe y se acompaña de otros procedimientos que se indican a continuación y que son necesarios para corroborar la información derivada de la indagación.
Observación	Observación del desempeño del control varias veces durante el período del informe para probar la aplicación de la actividad de control específica.
Examinación de Documentación /Inspección	Si se documenta el desempeño del control, se inspeccionan los documentos e informes que indican el desempeño del control.
Reproceso de las actividades de monitoreo o controles manuales	Los documentos obtenidos utilizados en la actividad de monitoreo o actividad de control manual y de forma independiente se reprocesaron los procedimientos. Comparar los elementos de excepción identificados con los identificados por el propietario del control responsable.
Reproceso de procesamiento programado	Introducir los datos de prueba, calcular manualmente los resultados esperados y comparar los resultados reales del procesamiento con las expectativas.

Reportar los resultados de las pruebas

El concepto de materialidad no se aplica al reportar los resultados de las pruebas de los controles para los que se han identificado desviaciones, debido a que Deloitte no tiene la capacidad de determinar si una desviación será relevante para un usuario en particular. En consecuencia, Deloitte informa de todas las desviaciones identificadas durante el periodo de revisión.

Criterios y controles relacionados proporcionados por SGT, pruebas de efectividad operativa y resultados por área tópica

Organización y Gestión

Descripción de la Estructura Organizacional

Valores

SGT ha establecido una base de valores que incorpora una cultura de ética y cumplimiento. El código de conducta, y sus valores, definen las leyes y políticas relacionadas con el cumplimiento e incluye los siete valores que se entrelazan en los procesos comerciales diarios:

a. Integridad
b. Responsabilidad
c. Servicio
d. Comunicación
e. Innovación
f. Calidad
g. Gente

Estructura organizativa

Las estructuras organizativas se han definido y documentado formalmente en el organigrama de la empresa, que se evalúa y revisa según sea necesario para abordar los compromisos y requisitos cambiantes.

Prácticas de personal

SGT es un empleador con igualdad de oportunidades. Las políticas requieren que SGT no discrimine a ningún empleado o solicitante por motivos de sexo, raza, color, religión, edad, origen nacional, ciudadanía, orientación sexual, discapacidad, o por cualquier otra razón prohibida por el gobierno federal, estatal o ley local. Esta política se aplica a todas las prácticas de empleo, incluida la contratación, el empleo, la colocación, la capacitación, la promoción, la compensación, la retención y la terminación de empleados, así como a otros términos y condiciones de empleo. Los supervisores llevan a cabo evaluaciones anuales de desempeño para revisar el desempeño del personal y evaluar si el individuo continúa siendo desafiado y creciendo profesionalmente. El objetivo de SGT es garantizar que las decisiones de contratación, transferencia, promoción, compensación, disciplina y despido se basen en las calificaciones y capacidades relacionadas con el trabajo de los empleados y los solicitantes.

El área de Recursos Humanos es responsable de identificar posibles candidatos para cubrir vacantes en toda la Compañía, incluida la educación y la experiencia / conjuntos de habilidades, para todas las nuevas contrataciones. Una vez que se completa un puesto, se requieren nuevas contrataciones para completar un conjunto de criterios obligatorios de incorporación, capacitación y cumplimiento. Además, las nuevas contrataciones deben reconocer formalmente el Código de Conducta de la Compañía.

El incumplimiento de las políticas y procedimientos de SGT dará lugar a acciones disciplinarias que pueden incluir el despido. Se encuentra disponible una línea directa de ética para denunciar cualquier infracción de las políticas de SGT y del Código de conducta.

Conformidad

SGT presenta un breve resumen del programa de cumplimiento a todos los nuevos empleados y contratistas durante su periodo de capacitación, explicando los mecanismos para informar sospecha de violaciones a nuestro código de conducta,

Criterios Comunes relacionados con Seguridad, Disponibilidad, Confidencialidad e Integridad

Tabla de pruebas de soporte

ID	Control Activity	Evidence
SS1.1.2	Dentro de la intranet corporativa existe un organigrama disponible para su consulta en el cual se definen las áreas operativas y los responsables de dichas áreas.	Solicitamos evidencia del organigrama funcional de la empresa en donde se describen y clasifican los puestos de cada area, así como de su publicación dentro de la intranet corporativa disponible para su consulta.
SS2.2.2 - SS2.2.3 - SS2.3.1 - SS2.4.1	Los documentos de políticas y procedimientos (Marco Normativo) para procesos significativos están disponibles en la intranet de la entidad.	Solicitamos evidencia de la pantalla de intranet en donde se encuentren disponibles las Normas y Procedimientos para su consulta por parte del personal de la entidad, con las versiones y cambios más recientes de los documentos.
SS1.3.2	La entidad cuenta con un proceso de adaptación y capacitación para preparar a los nuevos integrantes de la fuerza laboral en el desempeño de sus actividades.	Solicitamos evidencia de la Guía de bienvenida para nuevos empleados que se otorga a cada nuevo ingreso para brindar una perspectiva general del entorno laboral y operación de la entidad.
C1.3.8 - C1.8.1 - C1.7.1	Contar con políticas y procedimientos para la administración y control de respaldos de información, que contemplen, al menos, lo siguiente: a. Identificación del tipo de información que se respalda (bases de datos, programas, datos, sistema operativo, etc.). b. El tipo de respaldo de que se trate (completo, diferencial, incremental). c. Rotación y período de retención de los dispositivos de almacenamiento (diario, semanal, mensual o anual). d. Transporte de respaldos e. Pruebas periódicas de los respaldos f. Traslado de los respaldos fuera de sitio. g. Destrucción de respaldos, así como su registro en una bitácora indicando el motivo de la destrucción, persona que lo realiza, fecha y el medio de destrucción . h. Restricción para el almacenamiento de información crítica en equipos de cómputo personales sin esquemas de respaldo. i. Mecanismos de protección de la información almacenada en los dispositivos de respaldo que eviten que personas no autorizadas tengan acceso o hagan mal uso de ella.	Se cubrió con la visita realizada al Data Center, y por cuestiones de seguridad y políticas de la empresa, no es posible compartir información correspondiente a la operación del SITE.
SS1.4.1 - SS1.4.2 - SS6.2.8	Las políticas de la entidad incluyen los códigos de conducta así como las posibles sanciones por mala conducta de los miembros de la fuerza laboral.	Solicitamos evidencia del Código General de Ética y Conducta bajo el cual se rigen los lineamientos de conducta dentro de la entidad.
SS5.1.4 - SS5.3.3 - SS5.3.5 - PI1.5.7	Políticas y procedimientos se implementan validando que la infraestructura y software se encuentran debidamente configurados con Active Directory para el inicio de sesión.	Solicitamos evidencia de capturas de pantalla de los dominios de servidores con Active Directory implementado y de las políticas aplicables para el uso de Active Directory en los inicios de sesión.
SS2.2.1	Se publica un aviso de privacidad en todos los sitios web y software disponibles públicamente de la entidad. El aviso de privacidad describe los compromisos de privacidad de la entidad.	Solicitamos evidencia del aviso de privacidad publicado en internet mismo que esta disponible para todo cliente y proveedor que se relacione con Santander Global Technology.
SS5.5.13 - SS5.2.8 - SS5.5.11	La entidad recibe las bajas de personal realizadas por parte del proveedor, esto con la finalidad de remover los accesos otorgados al personal de servicio por parte del proveedor.	Se solicitó evidencia del correo de notificación que envía el proveedor en temas de bajas de usuarios para notificar a la empresa.

ID	Control Activity	Evidence
C1.2.5 - C1.2.7	La entidad cuenta con políticas y/o procedimientos aplicables para la seguridad, clasificación y resguardo de información confidencial.	Se solicitó evidencia del documento de "Requisitos de Ciber Seguridad para Usuarios Técnicos" sobre el cual examinamos la especificación de aspectos de confidencialidad, tales como clasificación, protección, uso y responsabilidades resultantes del uso de información confidencial.
SS5.2.3 - SS5.5.1 - SS5.5.2 - SS5.5.3 - SS5.5.9 - SS5.5.10 - SS5.5.7 - SS5.5.15 - SS5.5.16	El personal de la administración cuenta con una identificación a través de una credencial que los identifica como personal administrativo y operativo para tener acceso autorizado y limitado a las instalaciones.	Solicitamos evidencia de las políticas y/o procedimientos aplicables para el uso de credencial dentro de las instalaciones. En complemento, pedimos evidencia de el escaneo del formato de credencial para validar que cuente con la información correspondiente para el acceso otorgado.
SS5.7.1	Contar con esquemas de cifrado en los enlaces de telecomunicaciones para evitar que terceros no autorizados puedan acceder a la información de la Entidad.	Solicitamos evidencia de la guía de bastionado con la que cuenta la entidad como base para la configuración de los servidores (SO) en tema de cifrado de información.
SS5.8.3	Todos los sistemas Windows en HUB_MX cuentan con protección antivirus, gestionado y actualizado automáticamente de forma centralizada.	Solicitamos evidencia de los reportes de monitoreo de parámetros de antivirus que sirven como base para el responsable de Gestión de Antivirus asegure el cumplimiento con las políticas de seguridad
SS5.2.7 - SS5.5.12 - SS5.5.14	Cuando los empleados y trabajadores temporales finalizan su periodo laboral, se realiza una notificación a Recursos Humanos de manera oportuna.	Solicitamos evidencia del Reporte de bajas diarias que se comparte por correo a Recursos Humanos
AI1.3.2	El responsable de Gestión de Continuidad publica el plan de recuperación en la Intranet corporativa (Kosmos), de tal manera que se pueda acceder aun cuando el sitio primario no se encuentre operativo.	Solicitamos evidencia de la publicación del Plan de Recuperación ante Desastres en la intranet, donde se encuentre disponible para su consulta
AI1.2.8	El responsable de Gestión de Continuidad verifica que en los contratos, OLAs (Operating Level Agreement o Acuerdo del Nivel de Operación) establecidos con el proveedor del CAT se cuenta con cláusulas de niveles de servicio que aseguran la disponibilidad de los recursos provistos por los proveedores ante la declaración de desastres.	Solicitamos evidencia de los OLA's con los que cuenta la entidad con sus proveedores CAT para la comprobación de definición de Niveles de Atención para asegurar la disponibilidad del servicio
SS3.2.3 - AI1.2.7 - AI1.3.1	El equipo de Gestión de Continuidad verifica que se ejecutan pruebas y simulacros donde se valida que las actividades contempladas en el DRP son correctas y suficientes.	Solicitamos evidencia de las pruebas y simulacros realizados en el año
AI1.2.3 - AI1.2.9	El responsable de Gestión de la Continuidad en conjunto con el cliente verifica que el alcance y la estrategia contemplados en la Carta de Alcance es adecuado y suficiente.	Solicitamos evidencia de las Cartas de Alcance que se establecieron en conjunto con el cliente de SGT, para asegurar éstas sean adecuadas y suficientes
SS1.1.1 - SS1.1.4 - SS1.1.5 - SS1.2.1 - SS2.6.6 - SS5.1.7	El nivel de privilegios de acceso a las bases de datos que respaldan las aplicaciones es revisado por la gerencia al menos una vez al año para garantizar que el acceso se restrinja adecuadamente en función de las responsabilidades del trabajo	Solicitamos evidencia de la certificación de usuarios realizada durante el año 2019, en la cual observamos que se contara con el correo de IAM enviado a los responsables de la certificación, su respuesta y la conclusión de la modificación o estado de los usuarios.

