REPOSITORIO ACADÉMICO UPC

Gestión de la seguridad física y lógica para un centro de datos

Item Type	info:eu-repo/semantics/bachelorThesis
Authors	Flores Esteves, Jack Shannon; Puppi Becerra, Gino Alfredo
Publisher	Universidad Peruana de Ciencias Aplicadas (UPC)
Rights	info:eu-repo/semantics/openAccess
Download date	24/09/2020 22:45:32
Item License	http://creativecommons.org/licenses/by-nc-nd/4.0/
Link to Item	http://hdl.handle.net/10757/301540

UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS
Laureate International Universities®

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

Gestión de la seguridad física y lógica para un centro de datos

PROYECTO PROFESIONAL

Para obtener el Título de:

INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTORES:

Flores Esteves, Jack Shannon

Puppi Becerra, Gino Alfredo

ASESOR:

Villalta Riega, Rosario del Pilar

LIMA – PERÚ

2013

DEDICATORIA

El proyecto Gestión de la Seguridad Física y Lógica para un Centro de Datos, se lo dedicamos a nuestros padres y hermanos, quienes nos han apoyado a lo largo de nuestra vida y en especial por el apoyo y enseñanzas brindadas, las cuales nos han ayudado a superar todos los problemas y obstáculos que hemos encontrado. También queremos agradecerles por el apoyo que nos brindan para seguir adelante, lo que nos permite crecer como personas y profesionales.

Por otro lado, queremos agradeceré a todos los profesionales que de una u otra forma nos han apoyado con sus enseñanzas a lo largo de los cinco años de nuestra carrera profesional, compartiendo con nosotros su experiencia y así mejorar mutuamente.

TABLA DE CONTENIDO

RESUMEN EJECUTIVO **7**

ABSTRACT **9**

INTRODUCCION **11**

CAPÍTULO 1: DECLARACIÓN DEL PROYECTO **13**

OBJETO DE ESTUDIO 13

DOMINIO DEL PROBLEMA 13

Planteamiento de la Solución *13*

OBJETIVOS DEL PROYECTO 14

Objetivo general *14*

Objetivos específicos *14*

INDICADORES DE ÉXITO 14

PLANIFICACIÓN DEL PROYECTO 14

Alcance del Proyecto *14*

EQUIPO DE PROYECTO 16

RIESGO DEL PROYECTO 16

CAPÍTULO 2: MARCO TEÓRICO **18**

MARCO TEÓRICO 18

ANÁLISIS DE ESTÁNDARES Y NORMAS 23

EUP (Enterprise Unified Process) *23*

PMBOK (Project Management Body of Knowledge) *24*

BPMN (Business Process Modeling Notation) *25*

TIA (Telecommunications Industry Association) *28*

ITIL (Information Technology Infrastructure Library) *28*

ISO 27001 - NTP 17799 - ISO/IEC 17799:2005 ..... *35*

CAPÍTULO 3: SEGURIDAD FÍSICA Y LÓGICA **37**

METODOLOGÍA DE TRABAJO 37

MAPA DE PROCESOS 42

DIAGRAMA DE OBJETIVOS 43

SEGURIDAD A NIVEL FÍSICO 44

Diseño de la evaluación y del Checklist *44*

Subsistema de Arquitectura 46

Subsistema Eléctrico 59
Subsistema de Telecomunicaciones 90
Niveles de calificación de la evaluación 92
Resultados de la Evaluación 95
Interpretación de Resultados 123
Procesos de la gestión de la seguridad física 126
Definición de Procesos: Gestión de Evaluación de Seguridad 126
Definición de Procesos: Control de ingresos 135
Definición de Procesos: Revisión de Equipos 142
Definición de Procesos: Control de Protección Ambiental 153
Definición de Procesos: Gestión de solicitud de accesos 161
Política de Seguridad Física 168
Introducción 168
Alcance 168
Acrónimos y definiciones 168
Objetivos 168
Objetivo General 168
Objetivos Específicos 168
Enunciado de la Política 169
Responsabilidades 169
Violaciones a la política 169
Conceptos y directrices sobre la Política de Seguridad Física 170
Protección Física de Accesos 170
Controles de Acceso Físico 170
Desarrollo de Tareas en el Centro de datos 171
Protección ambiental 171
Perímetro de Seguridad Física 172
Suministros de energía 172
Seguridad del cableado 173
Protección de las Instalaciones 174
Transporte, protección, y mantenimiento de los equipos y documentación 175
Mantenimiento de equipos 175
Retiro de los equipos e información 175
Desafectación o reutilización segura de los equipos 176
Ubicación y protección de los equipos y copias de seguridad 177
Mapeo de procesos con directrices físicas 178
SEGURIDAD A NIVEL LÓGICO 179
Diseño de la evaluación y del Checklist 179
Interpretación de Resultados 192
Procesos de la gestión de la seguridad lógica 194
Definición de Procesos: Gestión de solicitud de respaldo de información 194

Definición de Procesos: Administración de Vulnerabilidades y Parches 207
Definición de Procesos: Gestión de Solicitud de Accesos Lógico 214
Definición de Procesos: Monitoreo de Componentes 221
Definición de Procesos: Gestión de Pruebas de Seguridad 231
Definición de Procesos: Restauración de Backup 238
Definición de Procesos: Control de Vulnerabilidades Técnicas 245
Definición de Procesos: Gestión de Claves 253
Definición de Procesos: Revisión e Instalación de Software 262
Política de Seguridad Lógica 271
Introducción 271
Alcance 271
Acrónimos y definiciones 271
Objetivos 271
Objetivo General 271
Objetivos Específicos 271
Enunciado de la Política 272
Responsabilidades 272
Violaciones a la política 272
Conceptos y directrices sobre la Política de Seguridad Lógica 272
Gestión de Comunicaciones y Operaciones 272
Protección contra software malicioso 272
Gestión de respaldo y recuperación 273
Gestión de seguridad en redes 273
Utilización de medios de información 274
Monitoreo 274
Control de Accesos 275
Responsabilidades de los usuarios 275
Gestión de acceso de usuarios 276
Control de acceso a la red 276
Control de acceso al sistema operativo 277
Control de acceso a las aplicaciones y la información 277
Adquisición y mantenimiento de sistemas 277
Requisitos de seguridad de los sistemas 278
Controles criptográficos 278
Seguridad de los archivos del sistema 278
Gestión de la vulnerabilidad técnica 279
Mapeo de procesos con directrices lógicas 280
CAPÍTULO 4: CONTINUIDAD Y CIERRE DEL PROYECTO 282
CONTINUIDAD DEL PROYECTO 282
INTERACCIONES CON OTROS PROYECTOS 282
DEFINICIÓN DE ROL Y MANUAL DE FUNCIONES 287

Información del Rol *287*
Definición 287
Funciones 287
Proceso Control de ingresos 287
Proceso Revisión de Equipos 287
Proceso Control de Protección Ambiental 288
Proceso Revisión e instalación de software 288
Proceso Control de Vulnerabilidades Técnicas 289
Proceso Gestión de Claves 289
Proceso Gestión de Solicitud de Accesos 289
Proceso Gestión de solicitud de respaldo de información 290
Proceso Administración de Vulnerabilidades y Parches 290
Proceso Gestión de Solicitud de Procesos Lógicos 291
Proceso Monitoreo de Componentes 291
Proceso Gestión de Pruebas de Seguridad 291
Proceso de Restauración de Backup 292
Proceso Control de Vulnerabilidades Técnicas 292
Assessment de Seguridad 292
CONCLUSIONES 304
RECOMENDACIONES 306
BIBLIOGRAFÍA 307
ANEXOS 310
ANEXO 1 310
ANEXO 2 317
ANEXO 3 ..... *326*

RESUMEN EJECUTIVO

El contenido del presente documento describe el trabajo realizado en el proyecto "Gestión de la Seguridad Física y Lógica para un Centro de Datos" desarrollado en la empresa virtual IT-Expert. La aplicación de este proyecto permitirá establecer roles, procesos y políticas para gestionar de manera adecuada un centro de datos pequeño, el caso de análisis es el centro de datos de la carrera de ingeniería de sistemas y software durante el segundo semestre del año 2010 y el primer semestre del año 2011.

La primera problemática a resolver era como cuantificar y detallar el estado actual del centro de datos analizado. Un componente esencial en este análisis era estudiar y revisar la información de los procesos que rigen la operativa del centro, las directrices y/o políticas establecidas y los activos o recursos que forman parte del caso de análisis. Para determinar cuál es el estado real del centro de datos, fue necesario investigar acerca de estándares y/o normas internacionales y nacionales, las cuales son la base del presente trabajo.

Al concluir la investigación, se hizo evidente que no existe un único estándar que asegure la gestión de la seguridad (física y lógica) para un centro de datos pequeño. Por lo que el proyecto determinó que debe tener múltiples fuentes y que éstas deben recoger ambos tipos de seguridad. El estándar más importante acerca de la seguridad en servidores y centro de datos, es la TIA-942, estándar reconocido mundialmente y sobre el cual los mejores y más avanzados centros de datos del mundo basan la gestión de la seguridad Otro estándar importante que trabaja la seguridad pero enfocado en su componente lógico es la NTP-ISO/IEC 17799:2007, el cual es una adopción de la norma ISO/IEC 17799:2005 Information Technology – Code of Practice for Information Security Management.

Con los estándares definidos, se inició la evaluación del centro de datos, con el objetivo de definir su estado real y establecer medidas para subsanar las observaciones encontradas. Se crearon dos checklist basados en los estándares y normas mencionados, cada uno de ellos se especializa en un enfoque de la seguridad. Esta evaluación brindará la pauta de lo que debe gestionarse en el corto, mediano y largo plazo. Los resultados de ambos checklist no fueron los esperados. El resultado estableció que ambos frentes de la seguridad estaban en su nivel más bajo y para levantar estas observaciones se necesitaba

trabajar sobre las recomendaciones catalogadas como mínimas. Por otro lado, se hizo evidente que era necesario establecer directrices, políticas y procesos que permita hablar de un centro de datos y no de una sala de computadoras, lo cual sería posible únicamente si se adoptan los niveles de seguridad sugeridos.

Uno de los principales entregables del proyecto, es la política –la misma que cubre los dos frentes de seguridad- basándola en la norma NTP-ISO/IEC 17799:2007. Al tener la política instaurada, se definieron y crearon los procesos que brinden soporte a las directrices de estas políticas; con la definición del proceso, fue necesario definir los roles para finalmente formar un estándar aplicable a centro de datos pequeños.

Por último, se han listado algunas recomendaciones y conclusiones del proyecto así como también un manual de funciones del rol del oficial de seguridad. Con el objetivo de continuar con esta iniciativa, se ha esquematizado y definido en un capitulo la continuidad del proyecto. Adicionalmente, se ha creado un assessment de seguridad con el fin de verificar que los cambios sugeridos por el proyecto se hayan llevado a cabo y ayudar a que cada ciclo se retroalimente la gestión de la seguridad con los nuevos requerimientos, incidencias, evaluaciones, etc.

ABSTRACT

The contents of this document describes the work done in the project of “Gestión de la Seguridad Física y Lógica para un Centro de Datos” developed in the virtual enterprise IT-Expert. The implementation of this project will establish roles, processes and policies to properly manage a small data center; the case analysis is the data center of the career of information systems and software engineering in 2011.

The first problem to solve was to quantify and detail the current state of the data center analyzed. An essential component of this analysis is to study and review the information governing the operational processes, guidelines or policies established and the assets or resources that are part of the case of analysis. To determine the actual state of the data center, it was necessary to investigate standards and international / national standards, which are the basis for establishing policies and processes within the data center.

As a result of this investigation, it was concluded that there is no single standard that ensures the management of a small data center around physical security as well as logical security. So, after investigation, it was determined that the project should be based on several standards and that it must collect both types of security. The most important standard is TIA-942, globally recognized standard and on which the best and most advanced data centers in the world base security management to be applied. Another important standard safety working but focused on its logical component is the NTP-ISO/IEC 17799:2007, which is an adoption of ISO / IEC 17799:2005 Information Technology - Code of Practice for Information Security Management.

With the defined standards, the project team began the data center assessment, with the aim of defining its actual state and establishes measures to address the observations found. We performed 2 checklist based on the standards and rules mentioned, each checklist specializing in each approach to security. This evaluation will provide the standard of what should be managed in the short, medium and long term. The results of both checklists were not as expected; the results established that both security fronts were at their lowest level and raise these observations that are needed to work on the recommendations listed as minimum to have an "acceptable" level of security. On the

other hand, it became clear that they should establish guidelines, policies and processes that allow talk of a data center and not a computer room; this would be possible only if adopted safety levels suggested.
The project team developed a policy for the two mentioned security fronts, basing on NTP-ISO/IEC 17799:2007 standard. Having the project team defined this policy; processes have been created to provide support to the guidelines of these policies, with the definition of the process, it was necessary to define the roles to finally form a standard applicable to small data center.

Finally, we have listed some recommendations and conclusions of the project as well as a functions manual of the role of the “Oficial de Seguridad”. In order to continue this initiative has been outlined and defined in a chapter called “Continuidad del Proyecto”. Additionally, it has created a security assessment in order to verify that the changes suggested by the project have been carried out and help each cycle feedback security management with new requirements, incidents, assessments, etc.

INTRODUCCION

El presente documento corresponde a la memoria del proyecto “Gestión de la Seguridad Física y Lógica para un Centro de Datos”, el cual tiene como objetivo la definición de un estándar que asegure la gestión de la seguridad tanto a nivel físico como a nivel lógico para un centro de datos.

Este proyecto es parte de los cursos Taller de Proyecto I y Taller de Proyecto II, los cuales son obligatorios en la malla curricular de la carrera de Ingeniería de Sistemas de Información de la Universidad Peruana de Ciencias Aplicadas. Dentro de estos cursos se maneja el concepto de empresa virtual, cada una de ellas tiene rubros y objetivos definidos. La empresa virtual encargada de los proyectos de Tecnologías de Información es IT-Expert, el objetivo central de esta empresa es brindar servicios tecnológicos de calidad al resto de las empresas virtuales. Este objetivo se soporta en la gestión de diversos proyectos y en la creación de nuevos servicios.

Este proyecto ha sido elegido como un proyecto viable por la importancia que va cobrando día a día la información en cualquier empresa alrededor del mundo, por la falta de estándares de seguridad para empresas medianas o pequeñas y porqué en la actualidad no se puede determinar si existen procedimientos, normas y/o políticas sobre la seguridad física y lógica en el centro de datos. Esto genera que no se puede asegurar la seguridad de cada activo presente en el centro de datos de la carrera de Ingeniería de Sistemas de Información de la UPC.

El primer capítulo corresponde al marco teórico, este capítulo brinda las definiciones claves acerca de los conceptos de seguridad, estándar, las partes que contiene un estándar; las actividades que corresponden a la seguridad (física y lógica) y cuáles son los estándares más conocidos en cuanto a la seguridad. Por otro lado, también se encontrará el dominio del problema, el planteamiento de la solución, los objetivos y la justificación del proyecto.

El segundo capítulo corresponde a la descripción en sí del proyecto. En este capítulo se detallará la metodología a utilizar, la misma que es una mezcla entre diversos marcos referenciales tales como Enterprise Unified Process (EUP), Project Management Body

of Knowledge (PMBOK), Telecommunications Industry Association (TIA), International Organization for Standardization ISO17799. Por otro lado también se detalla la organización del proyecto; el alcance y los riesgos.

El tercer capítulo corresponde a la aplicación de la metodología de trabajo y la formulación del estándar personalizado, parte de esta metodología involucra la creación de un checklist para evaluar el centro de datos a nivel físico, la interpretación de resultados, la nueva escala creada; el resultado de la evaluación; la política de seguridad física; los procesos que apoyan a la seguridad física y un mapeo de objetivos con aspectos específicos de la ISO. La misma estructura se sigue para la seguridad lógica.

Finalmente en el último capítulo se brindan recomendaciones, se presenta el resultado del assessment y como mantener el proyecto a lo largo del tiempo.

CAPÍTULO 1: DECLARACIÓN DEL PROYECTO

En el primer capítulo se encontrará la declaración del proyecto, la cual permitirá conocer y comprende el contexto del análisis utilizado en el proyecto.

Objeto de Estudio

"Determinar si existe un estándar que gestione de manera adecuada la seguridad lógica y física para centro de datos de pequeña y mediana envergadura aplicable a las empresas peruanas".

Dominio del Problema

El problema se basa en la poca o la falta de seguridad a nivel físico y lógico que posee el centro de datos de la carrera de Ingeniería de Sistemas de Información. Este déficit se debe principalmente a que en el momento del estudio no se contaba con procesos, directrices, políticas, delimitación de responsabilidades ni estándares a seguir.

Planteamiento de la Solución

La solución planteada para el problema antes detallado consiste en desarrollar una metodología de trabajo y evaluación, para así definir los procesos, las políticas y los roles de manera que estos sean aplicables y escalables a centros de datos de baja y mediana envergadura a nivel nacional.

Esta metodología está conformada por un sistema de evaluación a medida, construido a partir de las mejores prácticas descritas en la TIA 942, ITIL, NTP 17799 y el Orange Book. Al modificar, depurar y establecer las nuevas pautas a seguir, es necesario modificar el sistema de evaluación o checklist y crear un esquema de calificación acorde a las modificaciones realizadas. Esto genera que la metodología incluya un nuevo modelo de calificación e interpretación de resultados. Adicionalmente, es necesario definir cuáles serán los procesos mínimos requeridos para gestionar la seguridad física y lógica en un centro de datos. Estos procesos serán modelados según la notación BPMN y bajo el enfoque de gestión del BPM.

Objetivos del Proyecto

Objetivo general

Evaluar y diseñar los procesos, controles y procedimientos que formarán parte de un estándar para gestionar la seguridad física (seguridad ambiental, control de acceso, monitoreo, etc.) y la seguridad lógica (permisos en aplicativos, compartidos, bases de datos, roles, etc.) en el centro de datos de la carrera de Ingeniería de Sistemas de Información.

Objetivos específicos

1. Evaluar el estado actual del centro de datos de la carrera.
2. Definir los procesos que regirán a la gestión de seguridad lógica y física.
3. Integrar los conceptos de la NTP 17799 y la TIA 942, para la creación de un estándar a usar en el centro de datos de la carrera.

Indicadores de éxito.

- Reducir las observaciones encontradas en un 25% como mínimo.
- Obtener la conformidad de los encargados del centro de datos sobre las evaluaciones realizadas y los resultados obtenidos.
- Visar la metodología utilizada por un experto en el ámbito de la gestión de la seguridad.

Planificación del Proyecto

Alcance del Proyecto

El alcance del proyecto incluirá:

1. Evaluación de la situación actual del centro de datos de la carrera con base en los niveles del Tier. Referenciar la norma.
2. Creación de un estándar personalizado, para el control de la seguridad lógica y física del centro de datos de la carrera Ingeniería de Sistemas.

3. Desarrollo de los diagramas de procesos de seguridad lógica acordes al EBM.

4. Definición de controles que deben cumplirse para llegar determinado, considerando el no generar conflictos con los sistemas desplegados.

5. El proyecto solo involucrará el centro de datos de la carrera de Ing. De Sistemas de Información y Software.

6. Se entregará una relación de sugerencias a nivel físico para que sean evaluadas en cuanto a costo/beneficio por el director de la carrera, debido a que no se cuenta con presupuesto asignado.

El Alcance del proyecto NO incluirá:

1. La creación de un software.

2. La adquisición o implementación de algún componente de hardware o software.

3. La seguridad de las empresas virtuales ni los laboratorios asignados a los cursos de Talleres.

4. Sugerencias o mejoras sobre aspectos del centro de datos que se encuentren bajo responsabilidad de Servicios Generales.

