Asignatura	Datos del alumno	Fecha
Auditoría de seguridad	Apellidos: Paz Lopez Nombre: Angel Ramón	27/11/2021

ANTECEDENTES

En la actualidad donde la tecnología es el auge de mejoras en todos los servicios, las empresas que manejan grandes cantidades de información, como lo es CityCorp una entidad Bancaria con una amplia base de datos de sus clientes, datos privados, cuentas, transacciones, etc. Por el cual el objetivo de tener un Centro de Procesamiento de Datos es de poder almacenar todos los datos de sus clientes y las todas las actividades que se realicen sobre sus cuentas y así brindar un mejor servicio al cliente, por ende el Centro de Procesamiento de datos debe ser tratado como una unidad y no estar de manera aislada en la organización con áreas que son complementarias e interdependientes y cuya visión es brindar un servicio de calidad a los usuarios y clientes de la organización, para ello CityCorp cuenta con la infraestructura adecuada, con un espacio disponible amplio para el CPD, con áreas estratégicas para un eficaz acceso a los equipos y despliegue del personal, una excelente instalación de suministro eléctrico, acondicionamiento y todos los elementos de seguridad necesarios tanto físico como lógico para el diseño de un centro de procesamiento para que sea tolerante a fallos y a las vulnerabilidades que esta contenga y nos permita a la vez realizar cualquier tipo de actividad de mantenimiento sin que ningún servicio sea afectado.

CityCorp cuenta con controles generales en relación a la ISO (27002, 2017) con el que cuenta con 5 controles activos con el objetivo de tener 10 los cuales ya han sido auditados por el personal competente

Referencia	Control	Nivel de Cumplimiento	Madurez
8.1.1	Inventario de Activos	70%	Definido
9.1.1	Políticas de Control de Accesos	60%	Definido
9.3.1	Uso de información confidencial para la autenticación.	90%	Definido
11.1.1	Perímetro de seguridad física.	100%	Optimizado
11.2.1	Emplazamiento y protección de equipos.	100%	Optimizado

12.4.1	Registro y gestión de eventos de actividad.	0%	No existe, será implementado
12.7.1	Controles de auditoría de los sistemas de información	0%	No existe, será implementado
13.1.1	Controles de red.	0%	No existe, será implementado
16.1.1	Responsabilidades y procedimientos	0%	No existe, será implementado
18.1.4	Protección de datos y privacidad de la información personal.	0%	No existe, será implementado

La entidad Bancaria cuenta con el nivel del Centro de Procesamiento de Datos de Certificación TIER 4 ya que es el máximo nivel que puede alcanzar un data center la cual garantiza que la información y datos tendrán la mayor disponibilidad y el menor índice a cualquier fallo. El certificado tier ratifica y ofrece las siguientes garantías:

1. Que la entidad posee una infraestructura robusta, resistente, tolerante a fallos.
2. Que la entidad tiene un alto tiempo en el procesamiento de datos.
3. Que la entidad es resistente a desastres y posee las medidas y mecanismos de seguridad necesarias.

Con respecto al diseño del Centro de Procesamiento de datos podríamos mencionar:

El nivel de redundancia del CPD debe ser de nivel IV 2(n+1) con el cual cuenta con varios elementos y rutas de redundancia el cual brinda una disponibilidad de un 99.995% de disponibilidad, soportando casos e incidentes no planificados, con los debidos mecanismos y servicios de seguridad para el equipo y todas las áreas del CPD ya sea físico y lógico.

En cuanto al espacio y movilidad que debe tener el área del Centro de Procesamiento de datos podemos mencionar las características que deben tener las salas, una altura y anchura adecuadas cumpliendo con la norma ICREA-STD131-2015 para no dificultar la movilidad tanto de las personas como de los equipos, se recomienda suelo móvil o suelo falso con el objetivo de que los cables de energía eléctrica se ubiquen debajo del piso falso mediante bandejas sujetadas a soportes de las placas, con el suministro eléctrico hay que

tener cuidado con los voltajes correspondientes según el equipo para que no generen ningún corto circuito o evitar el daño de un equipo.