ID	Control Activity	Evidence
SS1.1.3 - SS1.2.2 - SS5.1.8 - PI1.6.2	Como parte del proceso de recertificación de accesos, las autorizaciones de acceso de los usuarios para las aplicaciones, bases de datos, sistemas operativos y las herramienta de infraestructura clave, se modifican / eliminan a tiempo y de acuerdo con las normas.	Solicitamos evidencia del reporte de certificación de usuarios y observamos que el cliente no se encuentra dentro del reporte. Sin embargo obtuvimos evidencia del proceso de baja.
SS1.3.5	El líder de proyecto da feedback al responsable o LP y solicita que entregue la información requerida con el fin de verificar que ésta se encuentre completa	De acuerdo al listado de proyectos se entregó una muestra de proyectos para solicitar la siguiente información con la finalidad de validar el cumplimiento del control: - Ticket de solicitud al proyecto - Captura de pantalla de los documentos solicitados para el proyecto (inputs) - Documento de Valoración Técnica
SS1.3.1 - SS1.4.3	El gestor del área de reclutamiento y selección de personal obtiene la aprobación de la Dirección con el fin de corroborar que la vacante se encuentre justificada	Solicitamos los correos de aprobación de las contrataciones para asegurar que éstas sean justificadas y aceptadas bajo el presupuesto de la entidad.
SS1.4.4 - SS1.4.6	El gestor de reclutamiento y selección recaba los documentos necesarios para la contratación (checklist) y consigue las firmas correspondientes en todos los documentos que integran el expediente del nuevo empleado.	Como parte de la revisión de contrataciones, solicitamos el checklist de documentos que integra el expediente del nuevo empleado, el cual asegura cumpla con los requisitos
SS3.2.1 - SS4.1.1	El Coordinador de Seguimiento actualiza las propiedades de los documentos, versión y detalle de las modificaciones solicitadas previo a su publicación con el fin de reflejar la operación vigente de la empresa.	Observamos que la compañía cuenta con un repositorio, en donde se almacenan los documentos que fueron previamente actualizados o mejorados y aprobados
SS5.5.8	Todos los visitantes deben ser escoltados por un miembro de la fuerza laboral cuando visiten las instalaciones donde el sistema sensible y los componentes del sistema se mantienen y operan.	Se cubrió con la visita realizada al Data Center, y por cuestiones de seguridad y políticas de la empresa, no es posible compartir información correspondiente a la operación del SITE.
AI1.2.1 - PI1.1.4	Contar con todos los controles y dispositivos de control ambiental instalados y operando para asegurar la operación adecuada de los equipos de procesamiento y telecomunicaciones de la Entidad. Dichos controles deberán incluir, al menos: a. Aire acondicionado b. Detectores de humo, humedad y líquidos c. Sistemas de extinción de incendios manuales o automáticos. De tratarse de extintores manuales, contar con los suficientes para cubrir la capacidad del centro de cómputo.	Se cubrió con la visita realizada al Data Center, y por cuestiones de seguridad y políticas de la empresa, no es posible compartir información correspondiente a la operación del SITE.
SS7.4.4 - SS7.4.10 - C1.1.1 - C1.2.4 - C1.3.1 - C1.3.6 - PI1.2.12 - PI1.3.6 - PI1.5.1 - PI1.5.4 - PI1.6.1 - PI1.3.2 - PI1.3.5	El Gestor de Despliegues verifica que el integrador incluya toda la documentación necesaria para llevar a cabo el despliegue solicitado. La información es registrada en la Herramienta Corporativa el cual incluye checks para cambiar de estado en caso de contar con la información requerida; en la Herramienta Corporativa pueden observarse datos como: Folio, estatus, objetivo, alcance, funcionalidad, categorización, planificación, autorización, código de cierre, entre otros. En caso de que no se cuente con toda la información necesaria para el despliegue éste es rechazado por el Gestor de Despliegues.	Solicitamos evidencia de los despliegues que fueron realizados, obteniendo así el ticket en la herramienta corporativa para la evaluación de la aprobación, planificación y ejecución de pruebas.

ID	Control Activity	Evidence
SS7.4.3 - PI1.2.6 - PI1.2.9 - PI1.2.10	El responsable de Gestión de Despliegues realiza la extracción de los despliegues registrados en la Herramienta Corporativa con el fin de generar los indicadores mensuales correspondientes a: Histórico de despliegues instalados, despliegues que generaron un incidente y despliegues no exitosos.	Solicitamos evidencia del envío del reporte de indicadores por medio de correo electrónico. Validamos además que incluya el histórico de despliegues instalados, despliegues que causaron incidentes y despliegues no exitosos.
SS5.1.2 - SS6.1.3	El SOC, Administrador de Vulnerabilidades y/o servicios de cyber seguridad contratados para tal fin, notifica las vulnerabilidades críticas que pudieran impactar a la infraestructura en la DMZ por medio de correo electrónico a las Áreas Técnicas e involucrados para la atención de las mismas.	Solicitamos evidencia de la notificación de vulnerabilidades que es enviada por el Administrador de Vulnerabilidades y/o servicios de cyber seguridad
SS7.4.5	El Administrador de Vulnerabilidades realiza el seguimiento a las vulnerabilidades críticas con las áreas involucradas para la remediación o mitigación de las vulnerabilidades hasta su cierre a través de correo electrónico añadiendo el número de ticket de atención que se generó en la herramienta corporativa de peticiones y/o cambios.	Solicitamos evidencia del seguimiento por correo o ticket, realizado después de la detección de la vulnerabilidad. En caso de que aplique, se implementan las soluciones determinadas para cada caso.
SS3.2.4	El Administrador de Vulnerabilidades notifica vía correo electrónico a la Dirección de CISO por medio de indicadores, las vulnerabilidades críticas reportadas por los distintos medios.	Solicitamos evidencia del envío de los indicadores al CISO de la entidad para el reporte de vulnerabilidades críticas
SS1.3.3 - SS2.2.4 - SS2.3.2 - C1.2.8	El asesor de Formación revisa y publica el calendario de cursos presenciales para informar las fechas, con el fin de que el participante asista puntualmente para el cumplimiento de las competencias comprometidas	Solicitamos evidencia de los cursos programados y publicados por parte del área de Formación de Personal, en donde comprobamos que estos se encuentran disponibles en la plataforma para que el personal pueda tener acceso y asistir a ellos.
SS1.3.4	El asesor de Formación realiza el reporte anual de capacitación donde se integran los resultados e indicadores que muestran anualmente cifras de las actividades de los empleados de cada área, mismos que sirven en la toma de decisiones para el desarrollo de las competencias al siguiente año	Solicitamos el Reporte Anual de Capacitación en donde observamos que la entidad plasma las cifras de capacitación para el desarrollo del personal, con el cual se apoya para la toma de decisiones
SS3.1.9	El Coordinador de la Configuración válida a través de la consulta en CMDB que la información proporcionada por el solicitante a través de una petición o por cambio se vea correctamente reflejada en CMDB.	Solicitamos evidencia de los tickets que fueron levantados para Gestión del Cambio de Infraestructura y confirmamos que para los cambios se cuenta con la descripción de la solicitud y que el cambio aplicado a CMDB coincide con ésta.
SS3.1.1	El Coordinador de Configuración revisa a través de los indicadores corporativos y locales que la infraestructura se encuentre correctamente declarada acorde al modelo actual de CMDB	Solicitamos evidencia y comprobamos que la entidad cuenta con el reporte de Indicadores Corporativos y Locales sobre la Configuración de Infraestructura, lo cual permite que se cuente con la información real sobre la infraestructura declarada y así las decisiones tomadas sean las adecuadas.
AI1.2.4 - PI1.1.1 - PI1.4.3	El analista de BackUp valida la existencia de un Vo.Bo. de Riesgo Tecnológico en ambiente de QA o Vo.Bo. de Gerencia de Backup	Solicitamos para los cambios seleccionados, que contaran con una aprobación para la restauración de backups. Verificamos también la restauración se haya efectuado después de la solicitud y que la persona que autoriza pertenezca al equipo de Backup y Restauración.
AI1.2.5 - PI1.1.2	El analista de Backup revisa diariamente y por turno que los respaldos programados hayan terminado correctamente y no se omita el reporte y seguimiento de procesos fallidos.	Obtuvimos evidencia de los respaldos identificados como 'missed' lo cual indica que no fueron finalizados adecuadamente. Solicitamos evidencia y confirmamos que todos cuentan con un seguimiento o justificación