Equipo de Proyecto

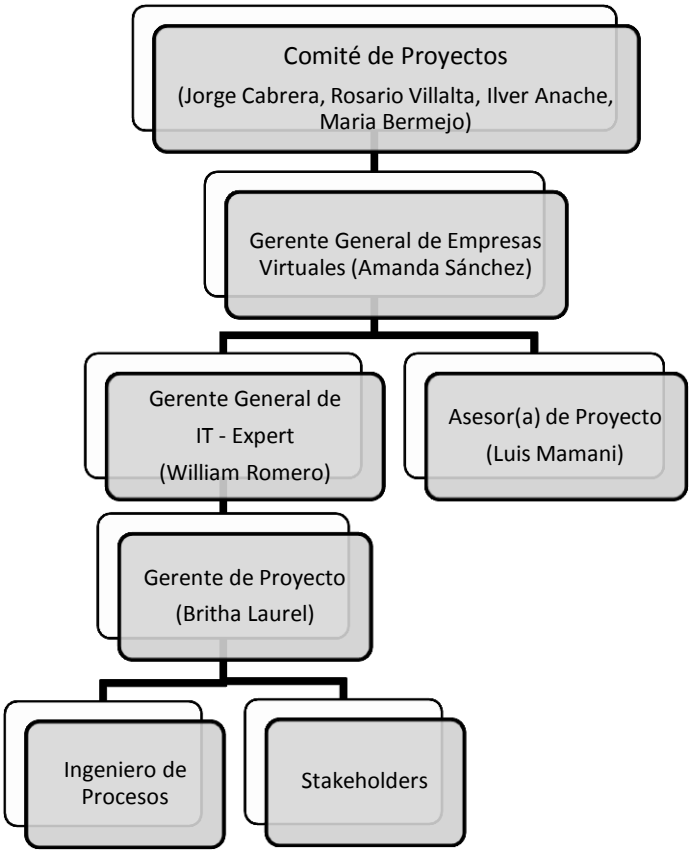


Imagen 01: Equipo de Proyecto

Fuente: Elaboración Propia

Riesgo del Proyecto

1. El contrato de validación y verificación firmado con QA caduque antes del fin de la inspección.

2. La inspección realizada por parte de QA sea incorrecta.

3. Disponibilidad de tiempo de los usuarios finales, para las reuniones de captura de requerimientos (niveles de seguridad, accesos, roles, etc.) y reuniones de control del avance del proyecto.

4. La aceptación o continuidad del proyecto estará a cargo del comité de proyectos.

5. Incertidumbre por parte de los Stakeholders para definir los requerimientos mínimos.

CAPÍTULO 2: MARCO TEÓRICO

En el segundo capítulo encontraran, el marco teórico, el cual permitirá comprender con mayor detalle lo que involucra un estándar para la gestión de la seguridad, un análisis de las normas y estándares utilizados.

Marco Teórico

Para entender a plenitud el enfoque y alcance del proyecto se debe tener una idea clara de los conceptos con los que se trabajará a lo largo de este documento, por lo que se ha creído conveniente la elaboración de un breve marco teórico que introducirá los términos usados tales como estándar, seguridad y dentro de este los de seguridad física y seguridad lógica, entre otros.

De acuerdo con la definición de la Real Academia Española, estándar es aquello que sirve como tipo, modelo, norma, patrón o referencia[1]. Así mismo, se puede asociar al significado moderno de esta palabra que denota lo que es establecido por la autoridad, la costumbre o el consentimiento general. En este sentido se utiliza como sinónimo de norma.

La palabra estándar proviene del inglés *standard*, y si se interpreta desde el punto de vista tecnológico, que es el enfoque que se le va a dar en el presente documento, debe entenderse como una especificación que regula la realización de ciertos procedimientos, de tal forma que garantice la interoperabilidad entre diversas plataformas, la continuidad de los productos desplegados en los diversos ambientes (producción, desarrollo y pruebas) y el correcto funcionamiento de todas y cada una de las partes de dicho proceso.

Actualmente existen entidades, tales como la International Organization for Standardization (ISO), American National Standards Institute (ANSI), Energy Information Administration (EIA), que comparten el objetivo de definir los patrones, modelos, pasos o pautas que se deben seguir para poder efectuar una adecuada gestión de la seguridad física y lógica. El producto final de dichas entidades son normas o

[1] Cfr. Real Academia Española 2011

estándares que son aceptados y regulados bajo varios organismos de diversos países, los mismos que proponen una solución eficaz a cualquier problema o determinar la forma adecuada de minimizar su ocurrencia e impacto.

El presente proyecto trabaja alrededor del concepto de seguridad, seguridad física y lógica, pero que involucra la seguridad, según la Real Academia Española de la Lengua, este término hace referencia a la cualidad de seguro que tiene algo[2].

Sin embargo, el uso que se le da a este término en el presente documento tiene un enfoque diferente. No existe una definición estricta de lo que se entiende por seguridad, puesto que ésta abarca múltiples y muy diversas áreas relacionadas que van desde la protección física del ordenador como componentes hardware, hasta la protección de la información que contiene o de las redes que lo comunican con el exterior.[3] En este documento cada vez que se referencie a la palabra seguridad será desde el enfoque que menciona la Universidad de Ciencias Exactas y Naturales y Agrimensura, es decir:

> "(…) [Se puede entender la seguridad como] una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. (…) [Cuando se habla de sistemas] se suaviza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) más que de seguridad; por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros." (Universidad de Ciencias Exactas y Naturales y Agrimensura 2011)

Este concepto de seguridad lo comparten el Dr. Lucio Molinas Focazzio, el cual define la seguridad como el hecho de asegurar que los recursos informáticos de cualquier empresa puedan y siempre cumplan con los propósitos por los cuales fueron diseñados sin ser alterados por circunstancias o factores externos[4] y el magister Alejandro Rodríguez, el cual menciona que seguridad es:

> "[Es el] conjunto de medidas (administrativas, organizativas, físicas, técnicas legales y educativas) dirigidas a prevenir, detectar y responder a las acciones que pongan en riesgo la integridad, confidencialidad y disponibilidad, de la informatización que se procesa, intercambie, reproduzca o conserve a través de las tecnologías de la información." (Rodríguez, Alejandro 2011)

---

[2] Cfr. Real Academia Española 2011
[3] Cfr. Universidad Técnica Particular de Loja 2011
[4] Cfr. Molinas, Lucio 2011

El concepto de seguridad informática, se puede disgregar dos conceptos, los mismos que son el eje central de este proyecto, es decir la seguridad física y la seguridad lógica.

Por un lado, al definir la seguridad física es ideal tomar como base el concepto al que hace mención la Universidad de Valencia, esta universidad la define como:

> "(…) todos aquellos mecanismos --generalmente de prevención y detección-- destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un simple teclado hasta una cinta de respaldo con toda la información que hay en el sistema, pasando por la propia CPU de la máquina. Dependiendo del entorno y los sistemas a proteger esta seguridad será más o menos importante y restrictiva, aunque siempre deberemos tenerla en cuenta." (Universidad de Valencia 2011)

Sin embargo, esta definición centraliza el concepto de seguridad física únicamente al ámbito de la protección de información, por eso se debe complementar con el cuidado y los procedimientos necesarios para asegurar la infraestructura de los sistemas, es decir estructura física, cableado, redes, UPS, entre otros.

Por otro lado, tal como lo dice Universidad Técnica Particular de Loja, no solo basta asegurar los sistemas sobre la seguridad física sino que esta se debe completar con la seguridad lógica, ya que la mayoría de los daños que puede sufrir un centro de cómputo no será sobre los medios físicos sino contra información por él almacenada y procesada[5]. Para esta universidad el concepto de seguridad lógica gira en torno a la aplicación de defensas y procedimientos que resguarden el acceso a los datos y solo permita acceder a las personas autorizadas para hacerlo.[6]

La seguridad lógica debe tener sus objetivos definidos de manera coherente, es decir los procedimientos implementados deben apoyar a los objetivos de seguridad por los cuales estas medidas fueron implementadas.

> "[Según la Universidad Técnica Privada de Loja, las principales funciones de la seguridad lógica son:]
>
> Restringir el acceso a los programas y archivos.

[5] Cfr. Universidad Técnica Particular de Loja 2011
[6] Cfr. Universidad Técnica Particular de Loja 2011

> Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
>
> Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
>
> Que la información transmitida sea recibida por el destinatario al cual ha sido enviada y no a otro.
>
> Que la información recibida sea la misma que ha sido transmitida.
>
> Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
>
> Que se disponga de pasos alternativos de emergencia para la transmisión de información." (Universidad Técnica Privada de Loja 2011)

Si se juntan estas dos definiciones, se puede llegar a la conclusión que un estándar para la gestión de la seguridad física y lógica es el conjunto de criterios, normas, procedimiento que determinan como se deben llevar a cabo todas las actividades y cuál es la infraestructura adecuada con la que debe contar un centro de datos. Es decir, la seguridad nos define los activos y los procesos para salvaguardar la Seguridad Física y Lógica.

Si se considera que existen diversas formas de gestionar la seguridad física y lógica ¿cómo se puede asegurar que se tiene una gestión adecuada? La respuesta correcta, es el seguimiento de los estándares. Existe una gran variedad de estándares que definen procesos, procedimientos, normas, políticas e infraestructura para gestionar la seguridad física y lógica. El estándar más completo en el ámbito de la seguridad física es el TIA 942 el cual es la fuente principal sobre la cual se determinará qué acciones se deben llevar a cabo en el centro de datos de la carrera para una gestión de la seguridad física.

La norma TIA 942 define niveles de seguridad conocidos como *tiers*, estos niveles van desde el número uno hasta el número cuatro, siendo este último el más completo asegurando una alta tolerancia a fallas y una disponibilidad del 99.995%[7]

Se debe tener en cuenta que para poder diseñar el estándar que debería ser implementado según la TIA 942, se deben tener como guía diversos estándares de

[7] Cfr. TIA 942 White Paper 2011

seguridad como el ISO 27000 ya que este es la base de la TIA 942. Este estándar base, brinda la primera perspectiva de la norma, sin embargo, tiene su par peruana en la NTP 17799, la misma que ha sido diseñada con base en la realidad peruana. La norma técnica peruana define los requisitos mínimos que se deben tener en cuenta al momento de diseñar un centro de datos y así para controlar la seguridad física.

Para poder analizar si un centro de cómputo tiene implementadas de forma correcta las sugerencias de la TIA, se puede realizar una evaluación.

Al implementar estas medidas de seguridad física se está dejando de lado el aspecto lógico de la gestión de la seguridad ya que la parte física es sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como se sabe el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física que la aseguren. Estas técnicas las brinda la Seguridad Lógica[8].

Por otro lado, para gestionar la seguridad lógica existen diversas soluciones, las mismas que serán cubiertas dentro del alcance del proyecto, tales como:

1. Investigación para las soluciones de infecciones virales.
2. Políticas de uso de programas y de información compartida.
3. Políticas de administración del sistema de seguridad.
4. Políticas para el control de LAN públicas y privadas.
5. Políticas para la utilización de puertos.
6. Definición de planes de respaldo y contingencia.
7. Planificación de Capacitación a los usuarios finales.

Al momento de diseñar las medidas de seguridad lógica se va a seguir una estructura de trabajo ya definida, la misma que ha sido generada a partir de una mezcla entre las sugerencias de la Universidad Técnica Particular de Loja y la metodología de trabajo de los integrantes del proyecto, esta estructura consiste en:

[8] Cfr. Universidad Técnica Particular de Loja 2011

1. Realizar un análisis de riesgos.
2. Cuantificación de riesgos.
3. Programa de control de riesgos.
4. Definición de políticas.
5. Implementación de políticas y normas.
6. Definición de planes (contingencia, continuidad y recuperación).
7. Auditoría interna.

Con esta serie de pasos se podrá asegurar que la gestión de la seguridad lógica se ha llevado a cabo de manera correcta y considerando todos los aspectos necesarios. El objetivo de estas medidas de seguridad es asegurar la continuidad del centro de datos de la carrera.

Finalmente, para tener imparcialidad y un resultado real sobre la gestión de seguridad física y lógica, se va brindar al proyecto Auditoría de TI de la empresa IT-Expert toda la información respectiva al proyecto para que pueda realizar su auditoría sobre la gestión de la seguridad física y lógica en el centro de cómputo de la carrera.

Análisis de Estándares y Normas

EUP (Enterprise Unified Process)

El EUP es una extensión del Rational Unified Process (RUP), estándar de proceso de desarrollo de software, donde se incluyen dos nuevas fases las cuales son Producción y Retiro, así también como nuevas disciplinas, dentro de las cuales encontramos las siete disciplinas empresariales, las mismas que son:

1. Modelamiento Empresarial
2. Gestión del Portafolio
3. Arquitectura Empresarial

4. Reuso
5. Gestión de Personas
6. Administración Empresarial
7. Mejora de Procesos de Software

Asimismo, el EUP permite explorar los procesos de negocios, el ambiente externo, la estructura de la organización, y las entidades empresariales críticas pertenecientes a la organización.

PMBOK (Project Management Body of Knowledge)

El Project Management Body of Knowledge (PMBOK) es un estándar desarrollado por el Project Management Institute, que brinda un conjunto de buenas prácticas para la gestión de proyectos. Estas mejores prácticas se dividen en áreas de conocimiento, las mismas que son comunes para los proyectos. Las áreas de conocimiento son las siguientes:

1. Gestión de la Integración del Proyecto
2. Gestión del Alcance del Proyecto
3. Gestión del Tiempo del Proyecto
4. Gestión de los Costos del Proyecto
5. Gestión de la Calidad del Proyecto
6. Gestión de los Recursos Humanos del Proyecto
7. Gestión de las Comunicaciones del Proyecto
8. Gestión de los Riegos del Proyecto
9. Gestión de las Adquisiciones del Proyecto

Durante el ciclo de vida del proyecto se podrán considerar las buenas prácticas en la mayoría de las áreas del conocimiento. La Gestión de los Costos y Adquisiciones del Proyecto no serán tomadas en cuenta como referencia por tratarse de un proyecto académico en el cuál no se incurrirá en gastos para la gestión y elaboración del mismo.

BPMN (Business Process Modeling Notation)

BPMN es una notación gráfica estandarizada que permite el modelado de procesos de un negocio en particular. Actualmente, la última versión aprobada es la 1.2, pero se está a la espera de una versión futura que sería la versión 2.0, que aún se encuentra en beta.

El objetivo principal del BPMN es el de proveer una notación estándar que permita el modelamiento del negocio, de tal forma que los procesos sean entendibles, de una forma fácil y sencilla, por los involucrados e interesados del negocio. El modelado en BPMN se realiza mediante diagramas simples y con un conjunto pequeño de elementos gráficos. En la versión actual, se cuenta con cuatro categorías básicas de elementos, que son los siguientes:

Objetos de flujo: Definen el comportamiento de los procesos. Está compuesto por eventos, actividades y gateways (Rombos de control de flujo).

Eventos: Ocurren durante el desarrollo de un proceso de negocio y afectan el flujo del proceso. Se encuentran clasificados en 3 tipos:

Imagen 02: Eventos BPMN

Fuente: Business Process Modeling Notation

Actividades*:* Representan actividades, las cuales pueden ser simples o compuestas, que se realiza dentro de un proceso de negocio. Los dos tipos de actividades que existentes:

Imagen 03: Actividades BPMN

Fuente: Business Process Modeling Notation

Gateways*:* Son elementos que sirven para el control del flujo del proceso de negocio. Existen 5 tipos de compuertas:

1. Compuerta exclusiva
2. Compuerta basada en eventos
3. Compuerta paralela
4. Compuerta inclusiva
5. Compuerta compleja

Imagen 04: Gateway BPMN

Fuente: Business Process Modeling Notation

Objetos de conexión: Utilizados para unir dos objetos del flujo del proceso de negocio. Existen 3 tipos de objetos de conexión:

1. Líneas de Secuencia
2. Asociaciones

3. Líneas de Mensaje

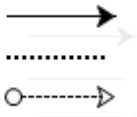


Imagen 05: Conectores BPMN

Fuente: Business Process Modeling Notation

Canales*:* Se utiliza para organizar las actividades del flujo en diferentes categorías visuales que representan áreas funcionales, roles o responsabilidades. Existen 2 tipos:

1. Pools
2. Lanes

Imagen 06: Canales BPMN

Fuente: Business Process Modeling Notation

Artefactos: Proveen información adicional sobre el proceso de negocio, existen 3 tipos:

1. Objetos de Datos o Grupos
2. Anotaciones
3. Objetos de Datos

Imagen 07: Artefactos BPMN

Fuente: Business Process Modeling Notation

TIA (Telecommunications Industry Association)

La Asociación Industrial de Telecomunicaciones público en abril del año 2005 el estándar TIA-942 para lograr unificar ideas respecto al diseño de áreas de tecnología.

Este estándar se basa específicamente en uno de los principales puntos del presente proyecto, la seguridad física en un centro de datos. El estándar se basa en recomendaciones del Uptime Institute, el cual establece cuatro niveles o también llamados tiers, los cuales determinan el nivel de disponibilidad del centro.

Por otro lado, divide la infraestructura soporte de un centro de datos en cuatro subsistemas:

1. Telecomunicaciones
2. Arquitectura
3. Sistema Eléctrico
4. Sistema Mecánico[9]

Este estándar muestra a detalle como cada uno de estos subsistemas debe cumplir con ciertas condiciones para poder calificarlas. El tipo de evaluación es asignado en base al menor nivel encontrado, por ejemplo: si 100 condiciones logran ser Tier 3 y una de ellas es Tier 2 entonces se concluye que ese subsistema aún está en Tier 2. En otras palabras, la condición con el nivel más bajo es el que determina en que Tier se encuentra el subsistema evaluado en el centro de datos.

ITIL (Information Technology Infrastructure Library)

Según la OGC (Office Government Commerce), ITIL se define como, la Biblioteca de Infraestructura de Tecnologías de Información es un conjunto de prácticas enfocadas en la gestión de servicios de tecnologías de la información, dando descripciones detalladas sobre los procedimientos de gestión para ayudar a las organizaciones a lograr eficiencia y calidad en sus operaciones de TI.[10]

Algunos de estos procedimientos de gestión son los siguientes:

---

[9] Cfr. TIA-942 2005
[10] Cfr. ITIL-OFFICIALSIT-E 2007

1. Gestión de Incidentes
2. Gestión de Problemas
3. Gestión de Configuraciones
4. Gestión de Cambios
5. Gestión de Versiones
6. Gestión de Niveles de Servicio
7. Gestión Financiera
8. Gestión de la Capacidad
9. Gestión de la Continuidad del Servicio
10. Gestión de la Disponibilidad
11. Gestión de la Seguridad[11]

Dentro de ese conjunto de procedimientos se encuentra la Gestión de Seguridad de la cual se dice lo siguiente:

"La Gestión de la Seguridad debe conocer en profundidad el negocio y los servicios que presta la organización TI para establecer protocolos de seguridad que aseguren que la información esté accesible cuando se necesita por aquellos que tengan autorización para utilizarla." (Osiatis 2009)

El conjunto de prácticas de la gestión de seguridad permitirá establecer las bases del proyecto y ver cómo se puede adaptar a las necesidades y características de la organización y sus servicios, en este caso el del centro de datos de la carrera.

Por otro lado, se debe observar, analizar y tener en cuenta los principales beneficios y dificultades que se tienen al implementar la Gestión de la Seguridad en la organización.

Con el paso del tiempo ITIL ha cobrado una mayor importancia en las empresas, hoy en día se maneja el concepto de obtener el máximo beneficio que brindan las mejores

[11] Cfr. Osiatis 2009

prácticas recomendadas por ITIL para esto se necesita involucrar a los clientes de los servicios de TI. Esta forma de interpretar ITIL hace que las tecnologías de información se conviertan en una experiencia colaborativa entre el cliente y los proveedores del servicio (internos y externos), pero sin descuidar que quienes definen los requerimientos son los clientes. Sin embargo, ITIL no es únicamente para los clientes y los proveedores de servicios, puesto que incluye a otros grupos tales como el directorio, la alta dirección, los auditores y los reguladores.