En cuanto al suministro eléctrico se recomienda que se realice en una linea independiente del resto de la instalación para evitar cualquier problema de saturación, para cualquier equipo también se recomienda que tengan las medidas de seguridad como las UPS y reguladores de voltaje y se recomienda también tener 2 generadores con la misma capacidad por cualquier evento imprevisto con la energía eléctrica como los cortes de energía, para que así cuando un generador falle el otro generador sirve como respaldo y así evitar cualquier problema con respecto a la energía eléctrica.

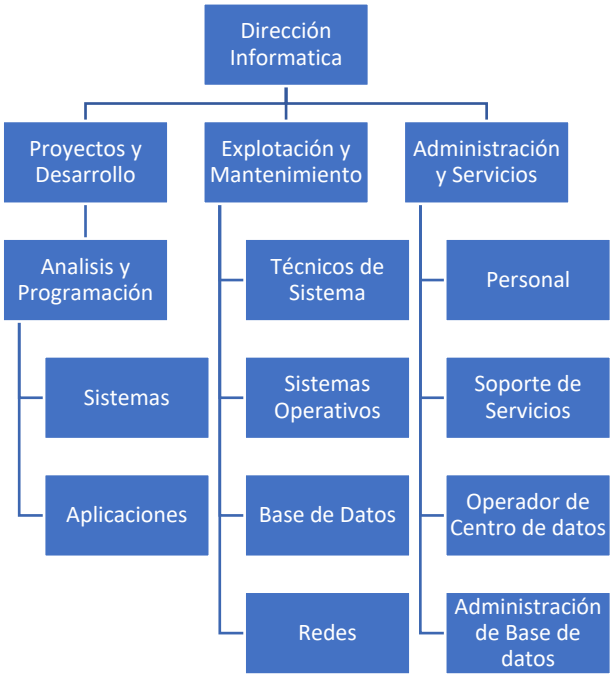
Con el sistema de iluminación también debe ser apropiado para evitar reflejos tanto en puertas de vidrio o en pantallas de los equipos por lo cual se recomienda utilizar la tecnología LED, también tener cuidado y evitar colocar el equipo a que sea expuesto al sol.

Con el equipo acústico también es importante mencionar de colocar aquellos equipos que generan ruido como impresora, aires acondicionados o cualquier tipo de equipo que genere vibraciones y colocarlos en un área aislada para que amortigüen dicho problema y no afecte a equipos sensibles por el ruido.

El Centro de Procesamiento de datos también debe contar con una excelente seguridad física como planes de contingencia para aquellas amenazas que afecten la infraestructura del CPD como los incendios y los desastres ambientales como inundaciones, terremotos etc.

ORGANIGRAMA FUNCIONAL EN CUMPLIMIENTO Y ANÁLISIS DE LA SEGREGACIÓN DE FUNCIONES

Representación gráfica del organigrama de la jerarquía entre las áreas de TI que conforma el Centro de Procesamiento de Datos de la Entidad Banca CityCorp.



SEGREGACION DE FUNCIONES

Con la segregación de funciones nos referimos a la separación de roles o cargos de los usuarios y personal del CPD que autoricen una transacción o proceso, con el objetivo de evitar que una misma persona tenga acceso y más de unas responsabilidades en los diferentes módulos dentro del sistema de información para así evitar cualquier riesgo de conductas irregulares que conlleven a un robo de información o fraude.

La segregación de funciones implicaría:

- CityCorp debe disponer de un manual de procedimientos y procesos de todas las funciones del organigrama tanto del CPD como en las totalidades sus áreas de trabajo, el cual cada persona tendrá sus responsabilidades de acuerdo al rol que desempeña en la organización.

- El recurso humano de CityCorp para un determinado cargo debe tener el perfil adecuado según el área que le corresponda para así el trabajo que este realice sea eficaz y eficiente.
- Cada persona debe conocer las funciones y responsabilidades que les son asignados.
- Respetar las jerarquías de la organización.
- Los usuarios en los sistemas de información deben contar con el mínimo privilegio, solo personal autorizado debería registrar, autorizar, modificar una transacción.
- Se debe identificar la distribución de las funciones dentro los procesos y diagramar todas las actividades que se realicen.