ID	Control Activity	Evidence
SS6.2.1 - SS6.2.2 - SS6.2.4 - SS6.2.5 - PI1.3.4 - PI1.5.6	El gerente de CCS al ver que la falla no ha sido resuelta, escala al siguiente nivel de atención e informa a los niveles ejecutivos correspondientes para que se apliquen acciones que resuelvan la falla.	Solicitamos evidencia de los reportes ejecutivos que se produjeron tras la incidencia reportada, estos son entregados al cliente tras su resolución. Sin embargo no se identificaron incidentes P3 (esta clasificación representa a aquellos incidentes centrales, los cuales son los que cubre el control) dentro del periodo de revisión 2019.
SS4.1.2 - SS6.2.3 - SS6.2.7	El analista de CGS valida que no se estén generando incidentes con la misma recurrencia posterior a la aplicación de un control de cambios, comunicar al personal de Gestión de Problemas si la solución aplicada fue exitosa o ha provocado otra falla o se sigue presentando la misma falla.	No se requirió de un cambio emergente, pues no se identificaron incidentes P3 (esta clasificación representa a aquellos incidentes centrales, los cuales son los que cubre el control), dentro del periodo de revisión
SS7.2.2 - SS7.3.1	El analista de gestión de incidentes notifica la existencia de un incidente y que este debe ser solucionado a través de un cambio emergente	No se requirió de un cambio emergente, pues no se identificaron incidentes P3 (esta clasificación representa a aquellos incidentes centrales, los cuales son los que cubre el control), dentro del periodo de revisión
SS1.4.5	El Gestor de Niveles de Servicio difunde a las áreas participantes el procedimiento de acuerdo de niveles de servicio, indicando los servicios y niveles comprometidos para su conocimiento	Solicitamos como evidencia el correo donde se compartieron los niveles de servicio para cada cliente, esto para asegurar que se encuentre disponible y que los empleados formen parte de la mejora a los niveles de servicio
SS2.2.6 - SS2.3.4 - SS2.4.2 - PI1.1.7	El Gestor de Niveles de Servicio documenta en el informe de seguimiento al servicio las causas del incumplimiento o comportamiento de los servicios fuera de lo habitual.	Obtuvimos evidencia de las presentaciones de Entrega de Servicio y observamos las incidencias reportadas sobre Niveles de Servicio en donde identificamos que no se registraron incidencias P3 durante el periodo de revisión.
C1.2.6	La solicitud de acceso para las bases de datos nuevas y modificadas y para el acceso a los sistemas operativos está debidamente aprobada, documentada y ejecutada.	Solicitamos evidencia de la Green List para la confirmación de que las solicitudes hayan sido aprobadas por la administración adecuada
SS5.1.10 - PI1.6.3	La solicitud de acceso para las bases de datos nuevas y modificadas y el acceso a los sistemas operativos se revisan apropiadamente, se documentan y ejecutan en la herramienta corporativa.	Con base en la ejecución de los scripts ACTT, obtuvimos la configuración de los usuarios administradores y los identificamos en la WhiteList
AI1.2.2 - PI1.1.5 - PI1.1.6	El personal de operaciones monitorea el estado de las protecciones ambientales durante cada turno para dar mantenimiento. Se han instalado mecanismos de alerta para comunicar cualquier discrepancia en los umbrales ambientales.	Se cubrió con la visita realizada al Data Center, y por cuestiones de seguridad y políticas de la empresa, no es posible compartir información correspondiente a la operación del SITE.
C1.3.9 - C1.4.1 - C1.4.2	Grupo Gobierno y Control firma el contrato verificando que los datos se encuentren acorde a la propuesta aprobada	Solicitamos y confirmamos que para cada uno de las propuestas aprobadas se cuenta con el contrato firmado por el proveedor y por los representantes de Gobierno y Control
SS5.3.1 - SS5.2.5 - SS7.4.8	Los componentes de infraestructura de SO (Unix, Linux, Windows) y BD (BBDDs DB2 / ORACLE / SQL) se encuentran configurados acorde a las guías de bastionado	Con base en los resultados extraídos con la herramienta ACTT, revisamos distintos parámetros y confirmamos que se encuentran acorde a la guía de bastionado definida por la compañía, por lo que cuentan con los parámetros de seguridad requeridos.

ID	Control Activity	Evidence
SS5.2.2 - SS5.4.2 - SS5.5.4 - SS5.5.5 - SS5.5.6 - C1.2.3	El guardia de Seguridad Física verifica en el listado de acceso el ingreso al CPD del personal autorizado de acuerdo a las fechas y horarios señalados.	Solicitamos evidencia del listado de acceso al CPD con el que los guardias de Seguridad Física revisan el acceso autorizado de acuerdo a las fechas y horarios autorizados.
SS5.5.17 - SS5.5.18	Áreas sensibles dentro de la entidad cuenta con dispositivos físicos que se utilizan para controlar el acceso a instalaciones altamente sensibles y bajo el control de acceso de los miembros designados de la gerencia.	Se cubrió con la visita realizada al Data Center, y por cuestiones de seguridad y políticas de la empresa, no es posible compartir información correspondiente a la operación del SITE.
SS3.1.2 - SS3.1.3 - SS3.1.4 - SS3.1.5 - SS3.1.7 - SS3.1.8	El CGRT valida periódicamente el nivel de riesgo de los indicadores del proceso definidos para identificar desviaciones y, en su caso, reportarlas para definir el tratamiento que se debe dar de acuerdo a su posible impacto	Solicitamos evidencia del análisis realizado para los indicadores, en el cual además de identificarlos, son reportadas para definir acciones a tomar
SS6.2.6 - SS6.2.9 - SS7.4.1 - SS6.2.6 - SS6.2.9 - SS7.1.2 - SS7.3.2 - SS7.4.1 - SS7.4.2 - SS7.4.7	El Gestor de Cambios verifica que las áreas promotoras incluyan la documentación y/o Vo.Bo. necesarios en la herramienta para llevar a cabo el cambio de infraestructura solicitado. En caso de que no se cuente con toda la información necesaria el cambio no es autorizado por el Gestor de Cambios.	Comprobamos que para todos los cambios se cuenta con la documentación y/o VoBo para la aplicación del cambio. Por medio de correo electrónico se notifican las actividades a realizar de manera diaria, en caso de que aplique.
SS3.1.10 - SS7.1.1 - SS7.2.1 - SS7.4.9	Se dispone de indicadores de cambios, en los que se reflejan las solicitudes de cambios, tipos de cambios y los cambios aprobados y/o rechazados.	Solicitamos evidencia de los informes mensuales de Indicadores de Gestión de Cambios, en donde se plasman las solicitudes, estados y clasificación de cambios
SS6.1.1	A partir de que se detecte la necesidad, el técnico de monitoreo del área de CCS solicita la revisión de los umbrales de alertas y/o alarmas para la creación, modificación o corrección de parámetros con el fin de tener mayor tiempo de reacción.	Solicitamos evidencia de los tickets levantados al equipo de monitoreo para la creación de un nuevo monitoreo, modificación o corrección de parámetros
PI1.1.8	Para los enlaces entre las instalaciones críticas (centro de cómputo principal y alterno), sucursales y corporativos, deberán contemplarse enlaces alternos a través de diferentes proveedores o en su defecto, por medios y tecnologías distintas.	Se cubrió con la visita realizada al Data Center, y por cuestiones de seguridad y políticas de la empresa, no es posible compartir información correspondiente a la operación del SITE.

Criterios de Seguridad

Criterios Comunes relacionados con Organización y Gestión

ID	Actividad de Control	Procedimiento de Prueba	Resultado
SS1.1.1	El nivel de privilegios de acceso a las bases de datos que respaldan las aplicaciones es revisado por la gerencia al menos una vez al año para garantizar que el acceso se restrinja adecuadamente en	Solicitamos evidencia de la certificación de usuarios realizada durante el año 2019, en la cual observamos que se cuente con el correo de IAM enviado a los responsables de la certificación, su respuesta y la conclusión de la modificación o estado de los usuarios.	Sin excepciones que reportar.

ID	Actividad de Control	Procedimiento de Prueba	Resultado
	función de las responsabilidades del trabajo	**Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS1.1.1, SS1.1.4, SS1.1.5, SS1.2.1, SS2.6.6 Y SS5.1.7** **Ver tabla de pruebas de soporte.**	
SS1.1.2	Dentro de la intranet corporativa existe un organigrama disponible para su consulta en el cual se definen las áreas operativas y los responsables de dichas áreas.	Solicitamos evidencia del organigrama funcional de la empresa en donde se describen y clasifican los puestos de cada área, así como de su publicación dentro de la intranet corporativa disponible para su consulta a través de un archivo descargable. **Nota: Prueba de control se encuentra en el ID SS1.1.2.** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS1.1.3 - SS1.2.2	Como parte del proceso de recertificación de accesos, las autorizaciones de acceso de los usuarios para las aplicaciones, bases de datos, sistemas operativos y las herramienta de infraestructura clave, se modifican / eliminan a tiempo y de acuerdo con las normas.	Se solicitó evidencia de la certificación de usuarios, en donde se observara la respuesta del encargado del personal sobre el estatus de los usuarios y, para aquellos que se haya definido una baja, solicitamos evidencia de la solicitud que se realizó en la herramienta corporativa. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS1.1.3, SS1.2.2, SS5.1.8 y PI1.6.2** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS1.1.4 - SS1.1.5 - SS1.2.1	El nivel de privilegios de acceso a las bases de datos que respaldan las aplicaciones es revisado por la gerencia al menos una vez al año para garantizar que el acceso se restrinja adecuadamente en función de las responsabilidades del trabajo	Solicitamos evidencia de la certificación de usuarios realizada durante el año 2019, en la cual observamos que se cuente con el correo de IAM enviado a los responsables de la certificación, su respuesta y la conclusión de la modificación o estado de los usuarios. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS1.1.1, SS1.1.4, SS1.1.5, SS1.2.1, SS2.6.6 y SS5.1.7** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS1.3.1 - SS1.4.3	El gestor del área de reclutamiento y selección de personal obtiene la aprobación de la Dirección con el fin de corroborar que la vacante se encuentre justificada	Se solicitó el listado de vacantes aprobadas durante nuestro periodo de prueba 2019, las cuales en total corresponden a 24 solicitudes y posteriormente se realizó una muestra de 5 contrataciones, de las cuales 2 han sido cubiertas, para validar que la contratación cuente con la aprobación requerida. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS1.3.1 y SS1.4.3** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS1.3.2	La entidad cuenta con un proceso de adaptación y capacitación para preparar a los nuevos integrantes de la fuerza laboral en el desempeño de sus actividades.	Solicitamos evidencia de las políticas y/o normas detallando el proceso de adaptación, capacitación y entrenamiento a nuevos integrantes (cursos de inducción). Además, examinamos la Guía de bienvenida para nuevos empleados que se otorga a cada nuevo ingreso para brindar una perspectiva general del entorno laboral y operación de la entidad.	Sin excepciones que reportar.

ID	Actividad de Control	Procedimiento de Prueba	Resultado
		Nota: Prueba de control se encuentra en el ID SS1.3.2 Ver tabla de pruebas de soporte.	
SS1.3.3	El asesor de Formación revisa y publica el calendario de cursos presenciales para informar las fechas, con el fin de que el participante asista puntualmente para el cumplimiento de las competencias comprometidas	Solicitamos evidencia de la publicación de cursos en la herramienta corporativa de la compañía (Santander Learning) para la comprobación de disponibilidad e impartición de aquellos cursos que son programados por calendario. En la plataforma observamos que se publican los cursos junto con el detalle de estatus, propósito y disponibilidad para tomarlos. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS1.3.3, SS2.2.4, SS2.3.2 y C1.2.8** Ver tabla de pruebas de soporte.	Sin excepciones que reportar.
SS1.3.4	El asesor de Formación realiza el reporte anual de capacitación donde se integran los resultados e indicadores que muestran anualmente cifras de las actividades de los empleados de cada área, mismos que sirven en la toma de decisiones para el desarrollo de las competencias al siguiente año	Se solicitó la captura de pantalla del reporte anual de capacitación donde se muestren los resultados e indicadores que anualmente se generan con las cifras de las actividades de capacitación realizadas en el año, eso para corroborar que se cuenta con bases para la toma de decisiones para el desarrollo de competencias de años contiguos. **Nota: Prueba de control se encuentra en el ID SS1.3.4** Ver tabla de pruebas de soporte.	Sin excepciones que reportar.
SS1.3.5	El líder de proyecto da feedback al responsable o LP y solicita que entregue la información requerida con el fin de verificar que ésta se encuentre completa	De acuerdo al listado de proyectos se entregó una muestra de proyectos para solicitar la siguiente información con la finalidad de validar el cumplimiento del control: - Ticket de solicitud al proyecto - Captura de pantalla de los documentos solicitados para el proyecto (inputs) - Documento de Valoración Técnica **Nota: Prueba de control se encuentra en el ID SS1.3.5** Ver tabla de pruebas de soporte.	Sin excepciones que reportar.
SS1.4.1 - SS1.4.2	Las políticas de la entidad incluyen los códigos de conducta así como las posibles sanciones por mala conducta de los miembros de la fuerza laboral.	Solicitamos evidencia de las políticas y/o normas detallando las posibles sanciones aplicables por mala conducta del personal, a lo cual se nos proporcionó el Código General de ética y Conducta bajo el cual se rigen los lineamientos de conducta dentro de la entidad, así es como identificamos que se contemplan las medidas para comunicar los códigos de conducta y posibles sanciones aplicables. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS1.4.1, SS1.4.2 y SS6.2.8** Ver tabla de pruebas de soporte.	Sin excepciones que reportar.