Toda gestión necesita ser definida y controlada, la Gestión de la Seguridad Física y Lógica no escapa a esta realidad por este motivo cuando se planteó el proyecto se alineó ITIL y COBIT. COBIT proporciona las herramientas para dirigir y supervisar todas las actividades relacionadas con las TI.

El objetivo de la tabla que se muestra a continuación es demostrar como los procesos y operaciones de TI son importantes para todo nivel y por ende el proyecto necesita mantener informado a todos los Stakeholders algunos de estos forman parte de las divisiones jerárquicas que se muestran en la tabla.

Aspectos de alta gestión basados en COBIT	Alta Dirección	Gerencias Funcionales	Gerencia de TI	Auditoría / Cumplimiento
Planificar y Organizar				
¿TI está alineada con las estrategias del negocio?	Ξ	Ξ	Ξ	
¿La empresa está logrando el uso óptimo de los recursos internos y externos?	Ξ	Ξ	Ξ	Ξ
¿Todo el personal de la empresa entiende los objetivos de TI?	Ξ	Ξ	Ξ	Ξ
¿Se ha entendido el impacto de TI en los riesgos de la empresa?	Ξ			
¿Se ha establecido la responsabilidad de la gestión de los riesgos de TI? ¿Se han entendido y se están gestionando los riesgos de TI?		Ξ	Ξ	Ξ
¿La calidad de los sistemas es apropiada para las necesidades de la empresa?		Ξ	Ξ	
Adquirir e Implementar				
¿Es probable que los nuevos proyectos entreguen soluciones que satisfagan las necesidades del negocio?		Ξ	Ξ	

¿Es probable que los nuevos proyectos se entreguen a tiempo y dentro del presupuesto?		Ξ	Ξ	Ξ
¿Los nuevos sistemas trabajarán correctamente cuando se implementen?		Ξ	Ξ	Ξ
¿Los cambios serán realizados sin trastornar la actual operación del negocio?		Ξ	Ξ	
Entrega y Soporte				
¿Los servicios de TI se entregan en línea con los requerimientos y las prioridades del negocio?		Ξ	Ξ	
¿Están optimizados los costos de TI?		Ξ	Ξ	Ξ
¿El personal está capacitado para utilizar los sistemas de TI en forma productiva y segura?		Ξ	Ξ	
¿Los sistemas de TI tienen adecuada confidencialidad, integridad y disponibilidad?		Ξ	Ξ	Ξ
Monitorear y Evaluar				
¿Se puede medir el desempeño de TI y detectar los problemas antes que sea demasiado tarde?	Ξ	Ξ	Ξ	
¿Los controles internos están operando eficazmente?	Ξ			Ξ
¿La empresa está cumpliendo las disposiciones regulatorias?	Ξ	Ξ	Ξ	Ξ

¿El gobierno de TI es eficaz?	Ξ	Ξ	Ξ	Ξ

Tabla 1: Aspectos de Gestión basados en COBIT

Fuente: Elaboración Propia

Pero ¿porque usar ITIL y no las mejores prácticas de cada empresa?, Tal como lo menciona ISACA la implementación de ITIL conlleva a una serie de beneficios. Estos beneficios son

1. La adopción eficaz de las mejores prácticas ayudará a obtener valor de las inversiones de TI y los servicios de TI:
2. Mejorando la calidad, la respuesta y la fiabilidad de las soluciones y los servicios de TI.
3. Mejorando la viabilidad, previsibilidad y repetitividad de resultados de negocio exitosos.
4. Ganando la confianza y el creciente involucramiento de usuarios y patrocinadores del negocio.
5. Reduciendo riesgos, incidentes y fallas en los proyectos.
6. Mejorando la habilidad del negocio para gestionar y supervisar la realización de beneficios de TI.

La empresa también se beneficia de la mejora de eficiencias y reducción de costos:

1. Evitando la reinvención de prácticas probadas.
2. Reduciendo la dependencia de expertos.
3. Incrementando el potencial del staff, menos experto pero correctamente entrenado.
4. Superando silos verticales y comportamientos no deseados.
5. Incrementando la estandarización que conduzca a la reducción de costos.
6. Haciéndolo más fácil para aprovechar la ayuda externa a través del uso de procesos estandarizados.

En un clima de creciente regulación y preocupación sobre los riesgos relacionados a TI, las mejores prácticas ayudarán a minimizar los aspectos de cumplimiento y la preocupación de los auditores:

1. Logrando el cumplimiento y la aplicación de controles internos de 'práctica normal de negocios'.

2. Demostrando adherirse a buenas prácticas aceptadas y probadas de la industria.

3. Mejorando la confianza y la seguridad de la dirección y los socios.

4. Generando respecto de los reguladores y otros supervisores externos.

La gestión de servicios de TI se refiere a la planificación, aprovisionamiento, diseño, implementación operación, apoyo y mejora de los servicios de TI que sean apropiados a las necesidades del negocio. ITIL proporciona un marco de trabajo de mejores prácticas integral, consistente y coherente para la gestión de servicios de TI y los procesos relacionados, la promoción de un enfoque de alta calidad para el logro de la eficacia y eficiencia del negocio en la gestión de servicios de TI.

Uno de los objetivos de ITIL es respaldar mas no fijar los procesos de negocio de una organización. En este contexto, la OGC no aprueba el término "Cumplimiento con ITIL". El papel del marco de trabajo de ITIL es describir los enfoques, las funciones, los roles y procesos en los que las organizaciones pueden basar sus propias prácticas. El rol de ITIL es brindar orientación en el nivel organizacional más bajo que pueda aplicarse.

Debajo de ese nivel, para implementar ITIL en una organización se requieren los conocimientos específicos de sus procesos de negocio para ajustar ITIL a fin de lograr una eficacia óptima.

ISO 27001 - NTP 17799 - ISO/IEC 17799:2005

La norma ISO 27001 tiene como finalidad proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de información. Esta norma está muy alineada con otras normas como por

ejemplo la norma ISO 9000:2000 y es aplicable a todos los tipos de organizaciones asegurando y proporcionando los controles de seguridad que protejan los activos de información.[12]

La Norma Técnica Peruana (NTP) fue elaborada por el comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos (EDI), durante los meses de junio y julio del año 2006. Esta norma es una adopción de la Norma ISO/IEC 17799:2005.[13]

La norma ISO/IEC 17799:2005 proporciona lineamientos de implementación que se deben utilizar cuando se habla de diseño de controles de seguridad.[14] Es decir, la NTP 17799 es una adaptación de la norma ISO/IEC mencionada pero enfocada en la realidad y el alcance de nuestro país. Es por este motivo que el proyecto seguiría los controles y guías de implementación presentados por esta norma NTP 17799:2005.

La relación que guardan ambos estándares con el proyecto desarrollado es directa, debido a que éstos se basan en la Tecnología de la información así también como en un código de buenas prácticas para la gestión de la seguridad de la información, la cual abarca los temas de Seguridad Física y Seguridad Lógica, temas principales del presente proyecto profesional.

[12] Cfr. QUALITAS 2011
[13] Cfr. INDECOPI 2007
[14] Cfr. QUALITAS 2011

CAPÍTULO 3: SEGURIDAD FÍSICA Y LÓGICA

En el presente capítulo se detallará el diseño de la metodología que servirá de base para la creación del estándar. Además, se presentará el método de interpretación creado para los resultados de la evaluación y finalmente se presentará cuáles son las políticas sugeridas.

Metodología de Trabajo

El proyecto Gestión de la Seguridad Física y Lógica para un centro de datos ha seguido las indicaciones de la Guía del PMBOK, es decir se ha estructurado el proyecto en fases. Las cuatro fases que se determinaron son:

1. Planificación (1)
2. Seguridad a Nivel Físico (2)
3. Seguridad a Nivel Lógico (3)
4. Assessment y Cierre del Proyecto (4)

La primera fase consiste en la planificación del proyecto per se (el alcance del proyecto, los riesgos, la planificación del cronograma, los entregables, los riesgos y los indicadores de éxito del mismo). En esta fase también se llevó a cabo la evaluación de los estándares internacionales, el análisis de fuentes y se establecieron los requisitos mínimos que se deben alcanzar al implementar los cambios en seguridad sugeridos por el proyecto.

Durante la primera fase se ha considerado que el estudio a realizar debe tener como base dos criterios, el primero es determinar cuáles son los requerimientos mínimos de seguridad con los que debe contar el centro de datos de la carrera y el segundo es la complejidad de los controles e implementación requerida por los principales estándares que existen, los cuales han apoyado en diferentes campos de la investigación.

La segunda fase se caracterizó por el levantamiento de información referente a la seguridad física a través de reuniones con los encargados del centro de datos, reuniones

con las personas de Servicios Generales para después de estas reuniones identificar los riesgos, generar el checklist de seguridad física, realizar la evaluación del centro de datos, generar los reportes de incidencias, realizar interpretación de resultados, detallar las recomendaciones a implementar y los procesos que deben ser adoptados a partir de este ciclo en el centro de datos. Todos los procesos creados para soportar la seguridad física han sido creados a partir de diversas fuentes y cada uno de ellos tiene métricas para el control de mismo.

La evaluación a nivel físico del centro de datos se basa principalmente en la TIA 942 y las recomendaciones brindadas por Purificación Aguilera en su libro seguridad informática. Sin embargo, la TIA 942 es un estándar que tiene un alcance superior al proyecto por lo cual se tuvo que adaptar considerando los requerimientos mínimos para el centro de datos. Al mismo tiempo, la escala de resultados tuvo que ser modificada, incorporando dos nuevas categorías debido a que el estándar tiende a ser de resultado superior es decir asume que se debe tener un mínimo de requisitos por lo cual no existían las categorías: "No Existe" y "No Aplica".

Al tener los resultados de la evaluación y los procesos definidos, se creó la política de seguridad física considerando que ésta debe soportar todas las actividades, procesos y los requerimientos mínimos detallados en la primera fase del proyecto.

Durante la tercera fase del proyecto se ha realizado el levantamiento de información con el personal encargado del centro de datos, se creó el checklist para la evaluación a nivel lógico, esta evaluación tiene principalmente tres fuentes, la norma técnica peruana 17799, el Orange Book libro desarrollado por el Ministerio de Defensa de Estados Unidos y las recomendaciones de Purificación Aguilera en su libro Seguridad Informática.

Al realizar la evaluación e interpretar los resultados de la misma, se logró identificar los riesgos presentes y por ende los puntos de mejora en seguridad lógica. A partir de las carencias detectadas se definieron los procesos para que soporten la seguridad lógica, los mismo que han sido creados a partir de diversas fuentes y cada uno de ellos tiene métricas para el control de mismo.

Con los resultados de la evaluación y los procesos definidos, se creó la política de seguridad lógica considerando todas las actividades, procesos y los requerimientos mínimos detallados en la primera fase del proyecto.

El proyecto se basa en gestionar la seguridad física y lógica del centro de datos de la carrera de Ingeniería de Sistemas de Información, por lo que se dividió el proyecto en dos grandes partes las cuales abarcarían un aspecto de la seguridad cada una.

La primera parte se centra en la Seguridad Física del centro de datos, la cual, se inició con la evaluación del estado actual de centro de datos en donde se dispuso del estándar TIA-942, el cual es un estándar especializado en lo que refiere a ubicación, cableado, monitoreo, sistemas de ventilación, entre otros. Se elaboró un checklist basado en dicho estándar el cual permite tener una visión global de estado actual del centro de datos. A su vez que, a fin de cumplir uno de los objetivos del proyecto el cual es el de elaborar un estándar para centro de datos, se adaptó el checklist específicamente para el centro de datos de la carrera de Ingeniería de Sistemas de Información ya que a lo largo de la evaluación el equipo de proyecto determinó que el alcance de la TIA-942 es mucho mayor al necesario en el centro de datos. Una vez que se hizo evidente el estado actual del centro de datos se procedió a elaborar una política de seguridad física basando el análisis en la Norma Técnica Peruana - NTP17799 la cual a su vez se basa en el ISO/IEC 17799 de seguridad de la información. La política está divida en 3 diferentes conceptos que apoyan a tres objetivos especificados dentro de esta, a su vez que los conceptos están apoyados por directrices. Finalmente, se han elaborado los procesos para apoyar estas directrices de manera que se asegure que la Seguridad Física del centro de datos está completamente resguardad.

La segunda parte del proyecto tiene como objetivo asegurar la Seguridad Lógica, para llevar a cabo esta gestión fue necesaria la elaboración del checklist, el mismo que tiene su origen en la Norma Técnica Peruana NTP17799, el Orange Book, el libro de Seguridad Informática de Purificación Aguilera, los cuales brindan la base para la evaluación de la seguridad lógica del centro de datos.

Debido a las restricciones y el alcance que maneja el proyecto no se brindarán recomendaciones y/o sugerencias a implementar en el diseño lógico o físico del diagrama de redes. Sin embargo, cabe resaltar que la administración de este punto se encuentra bajo responsabilidad del área de servicios generales de la universidad.

Si se desea implementar un esquema de seguridad de redes se debería tener presente los siguientes puntos brindados por la TIA 942:

Revisar y adaptar la información del Anexo A.

Este capítulo se encarga de brindar las mejores prácticas para el diseño del cableado a utilizar en un centro de datos, brindando especificaciones de distancia, creación de circuitos, conexiones con las consolas, conexión cruzada, entre otros.

Revisar y adaptar la información del Anexo B.

Este capítulo se encarga de brindar las mejores prácticas para el diseño de la infraestructura de las comunicaciones, brindando especificaciones de identificación de cableado y tipos de conexión.

Revisar y adaptar la información del Anexo C.

Este capítulo se encarga de brindar las mejores prácticas para el diseño los controles de acceso de información, brindando especificaciones de cableado UTP, circuitos cerrados, equipos de acceso remoto, equipos de acceso a proveedores de información.

Adicionalmente, se debe tener presente los siguientes controles para la seguridad de redes:

Configuración de Firewall.

- Internal Firewall
- Perimeter Firewall

Numero de puertos de entrada.

- Zona desmilitarizada.
- Configuración de la VLAN.

Se sugiere comprar aplicativos como TIVOLI para llevar un adecuado control del uso y de la estabilidad de la red.

Mapa de Procesos

-

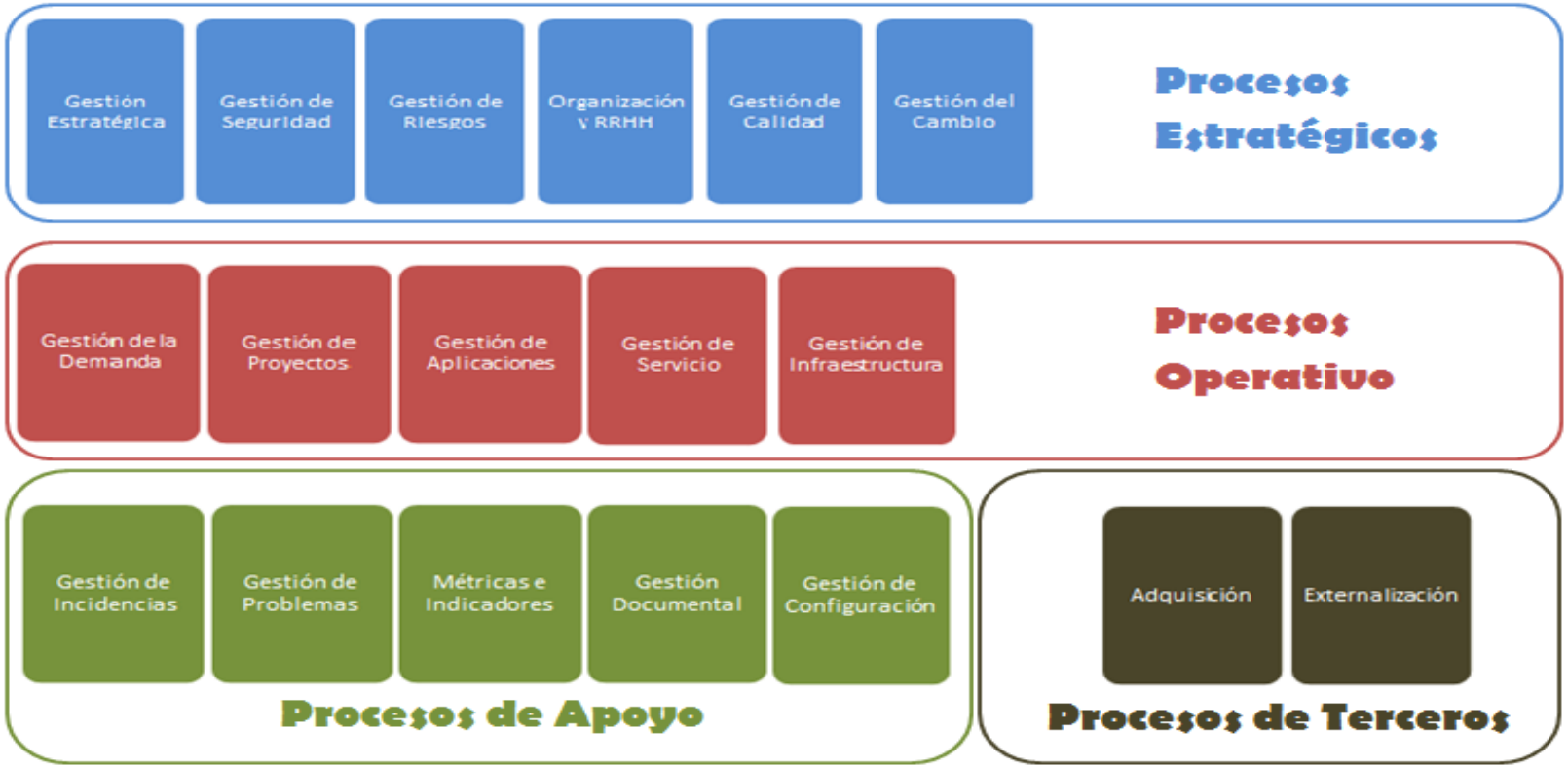


Imagen 08: Mapa de Procesos

Fuente: Elaboración Propia

Diagrama de Objetivos

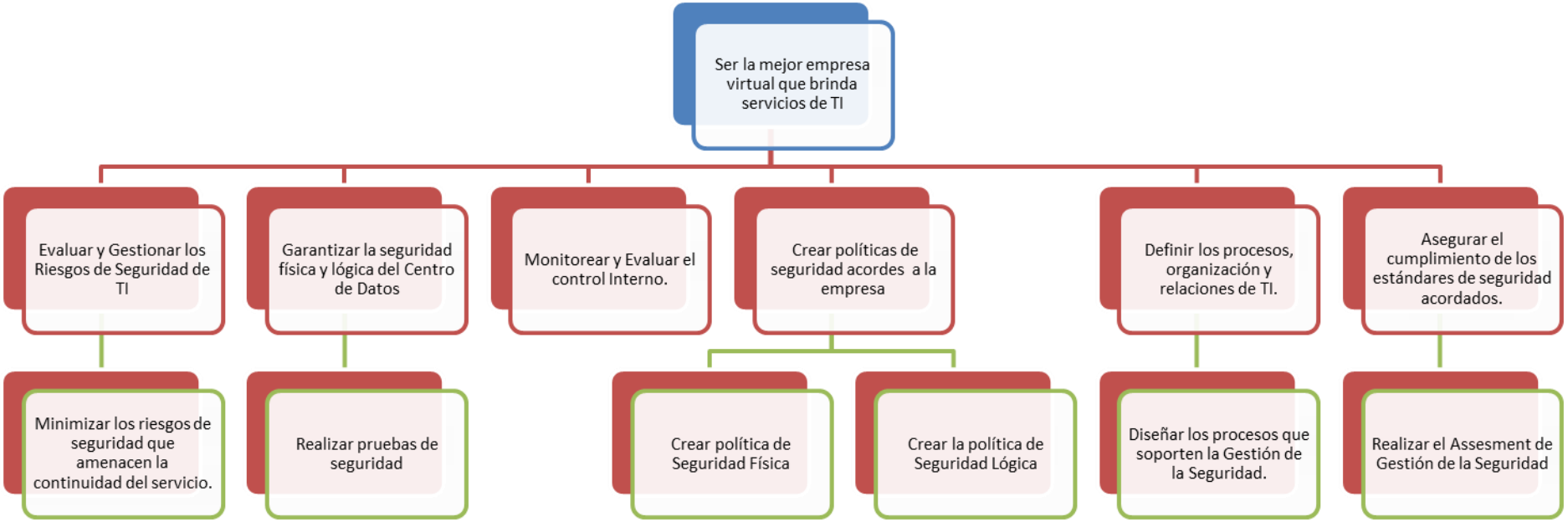


Imagen 09: Diagrama de Objetivos

Fuente: Elaboración Propia

Seguridad a nivel físico

Diseño de la evaluación y del Checklist

Para poder definir de manera real y coherente un estándar de seguridad (físico y lógico) para el centro de datos de la carrera, se necesita tener una visión global del estado actual. Esta visión global debe dar a conocer los riesgos, las vulnerabilidades y las posibles amenazas que se encuentran presentes dentro de las instalaciones para así poder determinar qué acciones se deben llevar a cabo para subsanarlas o reducir su impacto.