UBICACIÓN FUNCIONAL DE LAS ÁREAS TÉCNICAS Y PERSONAL A CARGO

El recurso humano es el recurso más importante que pueda tener una organización ya que con ello puede llevar a cabo todas sus actividades para cumplir sus objetivos y metas, por lo cual el personal de esta organización debe ser el adecuado y cumplir ciertos requisitos según el cargo que vaya desempeñar.

Director Informática:

Es el encargado de todo el funcionamiento del Centro de Procesamiento de datos, es el máximo responsable, se encarga de contratar el recurso humano en todas las áreas del CPD, de la estructura y de la dirección del personal, coordina las actividades y procesos que se realizan y controla los presupuesto.

Jefe del Área de Desarrollo

Es el encargado y el responsable de la creación de las aplicaciones o sistemas de información, se encarga de distribuir el personal a su cargo.

Jefe del Área de Explotación

Es el encargado del funcionamiento y explotación de los sistemas de información

Jefe de Proyectos

Trabaja de la mano con el jefe del área de Desarrollo

Jefe del Área Administración y Servicios

Encargado de la supervisión del soporte de los servicios brindados, operadores de centro de datos y de la administración de base de datos.

Técnicos de Sistemas

Su rol es el conocimiento profundo de los equipos y su sistema operativo para que estos siempre brinden los servicios de disponibilidad, confidencialidad, integridad.

Administrador de base de datos

Es el responsable de facilitar el uso de la base de datos a todo el personal autorizado, encargado también sobre asesoramiento de seguridad y uso de las bases de datos a los jefes de área, analistas. Es el encargado de toda la gestión de la base de datos.

Administrador de Sistemas

Es el responsable en controlar los permisos, roles y privilegios de los usuarios del personal informático que estarán utilizando los sistemas de información y hasta los sistemas operativos.

Analista de Sistemas

Es el encargado de realizar el respectivo análisis del diseño técnico y desarrollo de las aplicaciones, supervisar y ayudar a los programadores a poner en marcha en todo el ciclo de vida del desarrollo de sistemas.

Programadores

Son encargados de diseñar la aplicación por medio de diagramas de flujo, realizar el seudocódigo todo esto del análisis que haya realizado el analista de sistemas, codificando toda esta información a un lenguaje de programación para desarrollar la aplicación. También son los encargados de documentar todo el proceso de la puesta en marcha de la aplicación y los respectivos manuales para los usuarios a quienes va dirigido dicha aplicación.

Operadores

Es el responsable de poner en funcionamiento y operación directa de los sistemas de información, vela por la operatividad continua para que los servicios que presta el Centro de Procesamiento de Datos para que siempre estén disponibles para prevenir, resolver o alertar

apropiadamente los eventos. También es el encargado de monitorear los sistemas de la organización, coordinar llamadas entrantes para la resolución de problemas.

Grabadores de datos

Son los responsables de la carga y administración de los datos, también se le es conocido como transcriptores. Su jefe inmediato es el del Área de Explotación.

CityCorp debe tener una ubicación estratégica para El Centro de Procesamiento de datos debe tener un local físico adecuado y los siguientes requerimientos:

- Tener un espacio disponible y estratégico
- Acceso al equipo y al personal
- Tener un buen suministro eléctrico y un plan de contingencias cuando falle la energía eléctrica.
- Acondicionamiento térmico
- Mecanismos y controles de seguridad tanto físicamente como lógicamente.

CONTROLES GENERALES

Deben existir controles generales para un correcto funcionamiento de los sistemas de información y para el control de actividades y procesos que realicen en la organización creando un entorno adecuado y logrando los objetivos que la organización tiene estipulado.

Para ello se estarán modificando los controles 8.1.1, 9.1.1 y 9.3.2 mencionados en los antecedentes (ver Tabla), también se considera incorporar los controles que no existen.