ID	Actividad de Control	Procedimiento de Prueba	Resultado
SS1.4.4 - SS1.4.6	El gestor de reclutamiento y selección recaba los documentos necesarios para la contratación (checklist) y consigue las firmas correspondientes en todos los documentos que integran el expediente del nuevo empleado.	Se solicitó como evidencia el checklist que se realiza para cada una de las vacantes a cubrir, para la verificación de completitud, lo que indica que los documentos fueron entregados para la integración del expediente del candidato. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS1.4.4 y SS1.4.6** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS1.4.5	El Gestor de Niveles de Servicio difunde a las áreas participantes el procedimiento de acuerdo de niveles de servicio, indicando los servicios y niveles comprometidos para su conocimiento	Se solicitó la evidencia del correo de informe de renovación de niveles de servicio que se haya enviado en el año del periodo de revisión (2019), para la notificación de renovación de Niveles de Servicio al personal de la entidad, en donde se pudiera observar la fecha en que fue enviado y la redirección a los documentos que contienen los servicios y niveles comprometidos. **Nota: Prueba de control se encuentra en el ID SS1.4.5** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.

Criterios Comunes relacionados con Comunicaciones

ID	Actividad de Control	Procedimiento de Prueba	Resultado
SS2.2.2- SS2.2.3- SS2.3.1- SS2.4.1	Los documentos de políticas y procedimientos (Marco Normativo) para procesos significativos están disponibles en la intranet de la entidad.	Solicitamos evidencia de la pantalla de intranet en donde se encuentren disponibles las Normas y Procedimientos para su consulta por parte del personal de la entidad, con las versiones y cambios más recientes de los documentos, para validar que la entidad difunda y ponga a disposición del personal, las normas y políticas bajo las cuales se rige la empresa. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS2.2.2, SS2.2.3, SS2.3.1 y SS2.4.1** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS2.2.1	Se publica un aviso de privacidad en todos los sitios web y software disponibles públicamente de la entidad. El aviso de privacidad describe los compromisos de privacidad de la entidad.	Solicitamos evidencia del aviso de privacidad publicado en internet mismo que está disponible para todo cliente y proveedor que se relacione con Santander Global Technology. **Nota: Prueba de control se encuentra en el ID SS2.2.1** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.

ID	Actividad de Control	Procedimiento de Prueba	Resultado
SS2.2.4 - SS2.3.2	El asesor de Formación revisa y publica el calendario de cursos presenciales para informar las fechas, con el fin de que el participante asista puntualmente para el cumplimiento de las competencias comprometidas	Solicitamos evidencia de la publicación de cursos en la herramienta corporativa de la compañía (Santander Learning) para la comprobación de disponibilidad e impartición de aquellos cursos que son programados por calendario. En la plataforma observamos que se publican los cursos junto con el detalle de estatus, propósito y disponibilidad para tomarlos. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS1.3.3, SS2.2.4, SS2.3.2 y C1.2.8** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS2.2.6- SS2.3.4- SS2.4.2	El Gestor de Niveles de Servicio documenta en el informe de seguimiento al servicio las causas del incumplimiento o comportamiento de los servicios fuera de lo habitual.	Se solicitaron las presentaciones mensuales de Monitoreo del Servicio referentes al periodo de revisión Enero - Diciembre 2019, para la revisión de las causas de incumplimiento o comportamiento, y con base en la información contemplada en las presentaciones observaremos que se hayan tomado medidas para la solución de las incidencias. Sin embargo, identificamos que tanto para BS Perú como Consumer Perú no hubo ocurrencias de incidencias durante el año. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS2.2.6, SS2.3.4, SS2.4.2 y PI1.1.7** **Ver tabla de pruebas de soporte.**	No hubo ocurrencia de incidencias de incumplimiento de servicio o comportamiento de los servicios fuera de lo habitual durante el periodo de revisión 2019.
SS6.2.6- SS6.2.9- SS7.4.1	El Gestor de Cambios verifica que las áreas promotoras incluyan la documentación y/o Vo.Bo. necesarios en la herramienta para llevar a cabo el cambio de infraestructura solicitado. En caso de que no se cuente con toda la información necesaria el cambio no es autorizado por el Gestor de Cambios.	Recabamos el listado de cambios de infraestructura contemplados en el periodo de revisión de Enero - Diciembre 2019, equivalente a 25 cambios en la herramienta corporativa Remedy y 64 cambios en la herramienta Service Now. El listado se obtiene a través de un reporte emitido por la herramienta corporativa y con base en las solicitudes de cambio, extrajimos una muestra de 5 cambios (Remedy) y 7 cambios (SNOW) para validar que para cada solicitud se cuente con la documentación del cambio, la cual asegura que el cambio fue pre-aprobado por el CAB. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS6.2.6, SS6.2.9, SS7.4.1, SS6.2.6, SS6.2.9, SS7.1.2, SS7.3.2, SS7.4.1, SS7.4.2 y SS7.4.7** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS2.6.6	El nivel de privilegios de acceso a las bases de datos que respaldan las aplicaciones es revisado por la gerencia al menos una vez al año para	Solicitamos evidencia de la certificación de usuarios realizada durante el año 2019, en la cual observamos que se cuente con el correo de IAM enviado a los responsables de la certificación, su respuesta y la	Sin excepciones que reportar.

ID	Actividad de Control	Procedimiento de Prueba	Resultado
	garantizar que el acceso se restrinja adecuadamente en función de las responsabilidades del trabajo	conclusión de la modificación o estado de los usuarios. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS1.1.1, SS1.1.4, SS1.1.5, SS1.2.1, SS2.6.6 y SS5.1.7** **Ver tabla de pruebas de soporte.**	

Criterios Comunes relacionados con Gestión de Riesgos y Diseño e Implementación de Controles

ID	Actividad de Control	Procedimiento de Prueba	Resultado
SS3.1.1	El Coordinador de Configuración revisa a través de los indicadores corporativos y locales que la infraestructura se encuentre correctamente declarada acorde al modelo actual de CMDB	Solicitamos como evidencia la presentación de Indicadores Corporativos de Gestión de la Configuración, para con base en ello dar validez y garantizar que se tengan presentes los indicadores corporativos y locales de infraestructura, los cuales son tomados en cuenta como apoyo por parte de la entidad, en la toma de decisiones. **Nota: Prueba de control se encuentra en el ID SS3.1.1** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS3.1.2- SS3.1.3- SS3.1.4- SS3.1.5- SS3.1.7- SS3.1.8	El CGRT valida periódicamente el nivel de riesgo de los indicadores del proceso definidos para identificar desviaciones y, en su caso, reportarlas para definir el tratamiento que se debe dar de acuerdo a su posible impacto	Se solicitó evidencia del reporte de indicadores que se realiza de manera mensual para el periodo de revisión 2019, con el objetivo de comprobar que se realizó la identificación de desviaciones, así como la emisión de un reporte y el seguimiento que se efectuó para su resolución. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS3.1.2, SS3.1.3, SS3.1.4, SS3.1.5, SS3.1.7 y SS3.1.8** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS3.1.9	El Coordinador de la Configuración válida a través de la consulta en CMDB que la información proporcionada por el solicitante a través de una petición o por cambio se vea correctamente reflejada en CMDB.	Solicitamos el listado de tickets registrados para cambios o actualizaciones en la CMDB, el cual en su totalidad fue un equivalente de 1636 solicitudes, de las cuales extrajimos una muestra aleatoria de 15 actualizaciones, con el propósito de validar que cada solicitud contara con su respectiva descripción y que la modificación coincidiera con la petición realizada. **Nota: Prueba de control se encuentra en el ID SS3.1.9** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS3.1.10	Se dispone de indicadores de cambios, en los que se reflejan las solicitudes de cambios, tipos	Solicitamos la evidencia de dos de las presentaciones mensuales que realiza la compañía, en donde se incluyen los	Sin excepciones que reportar.

ID	Actividad de Control	Procedimiento de Prueba	Resultado
	de cambios y los cambios aprobados y/o rechazados.	indicadores de los cambios realizados a infraestructura mes con mes, esto para corroborar que la entidad cuenta con un método de retroalimentación para asegurar la satisfacción de los usuarios. En las presentaciones de indicadores, verificaremos que se cuente con el detalle (en cantidad) de los cambios realizados. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS3.1.10, SS7.1.1, SS7.2.1 y SS7.4.9** **Ver tabla de pruebas de soporte.**	
SS3.2.1	El Coordinador de Seguimiento actualiza las propiedades de los documentos, versión y detalle de las modificaciones solicitadas previo a su publicación con el fin de reflejar la operación vigente de la empresa.	Se solicitó captura de pantalla del sitio sharepoint de la compañía, en donde se encuentran almacenados los documentos de la Metodología Integral (MI) para la comprobación de la versión y estatus actualizado de los documentos ante su publicación correspondiente al periodo de revisión 2019. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS3.2.1 y SS4.1.1** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS3.2.3	El equipo de Gestión de Continuidad verifica que se ejecutan pruebas y simulacros donde se valida que las actividades contempladas en el DRP son correctas y suficientes.	Se solicitaron los informes de resultados de las pruebas, en donde se inspeccionará que se asegure la realización de las pruebas y simulacro realizados para comprobar la adecuación y suficiencia del alcance y la estrategia de respuesta ante un desastre por medio de las firmas de los involucrados. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS3.2.3, AI1.2.7 y AI1.3.1** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS3.2.4	El Administrador de Vulnerabilidades notifica vía correo electrónico a la Dirección de CISO por medio de indicadores, las vulnerabilidades críticas reportadas por los distintos medios.	Solicitamos la evidencia del correo que fue enviado a la Dirección de CISO, en donde se entrega el reporte de vulnerabilidades reportadas en el mes, en el reporte observamos que se cuenta con las capturas de pantalla de la notificación de vulnerabilidades por correo electrónico, así como el seguimiento realizado con el identificador de la herramienta corporativa en donde se reportó y la conclusión del estatus de la vulnerabilidad. **Nota: Prueba de control se encuentra en el ID SS3.2.4** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.