Para obtener esta visión global se llevó a cabo una evaluación, la misma que fue diseñada con las sugerencias del Estándar de Telecomunicaciones e Infraestructura para Centro de datos (TIA 942) y la Norma Técnica Peruana 17799 (NTP 17799). A partir de estas sugerencias se creó un checklist de evaluaciones, el cual se encargar de cubrir los cuatro principales subsistemas conocidos dentro de un centro de datos. Los cuatro subsistemas que existen son: Subsistema Arquitectónico, Subsistema Eléctrico, Subsistema Telecomunicaciones, Subsistema Mecánico.

El subsistema arquitectónico incluye las consideraciones sobre aparcamiento, baños y áreas de descanso, CCTV, centro de operaciones, componentes del edificio, construcción del edificio, control monitoreo y accesos de seguridad, corredores de salida, estructura, generador de respaldo y áreas de almacenamiento de combustible, material para techos, monitoreo CCTV, muros, ventanas y puertas resistentes a balas, oficina de seguridad, oficinas administrativas, puertas y ventanas, resistividad al fuego, seguridad, ubicación del centro de datos y la ubicación de los UPS y la sala de baterías.

El subsistema eléctrico incluye las consideraciones sobre baterías de tipo inundado, conexión a tierra, configuración de las baterías, sistema eléctrico en general, mantenimiento de los equipos, monitoreo del sistema eléctrico, pruebas de cargas, requisitos en la sala de baterías, sistema de cajas del UPS (Diésel), sistema de generación standby, sistemas de emergencia de corte de energía (EPO) y UPS.

El subsistema mecánico incluye consideraciones sobre la eliminación de calor (agua), eliminación de calor (aire), selección de sitio, sistema de agua fría, sistema de combustible de aceite, sistema de control HVAC, sistema de refrigeración por agua, sistema de refrigeración por aire, sistema de tuberías, supresión de fuego.

El subsistema de telecomunicaciones incluye consideraciones sobre la ubicación del sitio, cableado, router, switch, paneles eléctricos y tomacorrientes.

Considerando cada uno de los puntos descritos líneas arriba se creó el checklist que se muestra a continuación: Considerar que el checklist pueda estar en un anexo.

Subsistema de Arquitectura

General Selección de Sitio		TIER 1	TIER 2	TIER 3	TIER 4
1	Enrutamiento de agua o de drenaje sin tuberías en el equipo del centro de datos en el centro de datos y espacio.	Permitido pero no recomendado	Permitido pero no recomendado	No permitido	No permitido
2	La presión positiva en el aula de informática y espacios asociados en relación con el exterior y que no sean del centro de datos	No requiere	Si	Si	Si
3	Los desagües de condensado de agua se encuentran en el piso en sala de ordenadores, de agua del humidificador de color, y por aspersión de descarga de agua.	Si	Si	Si	Si
4	Sistemas mecánicos en generadores StandBy	No requiere	Si	Si	Si

Tabla 2: Subsistema de Arquitectura, General

Fuente: TIA-942

Sistema de refrigeración por agua		TIER 1	TIER 2	TIER 3	TIER 4
1	Cubierta de terminales de unidades de aire acondicionado	No aire acondicionados redundantes	Una unidad AC redundante por área crítica	Cantidad de unidades AC suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de unidades AC suficiente para mantener un área crítica durante la perdida de electricidad de una fuente
2	Control de humedad para el Centro de Datos	Humidificación provista	Humidificación provista	Humidificación provista	Humidificación provista
3	Servicio eléctrico a los equipos mecánicos	Equipos AC con una única ruta de acceso	Equipos AC con una única ruta de acceso	Múltiples equipos AC con una única ruta de acceso	Múltiples equipos AC con una única ruta de acceso

Tabla 3: Subsistema de Arquitectura, Sistema de refrigeración

Fuente: TIA-942

	Eliminación del calor	TIER 1	TIER 2	TIER 3	TIER 4
1	Seco-enfriadores (si procede)	Seco enfriadores no redundantes	Un Seco enfriadores redundante por sistema	Cantidad de seco enfriadores suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de seco enfriadores suficiente para mantener un área crítica durante la perdida de electricidad de una fuente
2	Circuito cerrado de fluido Enfriadores (si procede)	Enfriadores de fluido no redundantes	Un Enfriador de fluido por sistema	Cantidad de enfriadores de fluidos suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de enfriadores de fluidos suficiente para mantener un área crítica durante la perdida de electricidad de una fuente
3	Bombas de circulación	Bombas de circulación no redundantes	Una Bomba de circulación redundante por sistema	Cantidad de bombas de circulación suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de bombas de circulación suficiente para mantener un área crítica durante la perdida de electricidad de una fuente

4	Sistema de tuberías	Sistema de condensación de agua con una única ruta de acceso	Sistema de condensación de agua con una única ruta de acceso	Sistema de condensación de agua con ruta de acceso dual.	Sistema de condensación de agua con ruta de acceso dual.

Tabla 4: Subsistema de Arquitectura, Eliminación del calor

Fuente: TIA-942

	Sistema de Agua Fría	TIER 1	TIER 2	TIER 3	TIER 4
1	Cubierta de terminales unidades de aire acondicionado	Aires acondicionados no redundantes	Un aire acondicionado redundante por sistema	Cantidad de aires acondicionados suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de aires acondicionados suficiente para mantener un área crítica durante la perdida de electricidad de una fuente
2	Control de humedad para el Centro de Datos	Humidificación provista	Humidificación provista	Humidificación provista	Humidificación provista
3	Servicio eléctrico a los equipos mecánicos	Equipos AC con una única ruta de acceso	Equipos AC con una única ruta de acceso	Múltiples equipos AC con una única ruta de acceso	Múltiples equipos AC con una única ruta de acceso

Tabla 5: Subsistema de Arquitectura, Sistema de Agua Fría

Fuente: TIA-942

Eliminación del calor		TIER 1	TIER 2	TIER 3	TIER 4
1	Sistema de tuberías de agua fría	Sistema de tuberías de agua fría condensación de agua con una única ruta de acceso	Sistema de tuberías de agua fría condensación de agua con una única ruta de acceso	Sistema de tuberías de agua fría condensación de agua con rutas de acceso dual	Sistema de tuberías de agua fría condensación de agua con rutas de acceso dual
2	Bombas de circulación de agua fría	Bombas de circulación de agua fría no redundantes	Una Bomba de circulación de agua fría redundante por sistema	Cantidad de bombas de circulación de agua fría suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de bombas de circulación de agua fría suficiente para mantener un área crítica durante la perdida de electricidad de una fuente
3	Refrigeradores de refrigeración por aire	Refrigeradores de refrigeración por aire no redundantes	Un refrigerador de refrigeración por aire redundante por sistema	Cantidad de refrigeradores de refrigeración por aire suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de refrigeradores de refrigeración por aire suficiente para mantener un área crítica durante la perdida de electricidad de una fuente

4	Enfriadores refrigerados por agua	Enfriadores refrigerados por agua no redundantes	Un enfriador refrigerados por agua redundante por sistema	Cantidad de enfriadores refrigerados por agua suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de enfriadores refrigerados por agua suficiente para mantener un área crítica durante la perdida de electricidad de una fuente
5	Torres de enfriamiento	Torres de enfriamiento no redundantes	Una torre de enfriamiento redundante por sistema	Cantidad de Torres de enfriamiento suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de Torres de enfriamiento suficiente para mantener un área crítica durante la perdida de electricidad de una fuente
6	Condensadores de bombas de agua	Condensadores de bombas de agua no redundantes	Un condensador de bombas de agua redundante por sistema	Cantidad de condensadores de bombas de agua suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de condensadores de bombas de agua suficiente para mantener un área crítica durante la perdida de electricidad de una fuente

7	Sistema de tuberías de condensadores de agua	Sistema de condensación de agua con una única ruta de acceso	Sistema de condensación de agua con una única ruta de acceso	Sistema de condensación de agua con ruta de acceso dual.	Sistema de condensación de agua con ruta de acceso dual.

Tabla 6: Subsistema de Arquitectura, Eliminación del calor

Fuente: TIA-942

Sistema de refrigeración por aire		TIER 1	TIER 2	TIER 3	TIER 4
1	Cubierta de terminales unidades de aire acondicionado y al aire libre Condensadores	No aire acondicionados redundantes	Una unidad AC redundante por área crítica	Cantidad de unidades AC suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de unidades AC suficiente para mantener un área crítica durante la perdida de electricidad de una fuente
2	Servicio eléctrico a los equipos mecánicos	Equipos AC con una única ruta de acceso	Equipos AC con una única ruta de acceso	Múltiples equipos AC con una única ruta de acceso	Múltiples equipos AC con una única ruta de acceso
3	Control de humedad para el Centro de Datos	Humidificación provista	Humidificación provista	Humidificación provista	Humidificación provista

Tabla 7: Subsistema de Arquitectura, Sistema de Refrigeración por Aire

Fuente: TIA-942

	Sistema de Control HVAC	TIER 1	TIER 2	TIER 3	TIER 4
1	Sistema de Control HVAC	Falla en el sistema de control interrumpirá el enfriamiento de las áreas críticas	Falla en el sistema de control no interrumpirá el enfriamiento de las áreas críticas	Falla en el sistema de control no interrumpirá el enfriamiento de las áreas críticas	Falla en el sistema de control no interrumpirá el enfriamiento de las áreas críticas
2	Fuente de Poder para el Sistema de Control HVAC	Electricidad para el sistema de control HVAC con una única ruta de acceso	Electricidad de un UPS a los equipos AC redundantes	Electricidad de un UPS a los equipos AC redundantes	Electricidad de un UPS a los equipos AC redundantes

Tabla 8: Subsistema de Arquitectura, Sistema de Control HVAC

Fuente: TIA-942

	Sistema de Tuberías (para la eliminación del calor)	TIER 1	TIER 2	TIER 3	TIER 4
1	Fuentes duales para arreglar el agua	Fuente de agua única, sin respaldo en el lugar de almacenamiento.	Fuente de agua dual, o una fuente + respaldo en el lugar de almacenamiento.	Fuente de agua dual, o una fuente + respaldo en el lugar de almacenamiento.	Fuente de agua dual, o una fuente + respaldo en el lugar de almacenamiento.
2	Puntos de conexión para el sistema de condensación del agua	Un único punto de conexión	Un único punto de conexión	Dos punto de conexión	Dos punto de conexión

Tabla 9: Subsistema de Arquitectura, Sistema de Tuberías

Fuente: TIA-942

Sistema de combustible de aceite		TIER 1	TIER 2	TIER 3	TIER 4
1	Tanques de almacenamiento	Tanque de almacenamiento	Múltiples tanques de almacenamiento	Múltiples tanques de almacenamiento	Múltiples tanques de almacenamiento
2	Las bombas del tanque de almacenamiento y tuberías	Una Bomba y/o un tubo de provisiones	Múltiples Bombas, múltiples tubos de provisiones	Múltiples Bombas, múltiples tubos de provisiones	Múltiples Bombas, múltiples tubos de provisiones

Tabla 10: Subsistema de Arquitectura, Sistema de Combustible de Aceite

Fuente: TIA-942

Supresión de fuego		TIER 1	TIER 2	TIER 3	TIER 4
1	Sistema de detección de fuego	No	Si	Si	Si
2	Sistema de rociadores contra incendios	Cuando sea requerido	Pre-Acción (cuando requerido)	Pre-Acción (cuando requerido)	Pre-Acción (cuando requerido)
3	Sistema de supresión gaseosa	No	No	Agentes limpios listados en la NFPA 2001	Agentes limpios listados en la NFPA 2001
4	Sistema de aviso temprano de detección de humo	No	Si	Si	Si
5	Sistemas de detección de fugas de agua	No	Si	Si	Si

Tabla 11: Subsistema de Arquitectura, Supresión de Fuego

Fuente: TIA-942

Subsistema Eléctrico

General		TIER 1	TIER 2	TIER 3	TIER 4
1	Número de rutas de llegada/entrega.	1	1	1 activo y 1 pasivo	2 activos
2	Entrada de utilidad.	Alimentación única	Alimentación única	Doble alimentación (600 voltios o más)	Doble alimentación (600 voltios o más) desde diferentes subestaciones de utilidad
3	El sistema permite el mantenimiento concurrido.	No	No	Si	Si
4	Equipo de cables de alimentación de las computadoras y equipos de telecomunicaciones.	Cable de alimentación única con 100% de capacidad	Cable dual de alimentación con 100% de capacidad en c/cable	Cable dual de alimentación con 100% de capacidad en c/cable	Cable dual de alimentación con 100% de capacidad en c/cable
5	Todos los equipos del sistema eléctrico deben estar etiquetados con la certificación	Si	Si	Si	Si

	de una prueba de laboratorio de terceros.				
6	Puntos únicos de fallo	Uno o más puntos únicos de fallo para el equipo de servicio eléctrico o sistemas mecánicos	Uno o más puntos únicos de fallo para el equipo de servicio eléctrico o sistemas mecánicos	Ningún punto único de fallo para el equipo de servicio eléctrico o sistemas mecánicos	Ningún punto único de fallo para el equipo de servicio eléctrico o sistemas mecánicos
7	Sistema de transferencia de carga crítica	Interruptor de transferencia automática (ATS) con la función de mantenimiento de puente para servir al interruptor como interrupción al poder; cambio automático desde la utilidad hasta el generador cuando un corte de poder ocurra.	Interruptor de transferencia automática (ATS) con la función de mantenimiento de puente para servir al interruptor como interrupción al poder; cambio automático desde la utilidad hasta el generador cuando un corte de poder ocurra.	Interruptor de transferencia automática (ATS) con la función de mantenimiento de puente para servir al interruptor como interrupción al poder; cambio automático desde la utilidad hasta el generador cuando un corte de poder ocurra.	Interruptor de transferencia automática (ATS) con la función de mantenimiento de puente para servir al interruptor como interrupción al poder; cambio automático desde la utilidad hasta el generador cuando un corte de poder ocurra.
8	Sitio de Celdas	Ninguna	Ninguna	Humidificación provista	Ninguna

9	Generadores del tamaño correcto de acuerdo a la capacidad del UPS instalado	Si	Si	Si	Si
10	Capacidad del combustible del generador (a carga plena)	8 horas (no requiere del generador si el UPS tiene 8 minutos de tiempo de respaldo)	24 horas	72 horas	96 horas

Tabla 12: Subsistema Eléctrico, General

Fuente: TIA-942

UPS		TIER 1	TIER 2	TIER 3	TIER 4
1	Redundancia del UPS	N	N+1	N+1	2N
2	Topología del UPS	Módulo único o módulos paralelos no redundantes	Módulos paralelos redundantes o módulos redundantes distribuidos	Módulos paralelos redundantes o módulos redundantes distribuidos o sistema redundante de bloqueo	Módulos paralelos redundantes o módulos redundantes distribuidos o sistema redundante de bloqueo
3	Acuerdo de mantenimiento de derivación en el UPS	Poder bypass obtenido de la misma utilidad de alimentación de los módulos del UPS	Poder bypass obtenido de la misma utilidad de alimentación de los módulos del UPS	Poder bypass obtenido de la misma utilidad de alimentación de los módulos del UPS	Poder bypass obtenido del sistema de reserva del UPS el cual es alimentado de un bus diferente a los que se usa en los sistemas de UPS
4	Nivel de voltaje - Distribución de Poder del UPS	Nivel de voltaje 120/208V hasta cargas de 1440kVA y 480V para cargas mayores a 1440kVA	Nivel de voltaje 120/208V hasta cargas de 1440kVA y 480V para cargas mayores a 1440kVA	Nivel de voltaje 120/208V hasta cargas de 1440kVA y 480V para cargas mayores a 1440kVA	Nivel de voltaje 120/208V hasta cargas de 1440kVA y 480V para cargas mayores a 1440kVA

5	Tableros de paneles - Distribución del Poder del UPS	Tableros de paneles incorporados con estándar de interruptores térmicos de disparo magnético	Tableros de paneles incorporados con estándar de interruptores térmicos de disparo magnético	Tableros de paneles incorporados con estándar de interruptores térmicos de disparo magnético	Tableros de paneles incorporados con estándar de interruptores térmicos de disparo magnético
6	Todas las computadoras y equipos de telecomunicaciones son alimentados con PDU's	No	No	Si	Si
7	Transformadores K-Factor instalados en PDU's	Sí, pero no requeridos si se usan transformadores de anulación armonioso	Sí, pero no requeridos si se usan transformadores de anulación armonioso	Sí, pero no requeridos si se usan transformadores de anulación armonioso	Sí, pero no requeridos si se usan transformadores de anulación armonioso
8	Bus de sincronización de carga (LBS)	No	No	Si	Si
9	Componentes redundantes (UPS)	Diseño de UPS estático	Diseño de UPS estático o rotatorio. Convertidores rotatorios M-G Set.	Diseño de UPS estático o rotatorio. Convertidores rotatorios M-G Set.	Diseño de UPS estático o rotatorio. Convertidores rotatorios M-G Set.