Se identificará, analizara y evaluara los riesgos a los que los activos se enfrentan en la organización:

Activo	Descripción
Base de datos	Herramienta de recolección y organización de información confidencial de los clientes y usuarios de la organización
Sucursales	Oficinas o dependencia de la entidad bancaria en determinados lugares para la atención de sus clientes y usuarios.

Sistemas	Son las herramientas o mecanismos físicos o lógicas para realizar todos los procesos de las actividades para satisfacer las necesidades de clientes y organización.
Información / Datos	Conjunto de datos organizados y procesados que se utilizan para la toma de decisiones y así cumplir las metas de la organización.
Clientes / Proveedores	Personas u organizaciones que confían y apoyan a la organización para recibir u obtener un servicio.

Riesgos a los que puede se enfrentan los activos.

Activo	Riesgos
Base de datos	• Inyección de código malicioso • Ataques de Ingeniería Social • Explotación de Vulnerabilidades • Modificación, Eliminación de información • No cumplimiento de las normas y políticas.
Sucursales	
Sistemas	
Información / Datos	
Clientes / Proveedores	

Ahora analizaremos los controles para su modificación con el objetivo de la eficaz mitigación de los riesgos.

8.1.1. Inventario de Activos

Listar todos aquellos recursos tanto físicos como lógicos que tenga valor para la organización y priorizarlos para así realizar las debidas protecciones de seguridad y así poder mitigar los riesgos asociados a los activos. Se debe contar con un sistema de medición para medir la eficiencia mediante indicadores y clasificar los activos por categorías para una buena gestión del inventario de los activos.

9.1.1. Políticas de Control de Accesos

Implementar políticas de acceso de control tanto físicos y lógicos para evitar que personas no autorizadas puedan ingresar físicamente a las instalaciones, tanto usar los sistemas de información y realizar modificaciones o actividades sospechosas con el fin de mantener la seguridad de las instalaciones y sistemas de información.

9.3.1. Uso de información confidencial para la autenticación.

Según el objetivo de la (*Norma ISO 27002*, 2017) es controlar el acceso de los sistemas de información mediante restricciones y excepciones a la información y para impedir el acceso no autorizado al Sistema de Gestión de Seguridad de la Información se deberán implementar procedimientos formales para controlar los derechos y permisos en los accesos a cada sistema de información, base de datos, esto debe estar claro y bien documentado creando políticas funcionales. Los usuarios tienen que ser conscientes de sus responsabilidades durante el mantenimiento de los controles de acceso principalmente a la utilización de los mecanismos de autenticación que tenga que ver con el ingreso a sistemas mediante contraseñas, por ello es necesario la creación de políticas y procedimientos para evitar incidentes de flujo de información a personas ajenas de la organización, documentar y definir estrategias de forma clara las responsabilidades relativas a la seguridad de la información en todas las descripciones de los perfiles de cada puesto de trabajo.

11.1.1. Perímetro de seguridad física.

Definir una política general de seguridad de la información en la cual se debe estructurar una política específica sobre la seguridad física y del ambiente en la que oriente y defina las medidas y mecanismos de protección de la infraestructura, equipos contra amenazas físicas y del ambiente.

11.2.1. Emplazamiento y protección de equipos.

Los equipos deben estar en zonas estratégicas para que el personal se desplace de forma fluida y la zona brinde la protección al equipo para que se encuentre seguro ante los riesgos de las amenazas y peligros ambientales.

12.4.1. Registro y gestión de eventos de actividad.

Siguiendo con las normas («ISO 27002 punto por punto A12 Seguridad de las Operaciones», s. f.) se debe mantener un registro en todos los eventos de los sistemas de información como los accesos satisfactorios y fallidos, desconexiones del sistema, acciones ejecutadas, alertas por fallos del sistema, fecha y hora de los eventos, esto para prevenir cualquier incidente negativo y detectar actividades anómalas.

12.7.1. Controles de auditoría de los sistemas de información

Realizar auditorías técnicas sobre los sistemas de información para evaluar si los usuarios están trabajando con los privilegios correctos, la infraestructura es fiable y estable,

mecanismos de seguridad correctos, los monitoreos, pruebas y mantenimientos se realizan eficientemente, etc.