Criterios Comunes relacionados con Monitoreo de Controles

ID	Actividad de Control	Procedimiento de Prueba	Resultado
SS4.1.1	El Coordinador de Seguimiento actualiza las propiedades de los documentos, versión y detalle de las modificaciones solicitadas previo a su publicación con el fin de reflejar la operación vigente de la empresa.	Se solicitó captura de pantalla del sitio sharepoint de la compañía, en donde se encuentran almacenados los documentos de la Metodología Integral (MI) para la comprobación de la versión y estatus actualizado de los documentos ante su publicación correspondiente al periodo de revisión 2019. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS3.2.1 y SS4.1.1 Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS4.1.2	El analista de CGS valida que no se estén generando incidentes con la misma recurrencia posterior a la aplicación de un control de cambios, comunicar al personal de Gestión de Problemas si la solución aplicada fue exitosa o ha provocado otra falla o se sigue presentando la misma falla.	Se solicitó evidencia de los correos de VoBo para la resolución del incidente, en donde observaremos que fue resuelto y aprobado para su cierre. Solicitamos también que, en caso de contar con un reporte ejecutivo asociado al incidente, revisaremos que se encuentre el detalle de la causa del incidente, así como las actividades realizadas y la resolución del incidente. Sin embargo, identificamos que para los clientes no se identificaron ocurrencias de incidentes durante el periodo de prueba. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS4.1.2, SS6.2.3 y SS6.2.7 Ver tabla de pruebas de soporte.**	No hubo ocurrencias de incidentes P3 para los clientes Santander Perú y Consumer Perú durante el periodo de revisión 2019.

Criterios Comunes relacionados con Accesos Lógicos y Físicos

ID	Actividad de Control	Procedimiento de Prueba	Resultado
SS5.1.10	La solicitud de acceso para las bases de datos nuevas y modificadas y el acceso a los sistemas operativos se revisan apropiadamente, se documentan y ejecutan en la herramienta corporativa.	Se solicitó evidencia del ticket de solicitud, aprobación, justificación y evidencia del acceso para una muestra de accesos realizados durante el periodo para validar que cuentan con el proceso indicado y que éste ha sido otorgado conforme las reglas de autorización. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS5.1.10 y PI1.6.3 Ver tabla de pruebas de soporte.**	Identificamos un usuario de proceso el cual no se encontraba en la GreenList. Indagamos sobre el usuario y detectamos que este es un usuario que fue eliminado de la GreenList debido a que el aplicativo que lo usa, Bladelogic, está en proceso de ser removido por la entidad, por lo cual el usuario se eliminó en preparación al decomiso de la aplicación mencionada, sin embargo, se identificó que el acceso de administrador de este usuario es adecuado. Adicionalmente, en caso de que un usuario con permisos de administrador no se encontrara en la GreenList,

ID	Actividad de Control	Procedimiento de Prueba	Resultado
			esto sería detectado por medio del control de User Access Review. Para remediar este punto, la compañía agregó al usuario a la GreenList, mientras la aplicación Bladelogic es eliminada.
SS5.3.1 - SS5.2.5	Los componentes de infraestructura de SO (Unix, Linux, Windows) y BD (BBDDs DB2 / ORACLE / SQL) se encuentran configurados acorde a las guías de bastionado	Solicitamos evidencia de la información referente al listado de servidores de la entidad, una vez recibida la documentación, realizamos una muestra aleatoria de servidores y con base en los resultados de la muestra solicitamos a la entidad que realizara la ejecución de la herramienta ACTT para extraer la información de configuración con la que cuentan las Bases de Datos y Sistemas Operativos. La información extraída fue utilizada para confirmar que se encontrara bajo lo establecido en la Guía de Bastionado de la compañía. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS5.3.1, SS5.2.5 y SS7.4.8** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS5.1.2	El SOC, Administrador de Vulnerabilidades y/o servicios de cyber seguridad contratados para tal fin, notifica las vulnerabilidades críticas que pudieran impactar a la infraestructura en la DMZ por medio de correo electrónico a las Áreas Técnicas e involucrados para la atención de las mismas.	Se solicitó el listado de vulnerabilidades que fueron levantadas durante el periodo de prueba correspondiente al año 2019, con la finalidad de asegurar que la entidad cuente con un ticket o correo electrónico donde se notifique la vulnerabilidad a las Áreas Técnicas e involucradas para darle atención a la incidencia. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS5.1.2 y SS6.1.3** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS5.1.7	El nivel de privilegios de acceso a las bases de datos que respaldan las aplicaciones es revisado por	Solicitamos evidencia de la certificación de usuarios realizada durante el año 2019, en la cual observamos	Sin excepciones que reportar.

ID	Actividad de Control	Procedimiento de Prueba	Resultado
	la gerencia al menos una vez al año para garantizar que el acceso se restrinja adecuadamente en función de las responsabilidades del trabajo	que se cuente con el correo de IAM enviado a los responsables de la certificación, su respuesta y la conclusión de la modificación o estado de los usuarios. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS1.1.1, SS1.1.4, SS1.1.5, SS1.2.1, SS2.6.6 y SS5.1.7** **Ver tabla de pruebas de soporte.**	
SS5.1.8	Como parte del proceso de recertificación de accesos, las autorizaciones de acceso de los usuarios para las aplicaciones, bases de datos, sistemas operativos y las herramienta de infraestructura clave, se modifican / eliminan a tiempo y de acuerdo con las normas.	Se solicitó evidencia de la certificación de usuarios, en donde se observara la respuesta del encargado del personal sobre el estatus de los usuarios y, para aquellos que se haya definido una baja, solicitamos evidencia de la solicitud que se realizó en la herramienta corporativa. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS1.1.1, SS1.1.3, SS1.2.2, SS5.1.8 y PI1.6.2** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS5.1.4 - SS5.3.3 - SS5.3.5	Políticas y procedimientos se implementan validando que la infraestructura y software se encuentran debidamente configurados con Active Directory para el inicio de sesión.	Solicitamos evidencia de las políticas y procedimientos en donde se detalla que la infraestructura y software se encuentran debidamente configurados con Active Directory para el inicio de sesión, además de obtener evidencia de capturas de pantalla de los dominios de servidores con Active Directory implementado. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS5.1.4, SS5.3.3, SS5.3.5 y PI1.5.7** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS5.2.3 - SS5.5.1 - SS5.5.2 - SS5.5.3 - SS5.5.9 - SS5.5.10 - SS5.5.7	El personal de la administración cuenta con una identificación a través de una credencial que los identifica como personal administrativo y operativo para tener acceso	Solicitamos evidencia de las políticas y/o procedimientos aplicables para el uso de credencial dentro de las instalaciones. En complemento, pedimos evidencia de el escaneo del	Sin excepciones que reportar.

ID	Actividad de Control	Procedimiento de Prueba	Resultado
- SS5.5.15 - SS5.5.16	autorizado y limitado a las instalaciones.	formato de credencial para validar que cuente con la información correspondiente para el acceso otorgado. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS5.2.3, SS5.5.1, SS5.5.2, SS5.5.3, SS5.5.9, SS5.5.10, SS5.5.7, SS5.5.15 y SS5.5.16 Ver tabla de pruebas de soporte.**	
SS5.2.7 - SS5.5.12 - SS5.5.14	Cuando los empleados y trabajadores temporales finalizan su periodo laboral, se realiza una notificación a Recursos Humanos de manera oportuna.	Se solicitó evidencia del correo que es compartido por Peoplesoft y que después se carga al servidor para aplicar la baja de usuarios. Confirmaremos se cuente con el listado en donde se incluyan los usuarios con estatus de 'Terminado' para que sean procesados y su baja aplicada. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS5.2.7, SS5.5.12 y SS5.5.14 Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS5.2.2 - SS5.4.2 - SS5.5.4 - SS5.5.5 - SS5.5.6	El guardia de Seguridad Física verifica en el listado de acceso el ingreso al CPD del personal autorizado de acuerdo a las fechas y horarios señalados.	Se solicitó el listado de accesos realizados a los CPD's por mes, con ello se extrajo una muestra de 10 solicitudes en donde se validará que se cuente con la autorización(firma) y un ID de solicitud en la herramienta corporativa ligado, así como las actividades a realizar por el personal, nombres, empresa, fecha y horario de actividades. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS5.2.2, SS5.4.2, SS5.5.4, SS5.5.5, SS5.5.6 y C1.2.3 Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS5.5.13 - SS5.2.8 - SS5.5.11	La entidad recibe las bajas de personal realizadas por parte del proveedor, esto con la finalidad de remover los accesos otorgados al	Solicitamos evidencia de las políticas y/o procedimientos aplicables para las bajas por parte del proveedor además de obtener el reporte de bajas de personal realizadas	Sin excepciones que reportar.

ID	Actividad de Control	Procedimiento de Prueba	Resultado
	personal de servicio por parte del proveedor.	por parte del proveedor, esto con fin de realizar una muestra y obtener evidencia de la notificación de bajas del personal de servicio del proveedor a la entidad para validar que lo estipulado en las políticas sí se esté implementado y llevando a cabo de forma adecuada. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS5.5.13, SS5.2.8 y SS5.5.11** **Ver tabla de pruebas de soporte.**	
SS5.5.8	Todos los visitantes deben ser escoltados por un miembro de la fuerza laboral cuando visiten las instalaciones donde el sistema sensible y los componentes del sistema se mantienen y operan.	Observamos que la entidad cuenta con un proceso y política para el acceso físico al centro de cómputo. El proceso consiste en levantar un ticket o petición para ingresar al edificio, argumentando el motivo de la visita y se da seguimiento para su validación (Ref. S5.2.2, S5.2.3, S5.5.4, ...) En complemento, realizamos una visita al SITE y durante el recorrido identificamos que hubo una escolta por parte del personal de seguridad durante toda la visita, desde el ingreso a las instalaciones hasta la salida de las mismas. **Nota: Prueba de control se encuentra en el ID SS5.5.8** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS5.5.17 - SS5.5.18	Áreas sensibles dentro de la entidad cuenta con dispositivos físicos que se utilizan para controlar el acceso a instalaciones altamente sensibles y bajo el control de acceso de los miembros designados de la gerencia.	Realizamos una visita al Data Center de la entidad el cual se encuentra ubicado en Santiago de Querétaro y confirmamos que la entidad en sus exteriores cuenta con una barda perimetral, así como sensores fotobeam en bardas, malla ciclónica y cable microfónico para la detección perimetral. El edificio está cubierto por material de concreto con la capacidad de soportar 5 kg. de dinamita Además de	Sin excepciones que reportar.