10	El UPS se encuentra separado en un panel de distribución separado de los equipos de telecomunicaciones y computadoras.	No	Si	Si	Si

Tabla 13: Subsistema Eléctrico, UPS

Fuente: TIA-942

Conexión a Tierra		TIER 1	TIER 2	TIER 3	TIER 4
1	Sistema de protección de iluminación	En base a los análisis de riesgo según la NFPA 780 y requerimientos de seguro.	En base a los análisis de riesgo según la NFPA 780 y requerimientos de seguro.	Si	Si
2	Motivos de entrada de servicio y los motivos del generador se ajusta plenamente a NEC	Si	si	Si	Si
3	Accesorios de iluminación (277v) neutral, aislados de la entrada de servicio derivados de la iluminación del transformador para el aislador de fallas de tierra	Si	Si	Si	Si
4	La infraestructura de la conexión a tierra del centro de datos está dentro de la sala de computadoras.	No requerido	No requerido	Si	Si

Tabla 14: Subsistema Eléctrico, Conexión a Tierra

Fuente: TIA-942

Sistema de Emergencia de Corte de Energía en la sala de computadoras (EPO)		TIER 1	TIER 2	TIER 3	TIER 4
1	Activado por el sistema de emergencia de corte de energía (EPO) en las salidas apagando solo al sistema de telecomunicaciones y computadoras.	Si	Si	Si	Si
2	El supresor de fuego automático se libera después del apagado del sistema de telecomunicaciones	Si	Si	Si	Si
3	Sistema de alarma de fuego de la segunda zona se activa con el apagado del sistema de emergencia de corte de energía (EPO) de forma manual	No	No	No	Si
4	El control Maestro desconecta baterías y libera un supresor desde una estación atendida 24/7	No	No	No	Si

Tabla 15: Subsistema Eléctrico, Sistema de Emergencia de Corte de Energía en la Sala de Computadoras

Fuente: TIA-942

Sistema de Emergencia de Corte de Energía en sala de Baterías (EPO)		TIER 1	TIER 2	TIER 3	TIER 4
1	Activado por los botones del sistema de emergencia de corte de energía (EPO) en las salidas con liberación de un supresor manual	Si	Si	Si	Si
2	Se libera el supresor de fuego para el sistema de zonas únicas después del apagado del sistema de emergencias de corte de energía	Si	Si	Si	Si
3	Activación del sistema de alarma de fuego en la segunda zona. Desconecta las baterías en la primera zona con la liberación del supresor en la segunda zona.	No	No	Si	Si
4	El control Maestro desconecta baterías y libera un supresor desde una estación atendida 24/7	No	No	Si	Si

Tabla 16: Subsistema Eléctrico, Sistema de Emergencias de Corte de Energía en Sala de Baterías

Fuente: TIA-942

	Sistema de Emergencia de Corte de Energía (EPO)	TIER 1	TIER 2	TIER 3	TIER 4
1	Apagado del poder de los recipientes del UPS en el área de la sala de computadoras.	Si	Si	Si	Si
2	Apagado de Corriente AC para Cracs y enfriadores	Si	Si	Si	Si
3	Cumplimiento del código local (eje. Sistemas separados para el UPS y HVAC)	Si	Si	Si	Si

Tabla 17: Subsistema Eléctrico, Sistema de Emergencia de Corte de Energía

Fuente: TIA-942

	Monitoreo del Sistema	TIER 1	TIER 2	TIER 3	TIER 4
1	Desplegado localmente en el UPS	Si	Si	Si	Si
2	Interface con el BMS	No	No	Si	Si
3	Control Remoto	No	No	No	Si
4	Mensajes de texto automáticos para el servicio de localización de ingenieros	No	No	No	Si
5	Mensajes de texto automáticos para el servicio de localización de ingenieros	No	No	No	Si

Tabla 18: Subsistema Eléctrico, Monitoreo del Sistema

Fuente: TIA-942

	Configuración de Batería	TIER 1	TIER 2	TIER 3	TIER 4
1	Cadena de baterías comunes para todos los módulos	Si	No	No	No
2	Una cadena de batería para c/módulo	No	Si	Si	Si
3	Tiempo de espera mínimo para la carga plena	5 min	10 min	15 min	15 min
4	Tipo de Batería	Válvula de plomo-ácido (VRLA) o de tipo inundado	Válvula de plomo-ácido (VRLA) o de tipo inundado	Válvula de plomo-ácido (VRLA) o de tipo inundado	Válvula de plomo-ácido (VRLA) o de tipo inundado

Tabla 19: Subsistema Eléctrico, Configuración de Batería

Fuente: TIA-942

	Batería de Tipo Inundado	TIER 1	TIER 2	TIER 3	TIER 4
1	Montaje	Racks o gabinetes	Racks o gabinetes	Racks abiertos	Racks abiertos
2	Placas de envoltura	No	Si	Si	Si
3	Contenedores de derrame de ácido instalados	Si	Si	Si	Si
4	Pruebas de batería a carga plena / Horarios de inspección	Cada 2 años	Cada 2 años	Cada 2 años	Cada 2 años o anual

Tabla 20: Subsistema Eléctrico, Batería de Tipo Inundado

Fuente: TIA-942

	Sala de Baterías	TIER 1	TIER 2	TIER 3	TIER 4
1	Separado de los cuartos de los equipos UPS y celdas	No	Si	Si	Si
2	Las cadenas individuales de baterías están aisladas de uno con otro	No	Si	Si	Si
3	Vista a través de vidrio inastillable en la puerta de la sala de baterías.	No	No	No	Si
4	Las desconexiones de las baterías se localizan fuera de la sala de baterías	Si	Si	Si	Si
5	Sistema de monitoreo de baterías	Auto monitoreo del UPS	Auto monitoreo del UPS	Auto monitoreo del UPS	Sistema automatizado centralizado para la revisión de temperatura, voltaje e impedancia para cada celda

Tabla 21: Subsistema Eléctrico, Sala de Baterías

Fuente: TIA-942

Sistema de Cajas del UPS Rotador (con generadores Diesel)		TIER 1	TIER 2	TIER 3	TIER 4
1	Unidades encerradas separadas por las paredes nominales de fuego	No	No	Si	Si
2	Tanques de combustibles en el exterior	No	No	Si	Si
3	Tanques de combustibles en la misma sala que las unidades	Si	Si	No	No

Tabla 22: Subsistema Eléctrico, Sistema de Cajas del UPS Rotador

Fuente: TIA-942

	Sistema de generación Standby	TIER 1	TIER 2	TIER 3	TIER 4
1	Generador de tamaño	Solo para el tamaño de las computadoras y el sistema de telecomunicaciones, eléctrico y mecánico	Solo para el tamaño de las computadoras y el sistema de telecomunicaciones, eléctrico y mecánico	Solo para el tamaño de las computadoras y el sistema de telecomunicaciones, eléctrico y mecánico más 1 repuesto	Carga del edificio total + 1 de repuesto
2	Generadores en un único bus	Si	Si	Si	No
3	Un único generador por sistema con (1) generador de repuesto	No	Si	Si	Si
4	Una protección de falla de tierra individual de 83 ft. (pies) para c/generador	No	Si	Si	Si

Tabla 23: Subsistema Eléctrico, Sistema de generación Standby

Fuente: TIA-942

	Pruebas para el banco de cargas	TIER 1	TIER 2	TIER 3	TIER 4
1	Solo pruebas de los módulos del UPS	Solo para el tamaño de las computadoras y el sistema de telecomunicaciones, eléctrico y mecánico	Solo para el tamaño de las computadoras y el sistema de telecomunicaciones, eléctrico y mecánico	Solo para el tamaño de las computadoras y el sistema de telecomunicaciones, eléctrico y mecánico más 1 repuesto	Carga del edificio total + 1 de repuesto
2	Solo pruebas de los generadores	Si	Si	Si	No
3	Pruebas tanto de los módulos del UPS como de los generadores	No	Si	Si	Si
4	Una protección de falla de tierra individual de 83 ft. (pies) para c/generador	No	Si	Si	Si
5	Aparamenta del UPS	No	No	No	Si
6	Instalado permanente	No - Alquilado	No - Alquilado	No - Alquilado	Si

Tabla 24: Subsistema Eléctrico, Pruebas para el banco de descargas

Fuente: TIA-942

Mantenimiento de los equipos		TIER 1	TIER 2	TIER 3	TIER 4
1	Staff de mantenimiento	Solo para el tamaño de las computadoras y el sistema de telecomunicaciones, eléctrico y mecánico	Solo para el tamaño de las computadoras y el sistema de telecomunicaciones, eléctrico y mecánico	Solo para el tamaño de las computadoras y el sistema de telecomunicaciones, eléctrico y mecánico más 1 repuesto	Carga del edificio total + 1 de repuesto
2	Mantenimiento preventivo	Ninguno	Ninguno	Programa de mantenimiento preventivo limitado	Programa de mantenimiento preventivo comprensivo
3	Programas de formación con instituciones	Ninguno	Ninguno	Programa de formación comprensiva	Programa de formación comprensiva que incluye procedimientos de operación manual y si es necesario al sistema de control de bypass

Tabla 25: Subsistema Eléctrico, Mantenimiento de los Equipos

Fuente: TIA-942

Subsistema Mecánico

General Selección de Sitio		TIER 1	TIER 2	TIER 3	TIER 4
1	Enrutamiento de agua o de drenaje sin tuberías en el equipo del centro de datos en el centro de datos y espacio.	Permitido pero no recomendado	Permitido pero no recomendado	No permitido	No permitido
2	La presión positiva en el aula de informática y espacios asociados en relación con el exterior y que no sean del centro de datos	No requiere	Si	Si	Si
3	Los desagües de condensado de agua se encuentran en el piso en sala de ordenadores, de agua del humidificador de color, y por aspersión de descarga de agua.	Si	Si	Si	Si
4	Sistemas mecánicos en generadores StandBy	No requiere	Si	Si	Si

Tabla 26: Subsistema Mecánico, General

Fuente: TIA-942

Sistema de refrigeración por agua		TIER 1	TIER 2	TIER 3	TIER 4
1	Cubierta de terminales de unidades de aire acondicionado	No aire acondicionados redundantes	Una unidad AC redundante por área crítica	Cantidad de unidades AC suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de unidades AC suficiente para mantener un área crítica durante la perdida de electricidad de una fuente
2	Control de humedad para el Centro de Datos	Humidificación provista	Humidificación provista	Humidificación provista	Humidificación provista
3	Servicio eléctrico a los equipos mecánicos	Equipos AC con una única ruta de acceso	Equipos AC con una única ruta de acceso	Múltiples equipos AC con una única ruta de acceso	Múltiples equipos AC con una única ruta de acceso

Tabla 27: Subsistema Mecánico, Sistema de refrigeración por agua

Fuente: TIA-942

Eliminación de Calor		TIER 1	TIER 2	TIER 3	TIER 4
1	Seco-enfriadores (si procede)	Seco enfriadores no redundantes	Un Seco enfriadores redundante por sistema	Cantidad de seco enfriadores suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de seco enfriadores suficiente para mantener un área crítica durante la perdida de electricidad de una fuente
2	Circuito cerrado de fluido Enfriadores (si procede)	Enfriadores de fluido no redundantes	Un Enfriador de fluido por sistema	Cantidad de enfriadores de fluidos suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de enfriadores de fluidos suficiente para mantener un área crítica durante la perdida de electricidad de una fuente
2	Bombas de circulación	Bombas de circulación no redundantes	Una Bomba de circulación redundante por sistema	Cantidad de bombas de circulación suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de bombas de circulación suficiente para mantener un área crítica durante la perdida de electricidad de una fuente

3	Sistema de tuberías	Sistema de condensación de agua con una única ruta de acceso	Sistema de condensación de agua con una única ruta de acceso	Sistema de condensación de agua con ruta de acceso dual.	Sistema de condensación de agua con ruta de acceso dual.

Tabla 28: Subsistema Mecánico, Eliminación de Calor

Fuente: TIA-942

	Sistema de Agua Fría	TIER 1	TIER 2	TIER 3	TIER 4
1	Cubierta de terminales unidades de aire acondicionado	Aires acondicionados no redundantes	Un aire acondicionado redundante por sistema	Cantidad de aires acondicionados suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de aires acondicionados suficiente para mantener un área crítica durante la perdida de electricidad de una fuente
2	Control de humedad para el Centro de Datos	Humidificación provista	Humidificación provista	Humidificación provista	Humidificación provista
3	Servicio eléctrico a los equipos mecánicos	Equipos AC con una única ruta de acceso	Equipos AC con una única ruta de acceso	Múltiples equipos AC con una única ruta de acceso	Múltiples equipos AC con una única ruta de acceso

Tabla 29: Subsistema Mecánico, Sistema de Agua Fría

Fuente: TIA-942

	Eliminación del Calor	TIER 1	TIER 2	TIER 3	TIER 4
1	Sistema de tuberías de agua fría	Sistema de tuberías de agua fría condensación de agua con una única ruta de acceso	Sistema de tuberías de agua fría condensación de agua con una única ruta de acceso	Sistema de tuberías de agua fría condensación de agua con rutas de acceso dual	Sistema de tuberías de agua fría condensación de agua con rutas de acceso dual
2	Bombas de circulación de agua fría	Bombas de circulación de agua fría no redundantes	Una Bomba de circulación de agua fría redundante por sistema	Cantidad de bombas de circulación de agua fría suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de bombas de circulación de agua fría suficiente para mantener un área crítica durante la perdida de electricidad de una fuente
3	Refrigeradores de refrigeración por aire	Refrigeradores de refrigeración por aire no redundantes	Un refrigerador de refrigeración por aire redundante por sistema	Cantidad de refrigeradores de refrigeración por aire suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de refrigeradores de refrigeración por aire suficiente para mantener un área crítica durante la perdida de electricidad de una fuente

4	Enfriadores refrigerados por agua	Enfriadores refrigerados por agua no redundantes	Un enfriador refrigerados por agua redundante por sistema	Cantidad de enfriadores refrigerados por agua suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de enfriadores refrigerados por agua suficiente para mantener un área crítica durante la perdida de electricidad de una fuente
5	Torres de enfriamiento	Torres de enfriamiento no redundantes	Una torre de enfriamiento redundante por sistema	Cantidad de Torres de enfriamiento suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de Torres de enfriamiento suficiente para mantener un área crítica durante la perdida de electricidad de una fuente
6	Condensadores de bombas de agua	Condensadores de bombas de agua no redundantes	Un condensador de bombas de agua redundante por sistema	Cantidad de Condensadores de bombas de agua suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de Condensadores de bombas de agua suficiente para mantener un área crítica durante la perdida de electricidad de

					una fuente
7	Sistema de tuberías de condensadores de agua	Sistema de condensación de agua con una única ruta de acceso	Sistema de condensación de agua con una única ruta de acceso	Sistema de condensación de agua con ruta de acceso dual.	Sistema de condensación de agua con ruta de acceso dual.

Tabla 30: Subsistema Mecánico, Eliminación del Calor

Fuente: TIA-942

	Sistema de refrigeración por aire	TIER 1	TIER 2	TIER 3	TIER 4
1	Cubierta de terminales unidades de aire acondicionado y al aire libre Condensadores	No aire acondicionados redundantes	Una unidad AC redundante por área crítica	Cantidad de unidades AC suficiente para mantener un área crítica durante la perdida de electricidad de una fuente	Cantidad de unidades AC suficiente para mantener un área crítica durante la perdida de electricidad de una fuente
2	Servicio eléctrico a los equipos mecánicos	Equipos AC con una única ruta de acceso	Equipos AC con una única ruta de acceso	Múltiples equipos AC con una única ruta de acceso	Múltiples equipos AC con una única ruta de acceso
3	Control de humedad para el Centro de Datos	Humidificación provista	Humidificación provista	Humidificación provista	Humidificación provista

Tabla 31: Subsistema Mecánico, Sistema de Refrigeración por aire

Fuente: TIA-942

	Sistema de Control HVAC	TIER 1	TIER 2	TIER 3	TIER 4
1	Sistema de Control HVAC	Falla en el sistema de control interrumpirá el enfriamiento de las áreas críticas	Falla en el sistema de control no interrumpirá el enfriamiento de las áreas críticas	Falla en el sistema de control no interrumpirá el enfriamiento de las áreas críticas	Falla en el sistema de control no interrumpirá el enfriamiento de las áreas críticas
2	Fuente de Poder para el Sistema de Control HVAC	Electricidad para el sistema de control HVAC con una única ruta de acceso	Electricidad de un UPS a los equipos AC redundantes	Electricidad de un UPS a los equipos AC redundantes	Electricidad de un UPS a los equipos AC redundantes

Tabla 32: Subsistema Mecánico, Sistema de Control HVAC

Fuente: TIA-942

Sistema de Tuberías (para la eliminación del calor)		TIER 1	TIER 2	TIER 3	TIER 4
1	Fuentes duales para arreglar el agua	Fuente de agua única, sin respaldo en el lugar de almacenamiento.	Fuente de agua dual, o una fuente + respaldo en el lugar de almacenamiento.	Fuente de agua dual, o una fuente + respaldo en el lugar de almacenamiento.	Fuente de agua dual, o una fuente + respaldo en el lugar de almacenamiento.
2	Puntos de conexión para el sistema de condensación del agua	Un único punto de conexión	Un único punto de conexión	Dos punto de conexión	Dos punto de conexión

Tabla 33: Subsistema Mecánico, Sistema de Tuberías

Fuente: TIA-942

	Sistema de combustible de aceite	TIER 1	TIER 2	TIER 3	TIER 4
1	Tanques de almacenamiento	Tanque de almacenamiento	Múltiples tanques de almacenamiento	Múltiples tanques de almacenamiento	Múltiples tanques de almacenamiento
2	Las bombas del tanque de almacenamiento y tuberías	Una Bomba y/o un tubo de provisiones	Múltiples Bombas, múltiples tubos de provisiones	Múltiples Bombas, múltiples tubos de provisiones	Múltiples Bombas, múltiples tubos de provisiones

Tabla 34: Subsistema Mecánico, Sistema de Combustible de Aceite

Fuente: TIA-942

Supresión de Fuego		TIER 1	TIER 2	TIER 3	TIER 4
1	Sistema de detección de fuego	No	Si	Si	Si
2	Sistema de rociadores contra incendios	Cuando sea requerido	Pre-Acción (cuando requerido)	Pre-Acción (cuando requerido)	Pre-Acción (cuando requerido)
3	Sistema de supresión gaseosa	No	No	Agentes limpios listados en la NFPA 2001	Agentes limpios listados en la NFPA 2001
4	Sistema de aviso temprano de detección de humo	No	Si	Si	Si
5	Sistemas de detección de fugas de agua	No	Si	Si	Si

Tabla 35: Subsistema Mecánico, Supresión de Fuego

Fuente: TIA-942

Subsistema de Telecomunicaciones

General Selección de Sitio		TIER 1	TIER 2	TIER 3	TIER 4
1	Cableado, racks, gabinetes y vías cumplen con las especificaciones de la TIA.	Si	Si	Si	Si
2	Entradas de proveedor de accesos encaminadas diversamente y agujeros de mantenimiento con un mínimo de separación de 20m.	No	Si	Si	Si
3	Proveedor de servicios de acceso redundante, proveedores de acceso múltiple, oficinas centrales, proveedor de accesos de derechos de vía.	No	No	Si	Si
4	Entrada al cuarto secundaria	No	No	Si	Si
5	Área de distribución secundaria	No	No	No	Opcional
6	Rutas *Backbone* redundantes	No	No	Si	Si
7	Cableado horizontal redundante	No	No	No	Opcional
8	Los routers y switches tienen suministro de poder redundante y procesadores	No	Si	Si	Si

9	Múltiples routers y switches para redundancia	No	No	Si	Si
10	Paneles, tomacorrientes y cableado parchados y etiquetados por ANSI/TIA/EIA-606-A y el anexo B de este estándar. Gabinetes y racks etiquetados en el frente y la parte posterior.	Si	Si	Si	Si
11	Cordones y *jumpers* parcheados y etiquetados en ambos lados con el nombre de la conexión en ambos lados.	No	Si	Si	Si
12	Documentación de cumplimiento con ANSI/TIA/EIA-606-A y el anexo B de este estándar para el parcheado de los paneles y el parcheado de los cables.	No	No	Si	Si

Tabla 36: Subsistema de Telecomunicaciones, General

Fuente: TIA-942

Niveles de calificación de la evaluación

Para poder estandarizar los resultados de la evaluación, se decidió crear una clasificación de resultados, los cuales serán detallados a continuación.