13.1.1. Controles de red.

Con base a la Norma ISO (27002, 2017) se debe crear políticas generales y especificas en cuanto a la definición de las responsabilidades, procedimientos para que las redes sean gestionadas y controladas para proteger la información en los sistemas y aplicaciones.

16.1.1. Responsabilidades y procedimientos

Establecer responsabilidades y procedimientos de gestión en base a la Norma ISO (27002, 2017) para garantizar una respuesta rápida y efectiva a los incidentes que se puedan suscitar en los sistemas de información, realizar procedimientos para la planificación, para monitorear, analizar, detectar, evaluar los incidentes o eventos de seguridad y registrar todo proceso que se realice.

18.1.4. Protección de datos y privacidad de la información personal.

Garantizar y la protección de datos implementando políticas de privacidad para proteger la información personal del usuario, clientes y proveedores.

CONCLUSIONES DEL ESTUDIO

El Centro de Procesamiento de Datos es una localización centralizada donde los equipos de cómputo, redes, sistemas de información se concentran con el propósito de almacenar, procesar, distribuir y permitir el acceso a grandes cantidades de datos para brindar servicios de calidad a cualquier organización. Las ventajas que tiene una empresa implementando un CPD son: Tecnología, Seguridad, Conectividad y Eficiencia

Cada año que pasa la inversión en Centro de Procesamiento de Datos aumenta de forma paulatina durante el periodo, de forma que en el año 2020 se invirtieron 220.000 millones de dólares incrementando 5.000 millones con respecto al año anterior. (*Data centers*, s. f.)

Se identifico y menciono sobre el nivel del CPD Tier 4 con la infraestructura que debe contener, se identificaron los activos y los riesgos a los que esta expuestos y los controles para poder mitigar los riesgos con el objetivo de lograr los objetivos de la entidad bancaria CityCorp. Mencionamos los cargos importantes del CPD y definimos los perfiles importantes dentro de un CPD, y los controles generales que la organización tiene y cuales implementar.

Es importante que una organización tenga políticas y normas establecidas para el buen uso de los controles y mecanismos de seguridad ya que con ello facilitara y una buena gestión de los sistemas de información y telecomunicaciones con las que cuenta la empresa.

REFERENCIAS

- *ISO 27001: La implementación de un Sistema de Gestión de Seguridad de la Información*. (2015, enero 28). PMG SSI - ISO 27001. https://www.pmg-ssi.com/2015/01/iso-27001-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/
- *La segregación de funciones. Aspecto clave de control en los procesos de la organización*. (s. f.). Recuperado 11 de noviembre de 2021, de https://www.auditool.org/blog/control-interno/4228-la-segregacion-de-funciones-aspecto-clave-de-control-en-los-procesos-de-la-organizacion
- *Data centers: Inversión mundial 2012-2022*. (s. f.). Statista. Recuperado 25 de noviembre de 2021, de https://es.statista.com/estadisticas/875229/inversion-mundial-en-data-centers/
- ISO 27002 punto por punto A12 Seguridad de las Operaciones. (s. f.). *ISO 27001*. Recuperado 25 de noviembre de 2021, de https://normaiso27001.es/a12-seguridad-de-las-operaciones/
- *Norma ISO 27002: Control de accesos*. (2017, agosto 31). PMG SSI - ISO 27001. https://www.pmg-ssi.com/2017/08/norma-iso-27002-control-de-accesos/
- *Archivos*. (s. f.). Recuperado 27 de noviembre de 2021, de https://micampus.unir.net/courses/22815/files/folder/Grupos%2039%20al%2042%20(Sergio%20Sentecal)/Actividad%3A%20Estructuraci%C3%B3n%20funcional%20de%20un%20CPD?preview=4353257

- 27002, I. (mayo de 2017). *UNE-EN ISO/IEC 27002*. Obtenido de https://static.eoi.es/inline/une-en_iso-iec_27002_norma_mincotur.pdf