ID	Actividad de Control	Procedimiento de Prueba	Resultado
		implementar medidas de control de acceso como un sistema de apertura de puertas mediante tarjetas magnéticas y sistemas biométricos. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS5.5.17 y SS5.5.18** **Ver tabla de pruebas de soporte.**	
SS5.7.1	Contar con esquemas de cifrado en los enlaces de telecomunicaciones para evitar que terceros no autorizados puedan acceder a la información de la Entidad.	De acuerdo a la visita realizada al Data Center y las guías de bastionado de SO, identificamos que el cifrado ocurre dentro del servidor, por lo que el cifrado no ocurre en el enlace sino en la información que es transmitida. **Nota: Prueba de control se encuentra en el ID SS5.7.1** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS5.8.3	Todos los sistemas Windows en HUB_MX cuentan con protección antivirus, gestionado y actualizado automáticamente de forma centralizada.	Solicitamos capturas de pantalla del estatus de los servidores y la versión del DAT para la comprobación de las políticas de escaneo y actualización, esto desde la consola central de monitoreo. **Nota: Prueba de control se encuentra en el ID SS5.8.3** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.

Criterios relacionados con Operación de los sistemas

ID	Actividad de Control	Procedimiento de Prueba	Resultado
SS6.1.1	A partir de que se detecte la necesidad, el técnico de monitoreo del área de CCS solicita la revisión de los umbrales de alertas y/o alarmas para la creación, modificación o corrección de parámetros con el fin de tener mayor tiempo de reacción.	Se solicitó el listado de alertas que fueron levantadas para la corrección, modificación o creación de parámetros para realizar una muestra y obtener los correos de detección para cada caso, así como el ticket con la descripción de las actividades implementadas para la corrección de fallas, esto con el fin de evaluar que se cuente con la solicitud y seguimiento correspondiente de cada caso hasta su cierre.	Sin excepciones que reportar.

ID	Actividad de Control	Procedimiento de Prueba	Resultado
		Nota: Prueba de control se encuentra en el ID SS6.1.1 Ver tabla de pruebas de soporte.	
SS6.1.3	El SOC, Administrador de Vulnerabilidades y/o servicios de cyber seguridad contratados para tal fin, notifica las vulnerabilidades críticas que pudieran impactar a la infraestructura en la DMZ por medio de correo electrónico a las Áreas Técnicas e involucrados para la atención de las mismas.	Se solicitó el listado de vulnerabilidades que fueron levantadas durante el periodo de prueba correspondiente al año 2019, con la finalidad de asegurar que la entidad cuente con un ticket o correo electrónico donde se notifique la vulnerabilidad a las Áreas Técnicas e involucradas para darle atención a la incidencia. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS5.1.2 y SS6.1.3 Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS6.2.1 - SS6.2.2 - SS6.2.4- SS6.2.5	El gerente de CCS al ver que la falla no ha sido resuelta, escala al siguiente nivel de atención e informa a los niveles ejecutivos correspondientes para que se apliquen acciones que resuelvan la falla.	Se solicitó el listado de incidentes registrados en el año 2019 con prioridad P3, sobre los cuales solicitamos el reporte ejecutivo que se entrega al cliente para revisar que se encuentre el detalle de la causa del incidente, así como las actividades realizadas y la resolución del incidente. Sin embargo, identificamos que para los clientes no se identificaron ocurrencias de incidentes durante el periodo de prueba. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS6.2.1, SS6.2.2, SS6.2.4, SS6.2.5, PI1.3.4 y PI1.5.6 Ver tabla de pruebas de soporte.**	No hubo ocurrencias de incidentes P3 para los clientes Santander Perú y Consumer Perú durante el periodo de revisión 2019.
SS6.2.3 - SS6.2.7	El analista de CGS valida que no se estén generando incidentes con la misma recurrencia posterior a la aplicación de un control de cambios, comunicar al personal de Gestión de Problemas si la solución aplicada fue exitosa o ha provocado otra falla o se sigue presentando la misma falla.	Se solicitó evidencia de los correos de VoBo para la resolución del incidente, en donde observaremos que fue resuelto y aprobado para su cierre. Solicitamos también en caso de aplicar, un reporte ejecutivo asociado al incidente, revisaremos que se encuentre el detalle de la causa del incidente, así como las actividades realizadas y la resolución del incidente. Sin embargo identificamos que para los clientes no se identificaron ocurrencias de incidentes durante el periodo de prueba. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS4.1.2, SS6.2.3 y SS6.2.7 Ver tabla de pruebas de soporte.**	No hubo ocurrencias de incidentes P3 para los clientes Santander Perú y Consumer Perú durante el periodo de revisión 2019.
SS6.2.6 - SS6.2.9	El Gestor de Cambios verifica que las áreas promotoras incluyan la documentación y/o Vo.Bo. necesarios en la herramienta para llevar a cabo el cambio de infraestructura solicitado. En caso de que no se cuente	Recabamos el listado de cambios de infraestructura contemplados en el periodo de revisión de Enero - Diciembre 2019, equivalente a 25 cambios en la herramienta corporativa Remedy y 64 cambios en la herramienta Service Now. El listado se obtiene a través de un reporte emitido por la herramienta corporativa y con base en las solicitudes de cambio, extrajimos una	Sin excepciones que reportar.

ID	Actividad de Control	Procedimiento de Prueba	Resultado
	con toda la información necesaria el cambio no es autorizado por el Gestor de Cambios.	muestra de 5 cambios (Remedy) y 7 cambios (SNOW) para validar que para cada solicitud se cuente con la documentación del cambio, la cual asegura que el cambio fue pre-aprobado por el CAB. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS6.2.6, SS6.2.9, SS7.4.1, SS6.2.6, SS6.2.9, SS7.1.2, SS7.3.2, SS7.4.1, SS7.4.2 y SS7.4.7** **Ver tabla de pruebas de soporte.**	
SS6.2.8	Las políticas de la entidad incluyen los códigos de conducta así como las posibles sanciones por mala conducta de los miembros de la fuerza laboral.	Solicitamos evidencia de las políticas y/o normas detallando las posibles sanciones aplicables por mala conducta del personal, a lo cual se nos proporcionó el Código General de ética y Conducta bajo el cual se rigen los lineamientos de conducta dentro de la entidad, así es como identificamos que se contemplan las medidas para comunicar los códigos de conducta y posibles sanciones aplicables. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS1.4.1, SS1.4.2 y SS6.2.8** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.

Criterios comunes relacionados a la gestión de cambios

ID	Actividad de Control	Procedimiento de Prueba	Resultado
SS7.1.1 - SS7.2.1 -SS7.4.9	Se dispone de indicadores de cambios, en los que se reflejan las solicitudes de cambios, tipos de cambios y los cambios aprobados y/o rechazados.	Solicitamos la evidencia de dos de las presentaciones mensuales que realiza la compañía, en donde se incluyen los indicadores de los cambios realizados a infraestructura mes con mes, esto para corroborar que la entidad cuenta con un método de retroalimentación para asegurar la satisfacción de los usuarios. En las presentaciones de indicadores, verificaremos que se cuente con el detalle (en cantidad) de los cambios realizados. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS3.1.10, SS7.1.1, SS7.2.1 y SS7.4.9** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS7.1.2 - SS7.3.2 - SS7.4.1 - SS7.4.2 - SS7.4.7	El Gestor de Cambios verifica que las áreas promotoras incluyan la documentación y/o Vo.Bo. necesarios en la herramienta para llevar a cabo el cambio de infraestructura solicitado. En caso de que no se cuente con toda la información	Recabamos el listado de cambios de infraestructura contemplados en el periodo de revisión de Enero - Diciembre 2019, equivalente a 25 cambios en la herramienta corporativa Remedy y 64 cambios en la herramienta Service Now. El listado se obtiene a través de un reporte emitido por la herramienta corporativa y con base en las	Sin excepciones que reportar.

ID	Actividad de Control	Procedimiento de Prueba	Resultado
	necesaria el cambio no es autorizado por el Gestor de Cambios.	solicitudes de cambio, extrajimos una muestra de 5 cambios (Remedy) y 7 cambios (SNOW) para validar que para cada solicitud se cuente con la documentación del cambio, la cual asegura que el cambio fue pre-aprobado por el CAB. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS6.2.6, SS6.2.9, SS7.4.1, SS6.2.6, SS6.2.9, SS7.1.2, SS7.3.2, SS7.4.1, SS7.4.2 y SS7.4.7** **Ver tabla de pruebas de soporte.**	
SS7.2.2 - SS7.3.1	El analista de gestión de incidentes notifica la existencia de un incidente y que este debe ser solucionado a través de un cambio emergente	Se solicitó el listado de tickets registrados a Gestión de Incidentes para realizar una muestra, sin embargo identificamos que para los incidentes registrados ninguno de los casos evaluados derivó en un cambio emergente para su solución. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS7.2.2 y SS7.3.1** **Ver tabla de pruebas de soporte.**	No hubo ocurrencias de incidentes P3 para los clientes Santander Perú y Consumer Perú durante el periodo de revisión 2019.
SS7.4.3	El responsable de Gestión de Despliegues realiza la extracción de los despliegues registrados en la Herramienta Corporativa con el fin de generar los indicadores mensuales correspondientes a: Histórico de despliegues instalados, despliegues que generaron un incidente y despliegues no exitosos.	Se solicitaron los informes de indicadores mensuales correspondientes a los meses muestra de Marzo y Noviembre en donde buscamos asegurar que se cuente con el filtro y detalle de los despliegues instalados, despliegues que generaron un incidente y despliegues no exitosos. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS7.4.3, PI1.2.6, PI1.2.9 y PI1.2.10** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS7.4.4 - SS7.4.10	El Gestor de Despliegues verifica que el integrador incluya toda la documentación necesaria para llevar a cabo el despliegue solicitado. La información es registrada en la Herramienta Corporativa el cual incluye checks para cambiar de estado en caso de contar con la información requerida; en la Herramienta Corporativa pueden observarse datos como: Folio, estatus, objetivo, alcance, funcionalidad, categorización, planificación, autorización, código de cierre, entre otros. En caso de que no se cuente con toda la información necesaria para el despliegue éste es rechazado por el Gestor de Despliegues.	Se solicitó evidencia del reporte de la herramienta corporativa y sobre eso se eligió una muestra para la cual se pidió como evidencia el ticket en donde se muestre lo siguiente: - ID de Despliegue - Código de cierre - Planificación - Autorizaciones **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS7.4.4, SS7.4.10, C1.1.1, C1.2.4, C1.3.1, C1.3.6, PI1.2.12, PI1.3.6, PI1.5.1, PI1.5.4, PI1.6.1, PI1.3.2 y PI1.3.5** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.