La evaluación tiene seis posibles resultados:

TIER 1:

- Susceptibles a las interrupciones de los dos previstos y actividad no planificada un único camino por el poder y la distribución de refrigeración, no hay componentes redundantes (N)
- Puede o no tener un piso elevado, UPS o generador
- Toma 3 meses para implementación
- Tiempo de inactividad anual de 28,8 horas
- Debe ser cerrado por completo para realizar mantenimiento preventivo

TIER 2:

- Menos susceptibles a la interrupción de los dos previstos y actividad no planificada un único camino por el poder y la interrupción de refrigeración, incluye componentes redundantes (N +1)
- Incluye un piso falso, UPS y generadores
- Toma 3 a 6 meses para poner en práctica
- Tiempo de inactividad anual de 22,0 horas
- Mantenimiento de la trayectoria de alimentación y otras partes de la infraestructura requieren un cierre de procesamiento

TIER 3:

- Permite la actividad planificada sin interrumpir el equipo sucesos de operación de hardware, pero todavía no planificado causar una interrupción

- Múltiples energía y las rutas de distribución de refrigeración, pero con sólo una ruta activa, incluye componentes redundantes (N +1)

- La implementación dura de 15 a 20 meses

- Tiempo de inactividad anual de 1,6 horas

- Incluye un piso elevado y suficiente capacidad y de distribución para llevar carga en una ruta, mientras que realizar el mantenimiento de la otra.

TIER 4:

- Actividad planificada no interrumpa la carga y los datos críticos centro puede sostener por lo menos un peor de los casos no planificado evento sin impacto de la carga crítica

- Potencia de múltiples activos y las rutas de distribución de refrigeración, incluye componentes redundantes (2 (N +1), es decir, dos UPS cada uno con redundancia N +1)

- La implementación dura 15 a 20 meses.

- Tiempo de inactividad anual de 0,4 horas

NO APLICA:

- Este resultado aplica cuando no se puede evaluar porque el centro de datos evaluado no cuenta con la característica que se evaluarán.

NO CUMPLE:

- Este resultado aplica cuando el TIER1 tiene parámetros específicos.

La evaluación de cada subsistema se llevó a cabo de forma independiente con el objetivo de no mezclar los resultados y que la evaluación de cada subsistema sea lo más real y sincera posible. La metodología de evaluación se he denominado "El menor arrastra a todos", esta metodología consiste en calificar cada una de las sugerencias del

estándar TIA, asignándole la calificación correspondiente según los tipos de resultados y el resultado final de cada subsistema es el menor de todos.

Resultados de la Evaluación

Considerando únicamente la clasificación desarrollada en el proyecto, el resultado de la evaluación es:

ID	A EVALUAR	CATEGORIA	SUBCATEGORIA	RESULTADO
1	Proximidad al área de peligro de inundación como en un mapa federal de límites de riesgo de inundación o mapa de tasas de seguro de inundación	Arquitectónico	Selección de sitio	Tier 2
2	Proximidad con vías de agua costera	Arquitectónico	Selección de sitio	Tier 2
3	Proximidad con arterias de mayor tráfico	Arquitectónico	Selección de sitio	Tier 2
4	Proximidad con aeropuertos	Arquitectónico	Selección de sitio	Tier 2
5	Proximidad con una gran área metropolitana	Arquitectónico	Selección de sitio	Tier 2
6	División de las áreas de estacionamiento de los visitantes con los empleados	Arquitectónico	Aparcamiento	Tier 2
7	Separados de los muelles de carga	Arquitectónico	Aparcamiento	Tier 2

8	Proximidad del estacionamiento de los visitantes hacia las paredes perimetrales del edificio del data center	Arquitectónico	Aparcamiento	Tier 2
9	Número de inquilinos dentro del edificio	Arquitectónico	Aparcamiento	Tier 2
10	Tipo de construcción	Arquitectónico	Construcción del edificio	Tier 2
11	Muros exteriores	Arquitectónico	Requerimientos de resistividad al fuego	Tier 2
12	Muros interiores	Arquitectónico	Requerimientos de resistividad al fuego	Tier 2
13	Muros no portantes exteriores	Arquitectónico	Requerimientos de resistividad al fuego	Tier 2
14	Marco estructural	Arquitectónico	Requerimientos de resistividad al fuego	Tier 2
15	Tabiques al interior de lo que no es la sala de computadoras	Arquitectónico	Requerimientos de resistividad al fuego	Tier 2

16	Tabiques al interior de la sala de computadoras	Arquitectónico	Requerimientos de resistividad al fuego	Tier 2
17	Ejes de cajas	Arquitectónico	Requerimientos de resistividad al fuego	Tier 2
18	Pisos y techos de planta	Arquitectónico	Requerimientos de resistividad al fuego	Tier 2
19	Techos y cubiertas de techos	Arquitectónico	Requerimientos de resistividad al fuego	Tier 2
20	Cumple con los requisitos del NFPA75	Arquitectónico	Requerimientos de resistividad al fuego	Tier 1
21	Barreras de vapor para los muros y techo de la sala de computadores	Arquitectónico	Componentes del edificio	Tier 1
22	Múltiples entradas al edificio con controles de seguridad	Arquitectónico	Componentes del edificio	Tier 2
23	Piso de la construcción del panel	Arquitectónico	Componentes del edificio	Tier 2

24	Bajo la estructura	Arquitectónico	Componentes del edificio	Tier 2
25	Construcción de los techos	Arquitectónico	Techos dentro de las salas de computadoras	Tier 2
26	Altura del techo	Arquitectónico	Componentes del edificio	Tier 1
27	Clase	Arquitectónico	Material para techos	Tier 4
28	Tipo	Arquitectónico	Material para techos	Tier 2
29	Resistencia al levantamiento del viento	Arquitectónico	Material para techos	Tier 1
30	Azotea a cuestas	Arquitectónico	Material para techos	No aplica
31	Ratio de fuego f	Arquitectónico	Puertas y ventanas	Tier 2
32	Tamaño de la puerta	Arquitectónico	Puertas y ventanas	Tier 2
33	Dispositivo de seguridad unipersonal, portal o algún otro hardware designado para prevenir que se cuelguen	Arquitectónico	Puertas y ventanas	Tier 1

34	No hay ventanas exteriores en el perímetro de la sala de computadoras	Arquitectónico	Puertas y ventanas	Tier 2
35	Construcción provee protección contra la radiación electromagnética	Arquitectónico	Puertas y ventanas	Tier 2
36	Vestíbulo de entrada	Arquitectónico	Puertas y ventanas	Tier 1
37	Separado físicamente de otras áreas del centro de datos	Arquitectónico	Puertas y ventanas	Tier 1
38	Separación de fuego de otras áreas del centro de datos	Arquitectónico	Puertas y ventanas	Tier 2
39	Counter de seguridad	Arquitectónico	Puertas y ventanas	Tier 2
40	Dispositivo de seguridad unipersonal, portal o algún otro hardware designado para prevenir que se cuelguen	Arquitectónico	Puertas y ventanas	Tier 2
41	Separado físicamente de otras áreas del centro de datos	Arquitectónico	Oficinas administrativas	Tier 1

42	Separación de fuego de otras áreas del centro de datos	Arquitectónico	Oficinas administrativas	Tier 2
43	Separado físicamente de otras áreas del centro de datos	Arquitectónico	Oficina de seguridad	Tier 1
44	Separación de fuego de otras áreas del centro de datos	Arquitectónico	Oficina de seguridad	Tier 1
45	Mirillas de 180 grados en el equipo de seguridad y cuartos de monitoreo	Arquitectónico	Oficina de seguridad	Tier 1
46	Equipos de seguridad y cuartos de monitoreo con 16mm (5/8 in) madera contrachapada (excepto donde la resistencia a balas es recomendada o requerida)	Arquitectónico	Oficina de seguridad	Tier 1
47	Cuarto de seguridad dedicado para el equipo de seguridad y vigilancia	Arquitectónico	Oficina de seguridad	Tier 2
48	Separado físicamente de otras áreas del centro de datos	Arquitectónico	Centro de operaciones	Tier 2

49	Separación de fuego de otras áreas del centro de datos	Arquitectónico	Centro de operaciones	Tier 2
50	Proximidad con la sala de computadoras	Arquitectónico	Centro de operaciones	Tier 2
51	Proximidad con la sala de computadoras y áreas de soporte	Arquitectónico	Baños y áreas de descanso	Tier 2
52	Separación de fuego de otras áreas del centro de datos y áreas de soporte	Arquitectónico	Baños y áreas de descanso	Tier 2
53	Ancho de los pasillos para el mantenimiento, reparación o eliminación de equipos	Arquitectónico	Ups y sala de baterías	Tier 2
54	Proximidad con la sala de computadoras	Arquitectónico	Ups y sala de baterías	Tier 2
55	Separación de fuego de otras áreas del centro de datos y áreas de soporte	Arquitectónico	Ups y sala de baterías	Tier 2
56	Separación de fuego de otras áreas del centro de datos y áreas de soporte	Arquitectónico	Corredores requeridos de salida	Tier 2
57	Ancho	Arquitectónico	Corredores requeridos de	Tier 2

			salida	
58	Área de envíos y recibimientos	Arquitectónico	Corredores requeridos de salida	Tier 1
59	Separado físicamente de otras áreas del centro de datos	Arquitectónico	Corredores requeridos de salida	Tier 1
60	Separación de fuego de otras áreas del centro de datos	Arquitectónico	Corredores requeridos de salida	Tier 2
61	Protección física de los muros expuestas al levantamiento de equipo de tráfico	Arquitectónico	Corredores requeridos de salida	Tier 2
62	Número de muelles de carga	Arquitectónico	Corredores requeridos de salida	Tier 1
63	Muelles de carga separados de las áreas de aparcamiento	Arquitectónico	Corredores requeridos de salida	Tier 2
64	Counter de seguridad	Arquitectónico	Corredores requeridos de salida	Tier 2

65	Proximidad con la sala de computadoras y áreas de soporte	Arquitectónico	Generador y áreas de almacenamiento de combustible	Tier 2
66	Proximidad a áreas de acceso al público	Arquitectónico	Generador y áreas de almacenamiento de combustible	Tier 2
67	Capacidad del ups del CPU del sistema	Arquitectónico	Seguridad	Tier 1
68	Capacidad del ups de los paneles de recopilación de datos (paneles de campo)	Arquitectónico	Seguridad	Tier 1
69	Capacidad del ups del dispositivo de campo	Arquitectónico	Seguridad	Tier 1
70	Staff de seguridad por turno	Arquitectónico	Seguridad	Tier 1
71	Generadores	Arquitectónico	Control, monitoreo y accesos de seguridad	Tier 1
72	Ups, teléfonos y cuartos.	Arquitectónico	Control, monitoreo y accesos de seguridad	Tier 1

73	Bóvedas de fibra	Arquitectónico	Control, monitoreo y accesos de seguridad	Tier 1
74	Puertas de salida de emergencia	Arquitectónico	Control, monitoreo y accesos de seguridad	Tier 1
75	Ventana/apertura accesible desde el exterior	Arquitectónico	Control, monitoreo y accesos de seguridad	Tier 1
76	Centro de operaciones de seguridad	Arquitectónico	Control, monitoreo y accesos de seguridad	Tier 2
77	Centro de operaciones de red	Arquitectónico	Control, monitoreo y accesos de seguridad	Tier 2
78	Cuartos de equipos de seguridad	Arquitectónico	Control, monitoreo y accesos de seguridad	Tier 1
79	Puertas en cuartos de cómputo	Arquitectónico	Control, monitoreo y accesos de seguridad	Tier 1
80	Puertas de perímetro del edificio	Arquitectónico	Control, monitoreo y	Tier 1

			accesos de seguridad	
81	Puerta del vestíbulo hacia el piso	Arquitectónico	Control, monitoreo y accesos de seguridad	Tier 1
82	Counter de seguridad en el vestíbulo	Arquitectónico	Muros, ventanas y puertas resistentes a balas	Tier 2
83	Counter de seguridad en envíos y recepción	Arquitectónico	Muros, ventanas y puertas resistentes a balas	Tier 3
84	Perímetro del edificio y aparcamiento	Arquitectónico	Monitoreo CCTV	Tier 2
85	Generadores	Arquitectónico	Monitoreo CCTV	Tier 2
86	Puertas de acceso controladas	Arquitectónico	Monitoreo CCTV	Tier 1
87	Pisos de cuarto de computo	Arquitectónico	Monitoreo CCTV	Tier 2
88	Ups, teléfonos y cuartos.	Arquitectónico	Monitoreo CCTV	Tier 2
89	Grabación CCTV de todas las actividades en todas las cámaras	Arquitectónico	Ctv.	Tier 2

90	Ratio de grabación (frames por segundo)	Arquitectónico	Ctv.	Tier 2
91	Zona sísmica	Arquitectónico	Estructural	Tier 4
92	Instalación designada para los requerimientos de zona sísmica	Arquitectónico	Estructural	Tier 3
93	Espectro de respuesta - grados de aceleraciones sísmicas locales	Arquitectónico	Estructural	Tier 2
94	Factor de importancia	Arquitectónico	Estructural	Tier 1
95	Equipo de telecomunicaciones gabinetes/racks anclados a la base o soportada en la parte superior y base	Arquitectónico	Estructural	Tier 1
96	Limitaciones de deflexión en los equipos de telecomunicaciones dentro de los límites aceptables por los accesorios eléctricos	Arquitectónico	Estructural	Tier 2
97	Deterioro de los recorridos de los conductos eléctricos y las bandejas de los cables	Arquitectónico	Estructural	Tier 1

98	Deterioro del recorrido del mayor sistema mecánico	Arquitectónico	Estructural	Tier 1
99	Capacidad del piso de carga superimpuesta en carga viva	Arquitectónico	Estructural	Tier 1
100	Capacidad colgante del piso para cargas auxiliares suspendidas desde abajo	Arquitectónico	Estructural	Tier 1
101	Grosor de la losa de concreto	Arquitectónico	Estructural	Tier 1
102	Mezcla de concreto sobre las flautas de los pisos elevados afecta al tamaño del ancla que se pueda instalar	Arquitectónico	Estructural	Tier 1
103	Lfrs del edificio que indique desplazamiento de la estructura	Arquitectónico	Estructural	Tier 1
104	Disipación de la energía del edificio - pasivo (absorción de energía)	Arquitectónico	Estructural	Tier 2

105	Ups/batería vs composición del edificio. Pisos de concreto son más difíciles de mejorar para cargas intensas. Enmarcados de acero con cubierta de metal y llenado mucho más sencillo de mejorar	Arquitectónico	Estructural	Tier 1
106	Enmarcados de acero y llenado	Arquitectónico	Estructural	Tier 1
107	Cableado, racks, gabinetes y vías cumplen con las especificaciones de la TIA.	Telecomunicaciones	Selección de sitio	No cumple
108	Entradas de proveedor de accesos encaminadas diversamente y agujeros de mantenimiento con un mínimo de separación de 20m.	Telecomunicaciones	Selección de sitio	Tier 1
109	Proveedor de servicios de acceso redundante, proveedores de acceso múltiple, oficinas centrales, proveedor de accesos de derechos de vía.	Telecomunicaciones	Selección de sitio	No aplica
110	Entrada al cuarto secundaria	Telecomunicaciones	Selección de sitio	Tier 2
111	Área de distribución secundaria	Telecomunicaciones	Selección de sitio	Tier 3

112	Rutas backbone redundantes	Telecomunicaciones	Selección de sitio	Tier 2
113	Cableado horizontal redundante	Telecomunicaciones	Selección de sitio	Tier 3
114	Los routers y switches tienen suministro de poder redundante y procesadores	Telecomunicaciones	Selección de sitio	Tier 1
115	Múltiples routers y switches para redundancia	Telecomunicaciones	Selección de sitio	Tier 2
116	Paneles, tomacorrientes y cableado parchados y etiquetados por ANSI/TIA/eia-606-a y el anexo b de este estándar. Gabinetes y racks etiquetados en el frente y la parte posterior.	Telecomunicaciones	Selección de sitio	No cumple
117	Cordones y jumpers parcheados y etiquetados en ambos lados con el nombre de la conexión en ambos lados.	Telecomunicaciones	Selección de sitio	No cumple
118	Documentación de cumplimiento con ANSI/TIA/eia-606-a y el anexo b de este estándar para el parcheado de los paneles y el parcheado de los cables.	Telecomunicaciones	Selección de sitio	Tier 2

119	Enrutamiento de agua o tubería de drenaje no estén asociadas con los equipos del centro de datos en los espacios del data center	Sistema mecánico	Selección de sitio	Tier 4
120	La presión es positiva en el ambiente de computadoras y espacios asociados, en relación con el exterior y otros ambientes que no pertenezcan al centro de datos	Sistema mecánico	Selección de sitio	Tier 4
121	Desagües de piso para el agua condensada, la del humidificador de agua de lavatorios y aspersores de agua en el data center.	Sistema mecánico	Selección de sitio	No aplica
122	Sistemas mecánicos en generadores standby	Sistema mecánico	Selección de sitio	Tier 1
123	Terminales de unidades de aire acondicionado dentro del data center	Sistema mecánico	Sistema de refrigeración por agua	Tier 1
124	Control de humedad para el centro de datos	Sistema mecánico	Sistema de refrigeración por agua	No cumple
125	Servicio eléctrico a los equipos mecánicos	Sistema mecánico	Sistema de refrigeración	Tier 2

			por agua	
126	Dry-coolers (si aplica)	Sistema mecánico	Eliminación de calor1	No aplica
127	Closed-circuit fluid coolers (en caso aplique)	Sistema mecánico	Eliminación de calor1	No aplica
128	Bombas de circulación	Sistema mecánico	Eliminación de calor1	No aplica
129	Sistema de tuberías	Sistema mecánico	Eliminación de calor1	No aplica
130	Terminales unidades de aire acondicionado dentro del data center	Sistema mecánico	Sistema de agua fría	Tier 1
131	Control de humedad para el centro de datos	Sistema mecánico	Sistema de agua fría	No cumple
132	Servicio eléctrico a los equipos mecánicos	Sistema mecánico	Sistema de agua fría	No aplica
133	Sistema de tuberías de agua fría	Sistema mecánico	Eliminación de calor2	No aplica
134	Bombas de circulación de agua fría	Sistema mecánico	Eliminación de calor2	No aplica
135	Enfriadoras	Sistema mecánico	Eliminación de calor2	No aplica
136	Enfriadores refrigerados por agua	Sistema mecánico	Eliminación de calor2	No aplica

137	Torres de enfriamiento	Sistema mecánico	Eliminación de calor2	No aplica
138	Condensadores de bombas de agua	Sistema mecánico	Eliminación de calor2	Tier 1
139	Sistema de tuberías de condensadores de agua	Sistema mecánico	Eliminación de calor2	Tier 2
140	Unidades de aire acondicionado al aire libre e internas	Sistema mecánico	Sistema de refrigeración por aire	Tier 1
141	Servicio eléctrico a los equipos mecánicos	Sistema mecánico	Sistema de refrigeración por aire	Tier 1
142	Control de humedad para el centro de datos	Sistema mecánico	Sistema de refrigeración por aire	No aplica
143	Sistema de control HVAC	Sistema mecánico	Sistema de control HVAC	No cumple
144	Fuente de poder para el sistema de control HVAC	Sistema mecánico	Sistema de control HVAC	No cumple
145	Fuentes duales para el agua de aporte	Sistema mecánico	Sistema de tuberías	No aplica
146	Puntos de conexión para el sistema de condensación del agua	Sistema mecánico	Sistema de tuberías	No aplica

147	Estantes de almacenamiento	Sistema mecánico	Sistema de combustible de aceite	No aplica
148	Almacenamiento de bombas y tuberías	Sistema mecánico	Sistema de combustible de aceite	No aplica
149	Sistema de detección de fuego	Sistema mecánico	Supresión de fuego	Tier 4
150	Sistema de rociadores contra incendios	Sistema mecánico	Supresión de fuego	No aplica
151	Sistema de supresión gaseosa	Sistema mecánico	Supresión de fuego	Tier 2
152	Sistema de aviso temprano de detección de humo	Sistema mecánico	Supresión de fuego	Tier 4
153	Sistemas de detección de fugas de agua	Sistema mecánico	Supresión de fuego	Tier 1
154	Número de rutas de llegada/entrega.	Eléctrico	General	Tier 2
155	Línea de amperaje.	Eléctrico	General	Tier 3
156	El sistema permite el mantenimiento concurrido.	Eléctrico	General	Tier 2

157	Equipo de cables de alimentación de las computadoras y equipos de telecomunicaciones.	Eléctrico	General	Tier 1
158	Todos los equipos del sistema eléctrico deben estar etiquetados con la certificación de una prueba de laboratorio de terceros.	Eléctrico	General	No cumple
159	Puntos únicos de fallo	Eléctrico	General	Tier 2
160	Sistema de transferencia de carga crítica	Eléctrico	General	No cumple
161	Llave de bypass	Eléctrico	General	Tier 2
162	Generadores del tamaño correcto de acuerdo a la capacidad del ups instalado	Eléctrico	General	No cumple
163	Capacidad del combustible del generador (a carga plena)	Eléctrico	General	Tier 1
164	Redundancia del ups	Eléctrico	Ups	No cumple
165	Topología del ups	Eléctrico	Ups	No cumple

166	Acuerdo de mantenimiento de derivación en el ups	Eléctrico	Ups	No cumple
167	Nivel de voltaje - distribución de poder del ups	Eléctrico	Ups	No cumple
168	Tableros de paneles - distribución del poder del ups	Eléctrico	Ups	No cumple
169	Todas las computadoras y equipos de telecomunicaciones son alimentados con PDU's	Eléctrico	Ups	No cumple
170	Transformadores k-factor instalados en PDU’s	Eléctrico	Ups	No cumple
171	Bus de sincronización de carga (lbs.)	Eléctrico	Ups	No cumple
172	Componentes redundantes (ups)	Eléctrico	Ups	No cumple
173	El ups se encuentra separado en un panel de distribución separado de los equipos de telecomunicaciones y computadoras.	Eléctrico	Ups	No cumple
174	Sistema de protección de iluminación	Eléctrico	Conexión a tierra	No cumple
175	Terraje del generador y de la entrada de servicio cumple con la norma NEC	Eléctrico	Conexión a tierra	Tier 4

176	Accesorios de iluminación (277v) neutral, aislados de la entrada de servicio derivados de la iluminación del transformador para el aislador de fallas de tierra	Eléctrico	Conexión a tierra	No cumple
177	La infraestructura de la conexión a tierra del data center está dentro de la sala de computadoras.	Eléctrico	Conexión a tierra	Tier 2
178	Activado por el sistema de emergencia de corte de energía (EPO) en las salidas apagando solo al sistema de telecomunicaciones y computadoras.	Eléctrico	Conexión a tierra	No cumple
179	El supresor de fuego automático se libera después del apagado del sistema de telecomunicaciones	Eléctrico	Conexión a tierra	No cumple
180	Sistema de alarma de fuego de la segunda zona se activa con el apagado del sistema de emergencia de corte de energía (EPO) de forma manual	Eléctrico	Conexión a tierra	Tier 3
181	El control maestro desconecta baterías y libera un supresor desde una estación atendida 24/7	Eléctrico	Conexión a tierra	Tier 3

182	Activado por los botones del sistema de emergencia de corte de energía (EPO) en las salidas con liberación de un supresor manual	Eléctrico	Sistemas de emergencia de corte de energía (EPO)	No cumple
183	Se libera el supresor de fuego para el sistema de zonas únicas después del apagado del sistema de emergencias de corte de energía	Eléctrico	Sistemas de emergencia de corte de energía (EPO)	No cumple
184	Activación del sistema de alarma de fuego en la segunda zona. Desconecta las baterías en la primera zona con la liberación del supresor en la segunda zona.	Eléctrico	Sistemas de emergencia de corte de energía (EPO)	No cumple
185	El control maestro desconecta baterías y libera un supresor desde una estación atendida 24/7	Eléctrico	Sistemas de emergencia de corte de energía (EPO)	Tier 2
186	Apagado del poder de los recipientes del ups en el área de la sala de computadoras.	Eléctrico	Sistemas de emergencia de corte de energía (EPO)	No cumple
187	Apagado de corriente AC para cracs y enfriadores	Eléctrico	Sistemas de emergencia de corte de energía (EPO)	No cumple

188	Cumplimiento del código local (eje. Sistemas separados para el ups y HVAC)	Eléctrico	Sistemas de emergencia de corte de energía (EPO)	No cumple
189	Desplegado localmente en el ups	Eléctrico	Monitoreo del sistema	No cumple
190	Interface con el BMS	Eléctrico	Monitoreo del sistema	Tier 3
191	Control remoto	Eléctrico	Monitoreo del sistema	Tier 2
192	Mensaje de texto automático para el servicio de localización de ingenieros	Eléctrico	Monitoreo del sistema	Tier 3
193	Mensaje de texto automático para el servicio de localización de ingenieros	Eléctrico	Monitoreo del sistema	Tier 3
194	Cadena de baterías comunes para todos los módulos	Eléctrico	Configuración de la batería	No cumple
195	Una cadena de batería para c/módulo	Eléctrico	Configuración de la batería	No cumple
196	Tiempo de espera mínimo para la carga plena	Eléctrico	Configuración de la batería	No cumple
197	Tipo de batería	Eléctrico	Configuración de la batería	No cumple

198	Montaje	Eléctrico	Baterías de tipo inundado	No cumple
199	Placas de envoltura	Eléctrico	Baterías de tipo inundado	No cumple
200	Contenedores de derrame de ácido instalados	Eléctrico	Baterías de tipo inundado	No cumple
201	Pruebas de batería a carga plena / horarios de inspección	Eléctrico	Baterías de tipo inundado	No cumple
202	Separado de los cuartos de los equipos ups y celdas	Eléctrico	Sala de baterías	No cumple
203	Las cadenas individuales de baterías están aisladas de uno con otro	Eléctrico	Sala de baterías	No cumple
204	Vista a través de vidrio inastillable en la puerta de la sala de baterías.	Eléctrico	Sala de baterías	No cumple
205	Las desconexiones de las baterías se localizan fuera de la sala de baterías	Eléctrico	Sala de baterías	No cumple
206	Sistema de monitoreo de baterías	Eléctrico	Sala de baterías	No cumple
207	Unidades encerradas separadas por las paredes	Eléctrico	Sistema de cajas del ups rotador (con generadores	No cumple

	nominales de fuego		diésel)	
208	Tanques de combustibles en el exterior	Eléctrico	Sistema de cajas del ups rotador (con generadores diésel)	No cumple
209	Tanques de combustibles en la misma sala que las unidades	Eléctrico	Sistema de cajas del ups rotador (con generadores diésel)	No cumple
210	Tamaño del generador	Eléctrico	Sistema de generación standby	Tier 2
211	Generadores en un único bus	Eléctrico	Sistema de generación standby	Tier 3
212	Un único generador por sistema con (1) generador de repuesto	Eléctrico	Sistema de generación standby	Tier 1
213	Protección de falla de tierra individual de 83 ft. (pies) para c/generador	Eléctrico	Sistema de generación standby	No aplica

214	Pruebas a los módulos del ups	Eléctrico	Pruebas para el banco de cargas	No cumple
215	Pruebas de los generadores	Eléctrico	Pruebas para el banco de cargas	Tier 3
216	Pruebas al ups y generadores simultáneamente	Eléctrico	Pruebas para el banco de cargas	No cumple
217	Llave de bypass del ups	Eléctrico	Pruebas para el banco de cargas	No cumple
218	Equipos instalados permanentemente	Eléctrico	Pruebas para el banco de cargas	Tier 4
219	Staff de mantenimiento	Eléctrico	Mantenimiento de los equipos	Tier 2
220	Mantenimiento preventivo	Eléctrico	Mantenimiento de los equipos	Tier 2
221	Programas de formación con instituciones	Eléctrico	Mantenimiento de los	Tier 2

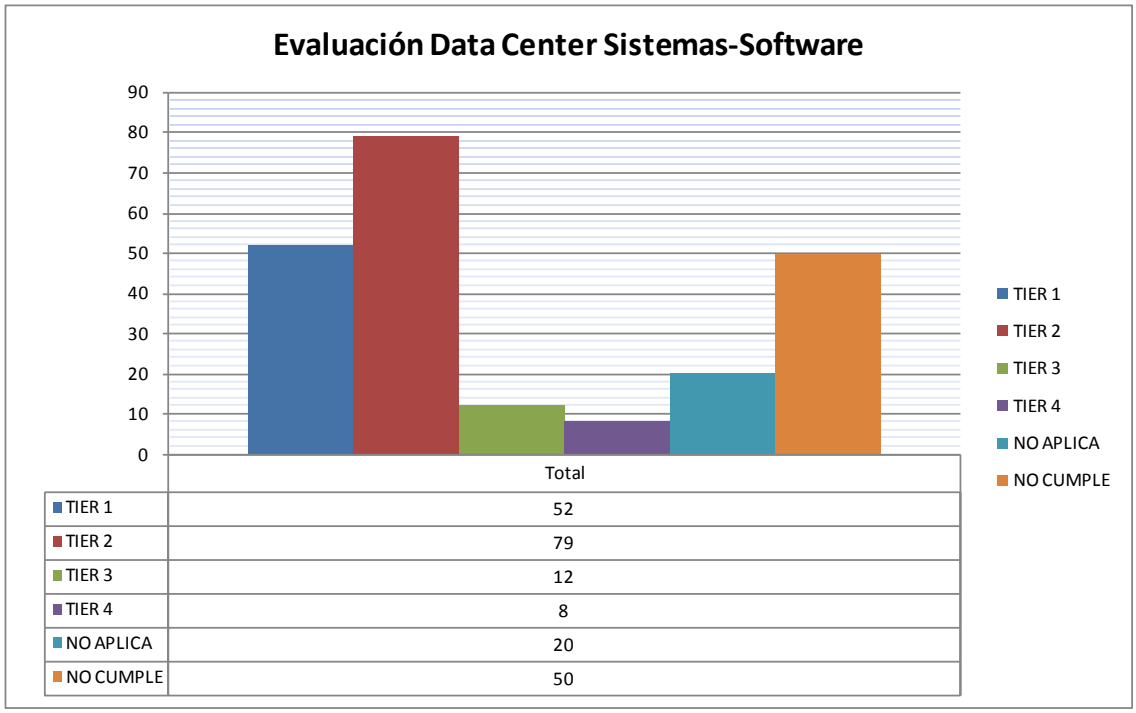
			equipos	

Tabla 37: Resultado de la Evaluación Física

Fuente: Evaluación Propia

Interpretación de Resultados

Al momento de analizar los resultados de evaluación a nivel global se obtiene el siguiente resultado:



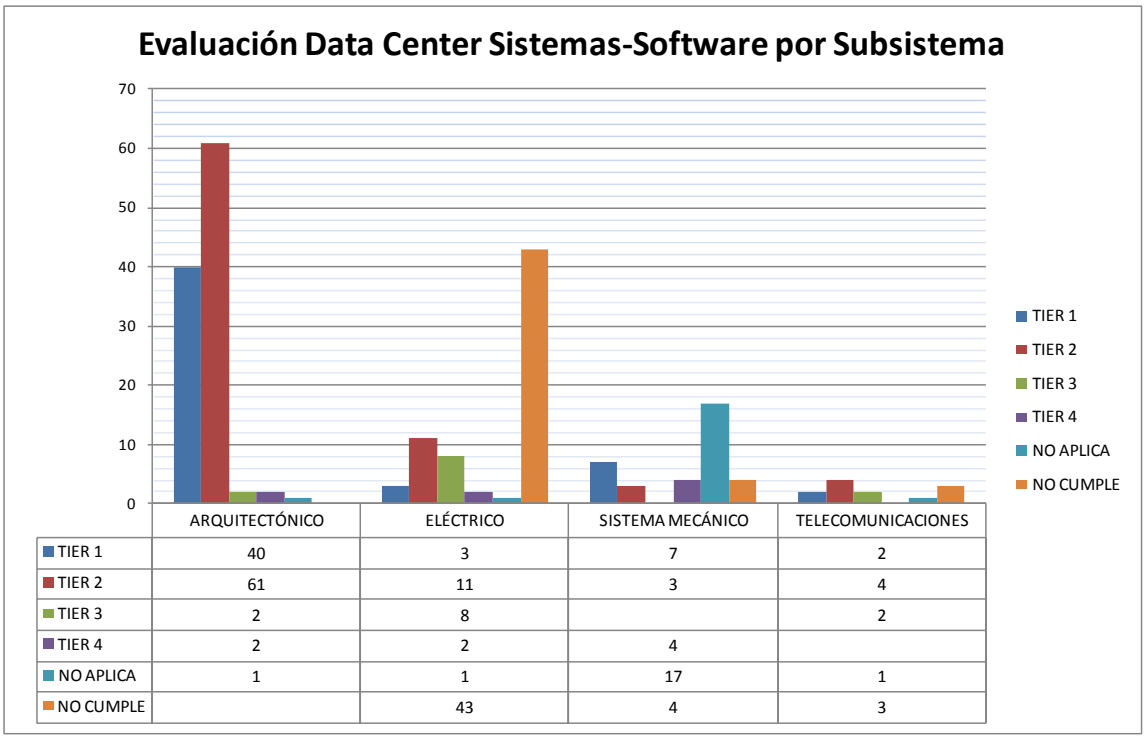
	Total
TIER 1	52
TIER 2	79
TIER 3	12
TIER 4	8
NO APLICA	20
NO CUMPLE	50

Imagen 10: Evaluación Data Center Sistemas - Software 1

Fuente: Elaboración Propia

Este gráfico muestra que el gran porcentaje de sugerencias brindadas por el checklist se encuentran en el nivel ***"TIER2"***, especialmente en el subsistema arquitectónico ya que el centro de datos ha cubierto gran parte de las sugerencias consideradas como críticas para este subsistema. Asimismo, el alto número de sugerencias que se encuentran dentro de la categoría ***"No Cumple"*** se debe a que el centro de datos no cumple con las características mínimas para ser evaluado como TIER1, en el subsistema eléctrico es donde se presenta el alto porcentaje de ***"No Cumple"*** ya que inclusive el nivel más bajo tiene requerimientos.

Por otro lado, si se realiza la evaluación por cada subsistema definido en esta memoria se obtiene el siguiente resultado:



	ARQUITECTÓNICO	ELÉCTRICO	SISTEMA MECÁNICO	TELECOMUNICACIONES
TIER 1	40	3	7	2
TIER 2	61	11	3	4
TIER 3	2	8		2
TIER 4	2	2	4	
NO APLICA	1	1	17	1
NO CUMPLE		43	4	3

Imagen 11: Evaluación Data Center Sistemas – Software 2

Fuente: Elaboración Propia

Al interpretar los resultados de la evaluación se evidencia que todos los subsistemas tienen por lo menos una sugerencia en nivel TIER1 lo cual hace que el resultado global de la evaluación para el centro de datos de la carrera sea TIER1. Al mismo tiempo, cada subsistema tiene como resultado TIER1 puesto que es la menor calificación alcanzada por cada uno.

Si se consideran los resultados de esta evaluación a detalle, se pueden diseñar las políticas y recomendaciones que ayudarán a superar la calificación de TIER1 para cada subsistema, logrando de esta forma que el centro de datos se encuentre en TIER2.

La estrategia a seguir para cada uno de los subsistemas es el levantar las observaciones calificadas como TIER1, No Aplica y No Cumple que se encuentren dentro del alcance del proyecto, para lograr esto se ha establecido una política que cubrirá las onces grandes directrices sugeridos por la NTP 17799.

Para cubrir las deficiencias encontradas se deberían comprar e implementar las siguientes recomendaciones.

Recomendación	Tipo	Costo aproximado
Puerta Contrafuego / Barra Anti pánico	*Seguridad Física*	$1,600
Staff de seguridad (turno)	*Seguridad Física*	$1,000 (mensual)
Sistema Biométrico	*Seguridad Física*	$700
2 Gabinetes	*Seguridad Física*	$4,000
Medidor de Temperatura y Humedad	*Seguridad Física*	$150
Aire Acondicionado de precisión (Liebert, Emerson)	*Seguridad Física*	$25,000
Estantes de almacenamiento	*Seguridad Física*	$200
Sistema de Rociadores contra incendios (FM-200 + detectores marca Vesda)	*Seguridad Física*	$30,000
Sistemas de detección de fugas de agua	*Seguridad Física*	$1,500
Certificación de los equipos	*Seguridad Física*	$3,000
Generadores del tamaño correcto de acuerdo a la capacidad del UPS instalado	*Seguridad Física*	$30,000
Tableros de Paneles de distribución de poder del UPS	*Seguridad Física*	$3,500
UPS (2x2kva)	*Seguridad Física*	$4,000

Tabla 38: Recomendaciones de Adquisiciones a Nivel Físico

Fuente: Elaboración Propia

Procesos de la gestión de la seguridad física

Definición de Procesos: Gestión de Evaluación de Seguridad.

Propósito del Proceso

El propósito del proceso de Gestión de Evaluación Seguridad es determinar cuál es el procedimiento adecuado para llevar a cabo las pruebas de seguridad al interior de las instalaciones del centro de datos y determinar si surgen nuevas incidencias en el centro de datos.

Descripción

El proceso de Gestión de Evaluación de Seguridad inicia cada segunda semana de cada trimestre del ciclo académico. Es en este momento que el Gerente de Seguridad revisa su manual de funciones y revisa el detalle del proceso aquí descrito para determinar cuál es el flujo adecuado para llevar a cabo la evaluación del centro de datos según el checklist.

El alcance de las pruebas se limita únicamente a los componentes que se encuentren dentro del centro de datos de la carrera de Ingeniería de Sistemas de Información. Las pruebas que se llevarán a cabo han sido determinadas mediante un análisis de seguridad y en estas se deben obtener los siguientes indicadores:

- Número de nuevos incidentes.
- Número de incidentes repetitivos.
- Número de incidentes detectados.
- Número de modificaciones en el checklist

Al final de proceso el Gerente de Seguridad se encarga de notificar al Gerente General de IT-Expert sobre las nuevas incidencias encontradas para que esté al tanto de las mismas y de los posibles riesgos inherentes a estas fallas.

Roles

Roles	Descripción
Gerente de Seguridad	Encargado de gestionar y supervisar todo lo relacionado a Seguridad dentro del Centro de Cómputo.
Gerente de Proyectos y Recursos	Es la persona encargada de administrar de los servidores del centro de cómputo, realizar seguimiento a los proyectos de la empresa y atender solicitudes de servicios de TI de las empresas virtuales.
Gerente IT-Expert	Encargado de monitorear el avance y la presentación de los entregables, además de realizar las coordinaciones necesarias entre el Jefe de Proyecto y el Comité de Proyectos.