ID	Actividad de Control	Procedimiento de Prueba	Resultado
SS7.4.5	El Administrador de Vulnerabilidades realiza el seguimiento a las vulnerabilidades críticas con las áreas involucradas para la remediación o mitigación de las vulnerabilidades hasta su cierre a través de correo electrónico añadiendo el número de ticket de atención que se generó en la herramienta corporativa de peticiones y/o cambios.	Se solicitó el listado de vulnerabilidades que fueron levantadas durante el periodo de prueba correspondiente al año 2019, con la finalidad de asegurar que la entidad cuente con un ticket o correo electrónico donde se notifique la vulnerabilidad a las Áreas Técnicas e involucradas para darle atención a la incidencia y confirmar que se entregara una conclusión respecto a la vulnerabilidad. **Nota: Prueba de control se encuentra en el ID SS7.4.5 Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
SS7.4.8	Los componentes de infraestructura de SO (Unix, Linux, Windows) y BD (BBDDs DB2 / ORACLE / SQL) se encuentran configurados acorde a las guías de bastionado	Solicitamos evidencia de la información referente al listado de servidores de la entidad, una vez recibida la documentación, realizamos una muestra aleatoria de servidores y con base en los resultados de la muestra solicitamos a la entidad que realizara la ejecución de la herramienta ACTT para extraer la información de configuración con la que cuentan las Bases de Datos y Sistemas Operativos. La información extraída fue utilizada para confirmar que se encontrara bajo lo establecido en la Guía de Bastionado de la compañía. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS5.3.1, SS5.2.5 y SS7.4.8 Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.

Criterios de Disponibilidad

ID	Actividad de Control	Procedimiento de Prueba	Resultado
AI1.2.1	Contar con todos los controles y dispositivos de control ambiental instalados y operando para asegurar la operación adecuada de los equipos de procesamiento y telecomunicaciones de la Entidad. Dichos controles deberán incluir, al menos: a. Aire acondicionado b. Detectores de humo, humedad y líquidos c. Sistemas de extinción de incendios manuales o automáticos. De tratarse de extintores manuales, contar con los suficientes para cubrir la	Con base en la visita realizada, examinamos los controles ambientales en materia de aire acondicionado, daños por inundación y peligros de incendio. Todos los controles ambientales cumplen satisfactoriamente con los lineamientos de seguridad y precaución para el aseguramiento de la operación adecuada del centro de cómputo. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: AI1.2.1 y PI1.1.4 Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.

ID	Actividad de Control	Procedimiento de Prueba	Resultado
	capacidad del centro de cómputo.		
AI1.2.2	El personal de operaciones monitorea el estado de las protecciones ambientales durante cada turno para dar mantenimiento. Se han instalado mecanismos de alerta para comunicar cualquier discrepancia en los umbrales ambientales.	Tomando en consideración la visita realizada al Data Center, corroboramos que existe un sistema de monitoreo electromecánico y un aula especial para dicha actividad. En complemento, se cuenta con una bitácora de registros para dar continuidad y seguimiento al monitoreo. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s:AI1.2.2, PI1.1.5 y PI1.1.6 Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
AI1.2.3 - AI1.2.9	El responsable de Gestión de la Continuidad en conjunto con el cliente verifica que el alcance y la estrategia contemplados en la Carta de Alcance es adecuado y suficiente.	Se solicitaron las Cartas de Alcance firmadas por los interesados, en donde se inspeccionará que para cada cliente se asegure la aceptación a los niveles de adecuación y suficiencia del alcance y la estrategia de respuesta ante un desastre. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: AI1.2.3 y AI1.2.9 Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
AI1.2.4	El analista de BackUp valida la existencia de un Vo.Bo. de Riesgo Tecnológico en ambiente de QA o Vo.Bo. de Gerencia de Backup	Se solicitó inicialmente el listado de solicitudes de restauraciones que ocurrieron durante el periodo de revisión de Enero - Diciembre 2019, lo cual resultó en un total de 48 solicitudes de restauración y sobre ello se seleccionó una muestra de 5 solicitudes de las cuales se pidió entregar el correo con el Vo.Bo para la ejecución de la recuperación. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: AI1.2.4, PI1.1.1 y PI1.4.3 Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
AI1.2.5	El analista de Backup revisa diariamente y por turno que los respaldos programados hayan terminado correctamente y no se omita el reporte y seguimiento de procesos fallidos.	En primera instancia se solicitó el listado de respaldos Missed que ocurrieron en el periodo de Enero - Diciembre 2019, en el cuál se identificaron 2258 respaldos, y sobre ello se seleccionó una muestra correspondiente a 10 respaldos basándonos en la frecuencia del control. Para cada muestra selecionada, pedimos nos entregaran el correo de seguimiento y la confirmación de resolución para asegurar la eficacia del control. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: AI1.2.5 y PI1.1.2 Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
AI1.2.7 - AI1.3.1	El equipo de Gestión de Continuidad verifica que se ejecutan pruebas y simulacros	Se solicitaron los informes de resultados de las pruebas, en donde se inspeccionará que se asegure la realización de las pruebas y	Sin excepciones que reportar.

ID	Actividad de Control	Procedimiento de Prueba	Resultado
	donde se valida que las actividades contempladas en el DRP son correctas y suficientes.	simulacro realizados para comprobar la adecuación y suficiencia del alcance y la estrategia de respuesta ante un desastre por medio de las firmas de los involucrados. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS3.2.3, AI1.2.7 y AI1.3.1** **Ver tabla de pruebas de soporte.**	
AI1.2.8	El responsable de Gestión de Continuidad verifica que en los contratos, OLAs (Operating Level Agreement o Acuerdo del Nivel de Operación) establecidos con el proveedor del CAT se cuenta con cláusulas de niveles de servicio que aseguran la disponibilidad de los recursos provistos por los proveedores ante la declaración de desastres.	Entablamos comunicación con el cliente para la extracción y obtención del documento Acuerdo Operational Level Agreement el cuál posteriormente validamos incluyera las cláusulas de niveles de servicio que aseguran la disponibilidad de los recursos provistos por los proveedores ante la declaración de desastres. **Nota: Prueba de control se encuentra en el ID AI1.2.8** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
AI1.3.2	El responsable de Gestión de Continuidad publica el plan de recuperación en la Intranet corporativa (Kosmos), de tal manera que se pueda acceder aun cuando el sitio primario no se encuentre operativo.	Se solicitó captura de pantalla de la publicación del Plan de Recuperación en la intranet Kosmos, además del plan en su versión más reciente. **Nota: Prueba de control se encuentra en el ID AI1.3.2** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.

Criterios de Confidencialidad

ID	Actividad de Control	Procedimiento de Prueba	Resultado
C1.1.1 - C1.2.4 - C1.3.1- C1.3.6	El Gestor de Despliegues verifica que el integrador incluya toda la documentación necesaria para llevar a cabo el despliegue solicitado. La información es registrada en la Herramienta Corporativa el cual incluye checks para cambiar de estado en caso de contar con la información requerida; en la Herramienta Corporativa pueden observarse datos como: Folio, estatus, objetivo, alcance, funcionalidad, categorización, planificación, autorización, código de cierre, entre otros. En caso de que no se cuente con toda la información necesaria para el despliegue éste es rechazado por el Gestor de Despliegues.	Se solicitó evidencia del reporte de la herramienta corporativa y sobre eso se eligió una muestra para la cual se pidió como evidencia el ticket en donde se muestre lo siguiente: - ID de Despliegue - Código de cierre - Planificación - Autorizaciones **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS7.4.4, SS7.4.10, C1.1.1, C1.2.4, C1.3.1, C1.3.6, PI1.2.12, PI1.3.6, PI1.5.1, PI1.5.4, PI1.6.1, PI1.3.2 y PI1.3.5** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.

ID	Actividad de Control	Procedimiento de Prueba	Resultado
C1.2.3	El guardia de Seguridad Física verifica en el listado de acceso el ingreso al CPD del personal autorizado de acuerdo a las fechas y horarios señalados.	Se solicitó el listado de accesos realizados a los CPD's por mes, con ello se extrajo una muestra de 10 solicitudes en donde se validará que se cuente con la autorización(firma) y un ID de solicitud en la herramienta corporativa ligado, así como las actividades a realizar por el personal, nombres, empresa, fecha y horario de actividades. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS5.2.2, SS5.4.2, SS5.5.4, SS5.5.5, SS5.5.6 y C1.2.3** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
C1.2.5 - C1.2.7	La entidad cuenta con políticas y/o procedimientos aplicables para la seguridad, clasificación y resguardo de información confidencial.	Se solicitó evidencia de las políticas y/o procedimientos aplicables para la seguridad, clasificación y resguardo de información confidencial, resultando en el documento de "Requisitos de Ciber Seguridad para Usuarios Técnicos" sobre el cual examinamos la especificación de aspectos de confidencialidad, tales como clasificación, protección, uso y responsabilidades resultantes del uso de información confidencial. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: C1.2.5 y C1.2.7** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
C1.3.8 - C1.8.1 - C1.7.1	Contar con políticas y procedimientos para la administración y control de respaldos de información, que contemplen, al menos, lo siguiente: a. Identificación del tipo de información que se respalda (bases de datos, programas, datos, sistema operativo, etc.). b. El tipo de respaldo de que se trate (completo, diferencial, incremental). c. Rotación y período de retención de los dispositivos de almacenamiento (diario, semanal, mensual o anual). d. Transporte de respaldos e. Pruebas periódicas de los respaldos f. Traslado de los respaldos fuera de sitio. g. Destrucción de respaldos, así como su registro en una bitácora indicando el motivo de la destrucción, persona que lo realiza, fecha y el medio de destrucción	Con base en la explicación proporcionada durante la visita en relación al respaldo de información, identificamos que la información a respaldar se categoriza y almacena en data domains. Cuando la capacidad de almacenamiento se sobrepasa, la información se traslada a un disco duro y posteriormente a una cinta. Referente al acceso de la información respaldada, existe un personal específico para el tratamiento de dicha información. Para el traslado de respaldos y la destrucción de los mismos se atribuye la responsabilidad a un personal autorizado, y se especifican los detalles de tanto el traslado como la destrucción, con previa autorización del dueño de la información. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: C1.3.8, C1.8.1 y C1.7.1** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.

ID	Actividad de Control	Procedimiento de Prueba	Resultado
	. h. Restricción para el almacenamiento de información crítica en equipos de cómputo personales sin esquemas de respaldo. i. Mecanismos de protección de la información almacenada en los dispositivos de respaldo que eviten que personas no autorizadas tengan acceso o hagan mal uso de ella.		
C1.2.6	La solicitud de acceso para las bases de datos nuevas y modificadas y para el acceso a los sistemas operativos está debidamente aprobada, documentada y ejecutada.	Se solicitó evidencia de la 'Green List' con la que cuenta la compañía, de esta manera se verificará que las solicitudes de accesos privilegiados sean realizadas por personal autorizado que cuente con el criterio para realizar la solicitud y que esto permita que esté debidamente justificada y pueda ser aprobada. **Nota: Prueba de control se encuentra en el ID C1.2.6 Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
C1.2.8	El asesor de Formación revisa y publica el calendario de cursos presenciales para informar las fechas, con el fin de que el participante asista puntualmente para el cumplimiento de las competencias comprometidas	Solicitamos evidencia de la publicación de cursos en la herramienta corporativa de la compañía (Santander Learning) para la comprobación de disponibilidad e impartición de aquellos cursos que son programados por calendario. En la plataforma observamos que se publican los cursos junto con el detalle de estatus, propósito y disponibilidad para tomarlos. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS1.3.3, SS2.2.4, SS2.3.2 y C1.2.8 Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
C1.3.9 - C1.4.1 - C1.4.2	Grupo Gobierno y Control firma el contrato verificando que los datos se encuentren acorde a la propuesta aprobada	Tras solicitar el listado de contratos aprobados por el área de Gobierno y Control de la entidad, reducido a los conceptos de Servicios Externalizados y Gastos de Personal, se realizó un muestreo con 7 contratos para la revisión y comprobación de los elementos antes mencionados para el periodo de prueba de Enero - Diciembre 2019. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: C1.3.9, C1.4.1 y C1.4.2 Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.

Criterios relacionados con Integridad

ID	Actividad de Control	Procedimiento de Prueba	Resultado
PI1.5.7	Políticas y procedimientos se implementan validando que la infraestructura y software se encuentran debidamente configurados con Active Directory para el inicio de sesión.	Solicitamos evidencia de las políticas y procedimientos en donde se detalla que la infraestructura y software se encuentran debidamente configurados con Active Directory para el inicio de sesión, además de obtener evidencia de capturas de pantalla de los dominios de servidores con Active Directory implementado. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS5.1.4, SS5.3.3, SS5.3.5 y PI1.5.7** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
PI1.6.2	Como parte del proceso de recertificación de accesos, las autorizaciones de acceso de los usuarios para las aplicaciones, bases de datos, sistemas operativos y las herramienta de infraestructura clave, se modifican / eliminan a tiempo y de acuerdo con las normas.	Se solicitó evidencia de la certificación de usuarios, en donde se observara la respuesta del encargado del personal sobre el estatus de los usuarios y, para aquellos que se haya definido una baja, solicitamos evidencia de la solicitud que se realizó en la herramienta corporativa. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS1.1.3, SS1.2.2, SS5.1.8 y PI1.6.2** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
PI1.1.4	Contar con todos los controles y dispositivos de control ambiental instalados y operando para asegurar la operación adecuada de los equipos de procesamiento y telecomunicaciones de la Entidad. Dichos controles deberán incluir, al menos: a. Aire acondicionado b. Detectores de humo, humedad y líquidos c. Sistemas de extinción de incendios manuales o automáticos. De tratarse de extintores manuales, contar con los suficientes para cubrir la capacidad del centro de cómputo.	Con base en la visita realizada, examinamos los controles ambientales en materia de aire acondicionado, daños por inundación y peligros de incendio. Todos los controles ambientales cumplen satisfactoriamente con los lineamientos de seguridad y precaución para el aseguramiento de la operación adecuada del centro de cómputo. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: AI1.2.1 y PI1.1.4** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
PI1.2.12 - PI1.3.6 - PI1.5.1 - PI1.5.4 - PI1.6.1 - PI1.3.2 - PI1.3.5	El Gestor de Despliegues verifica que el integrador incluya toda la documentación necesaria para llevar a cabo el despliegue solicitado. La información es registrada en la Herramienta Corporativa el cual incluye checks para cambiar de estado en caso de contar con la	Se solicitó evidencia del reporte de la herramienta corporativa y sobre eso se eligió una muestra para la cual se pidió como evidencia el ticket en donde se muestre lo siguiente: - ID de Despliegue - Código de cierre - Planificación	Sin excepciones que reportar.

ID	Actividad de Control	Procedimiento de Prueba	Resultado
	información requerida; en la Herramienta Corporativa pueden observarse datos como: Folio, estatus, objetivo, alcance, funcionalidad, categorización, planificación, autorización, código de cierre, entre otros. En caso de que no se cuente con toda la información necesaria para el despliegue éste es rechazado por el Gestor de Despliegues.	- Autorizaciones **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS7.4.4, SS7.4.10, C1.1.1, C1.2.4, C1.3.1, C1.3.6, PI1.2.12, PI1.3.6, PI1.5.1, PI1.5.4, PI1.6.1, PI1.3.2 y PI1.3.5 Ver tabla de pruebas de soporte.**	
PI1.2.6, -PI1.2.9 - PI1.2.10	El responsable de Gestión de Despliegues realiza la extracción de los despliegues registrados en la Herramienta Corporativa con el fin de generar los indicadores mensuales correspondientes a: Histórico de despliegues instalados, despliegues que generaron un incidente y despliegues no exitosos.	Se solicitaron los informes de indicadores mensuales correspondientes a los meses muestra de Marzo y Noviembre en donde buscamos asegurar que se cuente con el filtro y detalle de los despliegues instalados, despliegues que generaron un incidente y despliegues no exitosos. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS7.4.3, PI1.2.6, PI1.2.9 y PI1.2.10 Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
PI1.1.1 - PI1.4.3	El analista de BackUp valida la existencia de un Vo.Bo. de Riesgo Tecnológico en ambiente de QA o Vo.Bo. de Gerencia de Backup	Se solicitó inicialmente el listado de solicitudes de restauraciones que ocurrieron durante el periodo de revisión de Enero - Diciembre 2019, lo cual resultó en un total de 48 solicitudes de restauración y sobre ello se seleccionó una muestra de 5 solicitudes de las cuales se pidió entregar el correo con el Vo.Bo para la ejecución de la recuperación. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: AI1.2.4, PI1.1.1 y PI1.4.3 Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
PI1.1.2	El analista de Backup revisa diariamente y por turno que los respaldos programados hayan terminado correctamente y no se omita el reporte y seguimiento de procesos fallidos.	En primera instancia se solicitó el listado de respaldos Missed que ocurrieron en el periodo de Enero - Diciembre 2019, en el cuál se identificaron 2258 respaldos, y sobre ello se seleccionó una muestra correspondiente a 10 respaldos basándonos en la frecuencia del control. Para cada muestra selecionada, pedimos nos entregaran el correo de seguimiento y la confirmación de resolución para asegurar la eficacia del control. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de**	Sin excepciones que reportar.

ID	Actividad de Control	Procedimiento de Prueba	Resultado
		ID´s: AI1.2.5 y PI1.1.2 Ver tabla de pruebas de soporte.	
PI1.3.4 - PI1.5.6	El gerente de CCS al ver que la falla no ha sido resuelta, escala al siguiente nivel de atención e informa a los niveles ejecutivos correspondientes para que se apliquen acciones que resuelvan la falla.	Se solicitó el listado de incidentes registrados en el año 2019 con prioridad P3, sobre los cuales solicitamos el reporte ejecutivo que se entrega al cliente para revisar que se encuentre el detalle de la causa del incidente, así como las actividades realizadas y la resolución del incidente. Sin embargo, identificamos que para los clientes no se identificaron ocurrencias de incidentes durante el periodo de prueba. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS6.2.1, SS6.2.2, SS6.2.4, SS6.2.5, PI1.3.4 y PI1.5.6 Ver tabla de pruebas de soporte.**	No hubo ocurrencias de incidentes P3 para los clientes Santander Perú y Consumer Perú durante el periodo de revisión 2019.
PI1.1.7	El Gestor de Niveles de Servicio documenta en el informe de seguimiento al servicio las causas del incumplimiento o comportamiento de los servicios fuera de lo habitual.	Se solicitaron las presentaciones mensuales de Monitoreo del Servicio referentes al periodo de revisión Enero - Diciembre 2019, para la revisión de las causas de incumplimiento o comportamiento, y con base en la información contemplada en las presentaciones observaremos que se hayan tomado medidas para la solución de las incidencias. Sin embargo, identificamos que tanto para BS Perú como Consumer Perú no hubo ocurrencias de incidencias durante el año. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS2.2.6, SS2.3.4, SS2.4.2 y PI1.1.7 Ver tabla de pruebas de soporte.**	No hubo ocurrencia de incidencias de incumplimiento de servicio o comportamiento de los servicios fuera de lo habitual durante el periodo de revisión 2019.
PI1.6.3	La solicitud de acceso para las bases de datos nuevas y modificadas y el acceso a los sistemas operativos se revisan apropiadamente, se documentan y ejecutan en la herramienta corporativa.	Se solicitó evidencia del ticket de solicitud, aprobación, justificación y evidencia del acceso para una muestra de accesos realizados durante el periodo para validar que cuentan con el proceso indicado y que éste ha sido otorgado conforme las reglas de autorización. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: SS5.1.10 y PI1.6.3 Ver tabla de pruebas de soporte.**	Identificamos un usuario de proceso el cual no se encontraba en la GreenList. Indagamos sobre el usuario y detectamos que este es un usuario que fue eliminado de la GreenList debido a que el aplicativo que lo usa, Bladelogic, está en proceso de ser removido por la entidad, por lo cual el usuario se eliminó en preparación al

ID	Actividad de Control	Procedimiento de Prueba	Resultado
			decomiso de la aplicación mencionada, sin embargo, se identificó que el acceso de administrador de este usuario es adecuado. Adicionalmente, en caso de que un usuario con permisos de administrador no se encontrara en la GreenList, esto sería detectado por medio del control de User Access Review. Para remediar este punto, la compañía agregó al usuario a la GreenList, mientras la aplicación Bladelogic es eliminada.
PI1.1.5 – PI1.1.6	El personal de operaciones monitorea el estado de las protecciones ambientales durante cada turno para dar mantenimiento. Se han instalado mecanismos de alerta para comunicar cualquier discrepancia en los umbrales ambientales.	Tomando en consideración la visita realizada al Data Center, corroboramos que existe un sistema de monitoreo electromecánico y un aula especial para dicha actividad. En complemento, se cuenta con una bitácora de registros para dar continuidad y seguimiento al monitoreo. **Nota: Prueba de control se encuentra agrupada en el siguiente conjunto de ID´s: AI1.2.2, PI1.1.5 y PI1.1.6** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.
PI1.1.8	Para los enlaces entre las instalaciones críticas (centro de cómputo principal y alterno), sucursales y corporativos, deberán contemplarse enlaces alternos a través de diferentes proveedores o en su defecto, por medios y tecnologías distintas.	Realizando una visita al SITE, identificamos que la entidad cuenta con un alto nivel de redundancia por lo que al considerar enlaces alternos se tienen las medidas preventivas para utilizar la propia tecnología de la entidad y sistemas de duplicado para mantener las comunicaciones funcionando sin interrupciones. **Nota: Prueba de control se encuentra en el siguiente ID PI1.1.8** **Ver tabla de pruebas de soporte.**	Sin excepciones que reportar.