Entradas del Proceso

Entrada	Descripción	Encargado de Elaboración
-	-	-

Salidas del Proceso

Salida	Descripción	Encargado de Elaboración
Acciones tomadas	El Gerente de Seguridad toma acciones en base al informe consolidado enviado a los Gerentes de IT-Expert y Capstone.	Gerente de Seguridad

Caracterización

	Entrada	Actividad	Salida	Descripción	Responsable
1	-	Inicio	Manual de Oficial de Seguridad. Checklist de Seguridad Físico. Checklist de Seguridad Lógico.	El proceso inicia cada segunda semana del ciclo académico.	Gerente de Seguridad
2	Manual de Oficial de Seguridad. Checklist de Seguridad Físico. Checklist de Seguridad	Revisar el manual del Oficial de Seguridad	Manual de Oficial de Seguridad. Checklist de Seguridad Físico. Checklist de Seguridad	El gerente de seguridad revisa el manual de sus funciones para determinar cómo se deben realizar las evaluaciones que se desarrollaran a continuación.	Gerente de Seguridad

	Lógico.		Lógico.		
3	Checklist de Seguridad Físico. Checklist de Seguridad Lógico.	Checklist coherente	Checklist de Seguridad Físico. Checklist de Seguridad Lógico.	Se analiza si el checklist de seguridad físico o lógico es coherente con el estado del centro de datos.	Gerente de Seguridad
4	Checklist de Seguridad Físico. Checklist de Seguridad Lógico.	Actualizar checklist	Checklist de Seguridad Físico. Checklist de Seguridad Lógico.	En caso no se encuentre actualizado el checklist con las nuevas incidencias o actualizaciones de los diversos estándares usados.	Gerente de Seguridad
5	Checklist de Seguridad Físico. Checklist de Seguridad	Verificar tipo de Seguridad	Checklist de Seguridad Físico. Checklist de Seguridad	Esta actividad sirve para determinar cuál es el tipo de evaluación que se desea realizar según manual.	Gerente de Seguridad

	Lógico.		Lógico.		
6	Checklist de Seguridad Físico.	Evaluar Seguridad Física	Informe de Evaluación	El gerente de seguridad se encarga de llevar a cabo las pruebas con el objetivo de generar el reporte de evaluación.	Gerente de Seguridad
7	Checklist de Seguridad Lógico.	Evaluar Seguridad Lógica	Informe de Evaluación	El gerente de seguridad se encarga de llevar a cabo las pruebas con el objetivo de generar el reporte de evaluación.	Gerente de Seguridad
8	Informe de Evaluación	Generar Informe Físico	Informe de Evaluación	Esta actividad genera el reporte de la evaluación de seguridad a nivel físico.	Gerente de Seguridad
9	Informe de Evaluación	Generar Informe Lógico	Informe de Evaluación	Esta actividad genera el reporte de la evaluación de seguridad a nivel lógico.	Gerente de Seguridad
10	Informe de Evaluación	Consolidar y Enviar informes	Informe de Evaluación	Esta actividad sirve para determinar consolidar todos los documentos necesarios para informar al Gerente de Proyectos y Recursos el estado de la	Gerente de Seguridad

				evaluación.	
11	Informe de Evaluación	Recibir y Reenviar Informe Consolidado	Informe de Evaluación	El Gerente de Proyectos y Recursos recibe el informe consolidado y se lo reenvía al Gerente de la empresa virtual IT-Expert.	Gerente de Proyectos y Recursos
12	Informe de Evaluación	Revisar y brindar VoBo	Informe de Evaluación	El Gerente de la empresa virtual IT-Expert revisa y verifica que el informe sea coherente y se hayan considerados todos los activos del centro de datos.	Gerente IT-Expert
13	Informe de Evaluación Incoherente	Solicitar correcciones	Informe de Evaluación Incoherente	El Gerente IT-Expert solicita la revisión y posible re-evaluación del centro de datos.	Gerente IT-Expert
14	Informe de Evaluación Incoherente	Recibir y Reenviar correcciones	Informe de Evaluación Incoherente	El Gerente de Proyectos y Recursos recibe y reenvía el informe al Gerente de Seguridad para que este vuelva a realizar s u informe.	Gerente de Proyectos y Recursos
15	Informe de Evaluación	Enviar Informe Consolidado	Informe de Evaluación	El Gerente IT-Expert envía el informe al Gerente de las Empresas Virtuales.	Gerente IT-Expert

16	Informe de Evaluación	Revisar Informe	Informe de Evaluación	El Gerente de las empresas virtuales revisa el informe.	Gerente Capstone
17	Informe de Evaluación	Enviar Comentarios	Acciones a tomar	El Gerente de las empresas virtuales envía las acciones a tomar al Gerente IT-Expert.	Gerente Capstone
18	Acciones a tomar	Recepcionar y Enviar Acciones a Tomar	Acciones a tomar	El Gerente IT-Expert recepciona y envía las observaciones y acciones a tomar al Gerente de Proyectos y Recursos.	Gerente IT-Expert
19	Acciones a tomar	Recibir y Reenviar Acciones a tomar	Acciones a tomar	Gerente de Proyectos y Recursos de la empresa IT-Expert recibe y reenviar el documento con las acciones a tomar al Gerente de Seguridad.	Gerente de Proyectos y Recursos.
20	Acciones a tomar	Recibir Acciones a tomar	Acciones tomadas	El Gerente recibe las acciones a tomar y realiza la tarea indicada según el documento.	Gerente de Seguridad

21	Acciones tomadas	Fin	-	Finaliza el proceso con el Gerente de Seguridad luego de haber tomado acabo las acciones mencionadas.	Gerente de Seguridad

Tabla 39: Gestión de Evaluación de Seguridad

Fuente: Elaboración Propia

Diagrama del Proceso

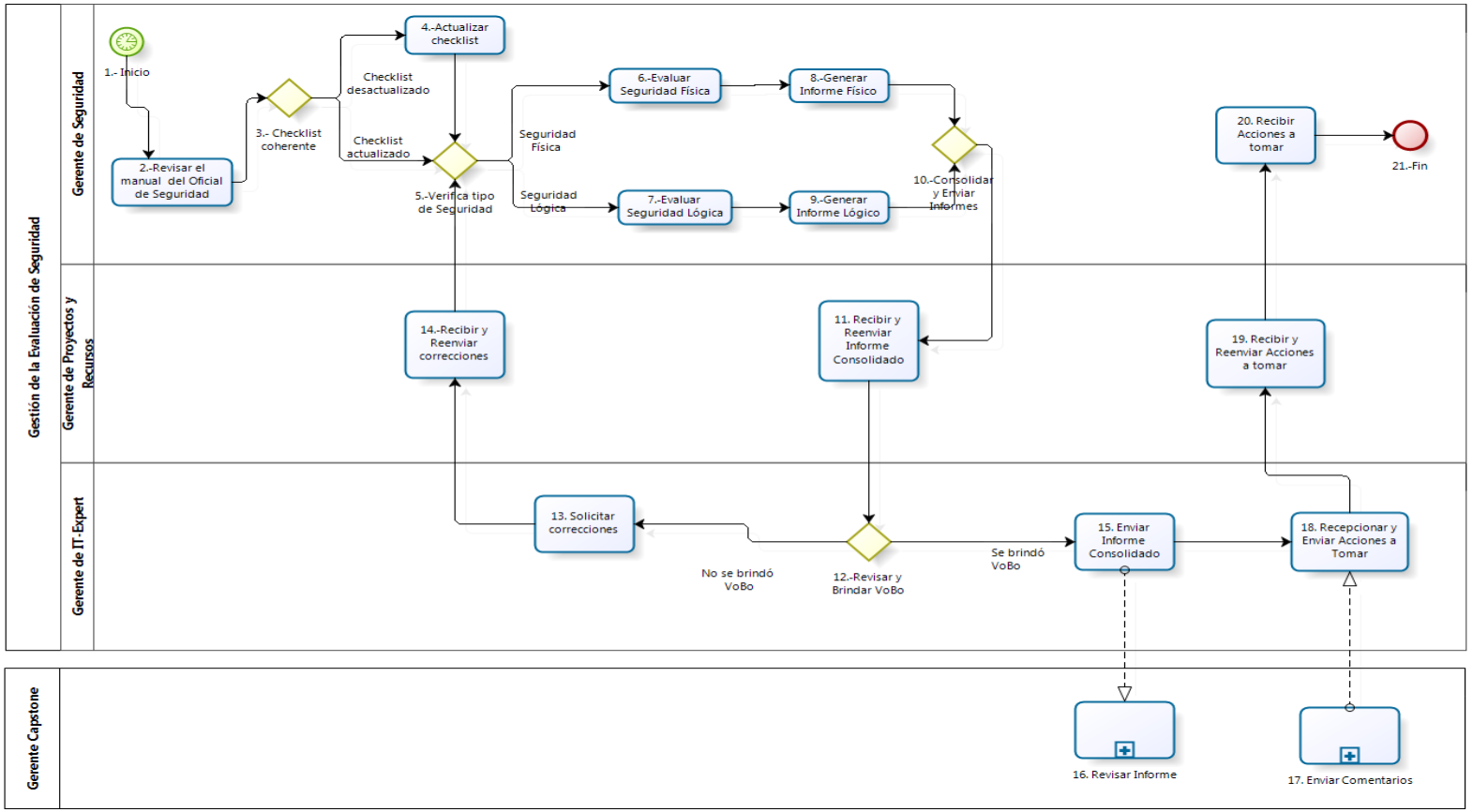


Imagen 12: Gestión de Evaluación de Seguridad

Fuente: Elaboración Propia

Definición de Procesos: Control de ingresos

Propósito del Proceso

El propósito del proceso de Control de Ingresos es controlar las entradas tanto de solicitantes con permisos o sin permisos asegurando la integridad, disponibilidad y confidencialidad. Se basa en las políticas definidas para la gestión de la seguridad física y lógica. Finalmente, este proceso es clave para mantener protegido de daños y robos al centro de datos de la carrera.

Descripción

El proceso de Control de Ingresos se inicia cuando un solicitante sea alumno, operador o visitante requiere ingresar al centro de datos a realizar alguna actividad y genera la solicitud a través de Gerente de Recursos. El gerente de seguridad de turno debe asegurarse que los ingresantes al centro de datos cumplan con ciertos requisitos dependiendo si tienen permisos de ingreso o no, como por ejemplo, presentación de DNI/TIU, presentación de permiso de autorización de ingreso y presentación de permiso de ingreso de dispositivos tecnológicos.

Roles

Roles	Área Funcional	Descripción
Gerente de Seguridad	IT-Expert	Encargado del centro de datos de la carrera. Vela por la seguridad de éste.

Entradas del Proceso

Entrada	Descripción	Encargado de Elaboración
Solicitud de ingreso al Centro de Datos	Nace de la necesidad de ingresar al centro de datos a realizar alguna actividad por lo que el solicitante envía una solicitud que es revisada por el supervisor de turno del centro de datos.	Gerente de Seguridad

Salidas del Proceso

Salida	Descripción	Encargado de Elaboración
Registro de Ingresos	Este documento contiene el detalle de los ingresos al centro de datos por día, hora, nombre, documento de identidad, tipo de ingresante, si contó con permisos de ingreso de dispositivos tecnológicos, el detalle de estos.	Gerente de Seguridad

Caracterización

	Entrada	Actividad	Salida	Descripción	Responsable
1	-	Inicio	Solicitud de ingreso al Centro de Datos	Un recurso de otra empresa solicita ingresar al centro de datos de la carrera.	Gerente de Seguridad
2	Pedido de ingreso al Centro de Datos	Ingresar solicitud de Ingreso	Solicitud de ingreso al Centro de Datos	Los responsables de algún proyecto desarrollado en otra empresa virtual le hacen llegar a su Gerente de Recursos un pedido de ingreso al centro de datos, éste lo valida y genera la solicitud.	Gerente de Recursos
3	Solicitud de ingreso al Centro de Datos	Revisar Solicitud de Ingreso	Solicitud de ingreso al Centro de Datos recibida	El supervisor del Centro de Datos se encarga de Revisarla solicitud.	Gerente de Seguridad
4	Solicitud de ingreso al Centro de Datos recibida	Revisar documentación	Solicitud de ingreso al Centro de Datos revisada	El supervisor revisa la documentación del solicitante.	Gerente de Seguridad

5	Solicitud de ingreso al Centro de Datos revisada	Validar documentación	No contó con la documentación requerida. Contó con la documentación requerida	El supervisor revisar la documentación, asegurándose que esta pertenece efectivamente al solicitante.	Gerente de Seguridad
6	No contó con la documentación requerida.	Cancelación	--	En caso la documentación no era la requerida se da por terminado el proceso.	Gerente de Seguridad
7	Contó con la documentación requerida	Solicitar dispositivos tecnológicos	Dispositivos tecnológicos solicitados	Después de validar la documentación, el supervisor, se encarga de solicitar los dispositivos tecnológicos con los que cuenta el ingresante a fin de evitar que se ingrese cualquier dispositivo no permitido.	Gerente de Seguridad
8	Dispositivos tecnológicos solicitados	Validar permisos de ingreso de dispositivos tecnológicos	No cuenta con permisos. Cuenta con permisos	El supervisor revisa que tengo los permisos para ingresar con los dispositivos tecnológicos.	Gerente de Seguridad

9	No cuenta con permisos.	Guardar dispositivos tecnológicos	Dispositivos tecnológicos confiscados	En caso no cuente con permisos, el solicitante puede ingresar pero sin los dispositivos tecnológicos, por lo que el supervisor se encarga confiscarlos hasta el término de la visita al centro de datos. En esta actividad se podrá verificar el número de dispositivos tecnológicos guardados (confiscados) al centro de datos de forma diaria/semanal/mensual.	Gerente de Seguridad
10	Cuenta con permisos	Registrar dispositivos tecnológicos	Dispositivos tecnológicos registrados	En caso el solicitante cuente con permisos, se encarga de registrar los dispositivos tecnológicos que están permitidos y que se están ingresando al centro de datos. En esta actividad se podrá verificar el número de dispositivos tecnológicos registrados (ingresados) al centro de datos de forma diaria/semanal/mensual.	Gerente de Seguridad
11	Dispositivos tecnológicos registrados Dispositivos tecnológicos confiscados	Ingresar	Dispositivos tecnológicos ingresados	Se permite el ingreso al solicitante, validando si se confiscaron dispositivos o se registraron. En esta actividad se podrá verificar el porcentaje de dispositivos registrados vs confiscados en el centro de datos diariamente/semanalmente/mensualmente.	Gerente de Seguridad

12	Dispositivos tecnológicos ingresados	Registrar ingreso	Registro de Ingresos	El supervisor registra la información del solicitante así como también si se ingresó con o sin dispositivos tecnológicos, registrando también el detalle de estos. En esta actividad se podrá verificar el número de registros realizados (ingresos) al centro de datos de forma diaria/semanal/mensual.	Gerente de Seguridad
14	Registro de Ingresos	Fin	--	El proceso finaliza cuando el solicitante ingresa al centro de datos.	Gerente de Seguridad

Tabla 40: Control de Ingresos

Fuente: Elaboración Propia

Diagrama del Proceso

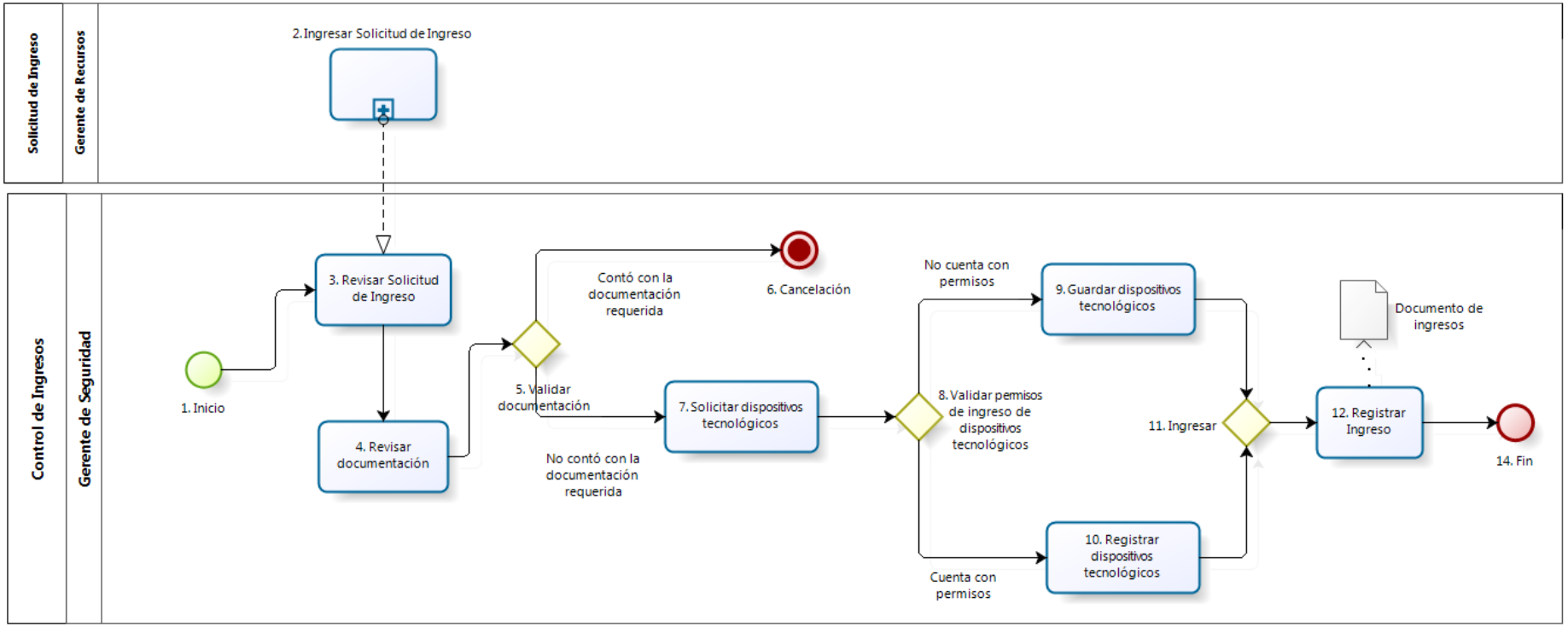


Imagen 13: Control de Ingresos

Fuente: Elaboración Propia

Definición de Procesos: Revisión de Equipos

Propósito del Proceso

El propósito del proceso de Revisión de Equipos es el de monitorear el equipamiento del centro de datos asegurando así la disponibilidad y confidencialidad de la información de los alumnos de la carrera. Se basa en las políticas definidas para la gestión de la seguridad física y lógica. Finalmente, este proceso es clave para mantener siempre equipado y monitoreado de la mejor manera el centro de datos.

Descripción

El proceso de Revisión de Equipos se inicia cuando el supervisor de turno debe realizar según el cronograma la revisión de equipos del centro de datos. Dentro de esta actividad el supervisor verifica si se ha retirado algún equipo sin autorización así como también si se necesita revocar algún equipo del cuál su garantía este por expirar. En caso de pérdida el supervisor debe comunicar al jefe de supervisores este tema siendo el mismo jefe el que verifique revisando reportes generales de revisión de equipos pasados en caso haya habido una equivocación por parte de alguno de los supervisores que realizaron los reportes pasados; si no es así entonces realiza un informe para el área de seguridad de la universidad con el fin de que investiguen sobre el extravío del equipo. Por otro lado, en el caso de una des asignación, el supervisor debe realizar una solicitud al jefe de supervisores para que este de su conformidad respecto del equipo o equipos a ser desafectado o desafectados.

Roles

Roles	Área Funcional	Descripción
Gerente General	IT-Expert	Encargada de monitorear el avance y la presentación de los entregables, además de realizar las coordinaciones necesarias entre el Jefe de Proyecto y el Comité de Proyectos.
Gerente de Proyectos y	IT-Expert	Encargado de supervisar y administrar todos los proyectos de la empresa IT-

Recursos		Expert.
Administrador del Centro de Datos	IT-Expert	Encargado de turno del centro de datos.
Gerente de Seguridad	IT-Expert	Encargado de gestionar y supervisar todo lo relacionado a Seguridad tanto dentro como fuera del Centro de Cómputo.

Entradas del Proceso

Entrada	Descripción	Encargado de Elaboración
Cronograma de revisiones de equipos.	Contiene las fechas en la cual están programadas las revisiones de equipos.	Gerente de Seguridad

Salidas del Proceso

Salida	Descripción	Encargado de Elaboración
Reporte general de revisión de equipos	Este documento muestra el reporte de todas las incidencias ocurridas durante la actividad de revisión de equipos.	Administrador del Centro de Datos

Caracterización

	Entrada	Actividad	Salida	Descripción	Responsable
1	--	Inicio	Realización de revisión según cronograma	Inicia el proceso al inicio del ciclo académico.	Gerente de Seguridad
2	Realización de revisión	Revisar equipos	Resultado de revisión de equipos	El supervisor se encarga de realizar la revisión de los equipos del centro de datos al inicio del ciclo académico.	Gerente de Seguridad
3	Resultado de revisión de equipos	Validar retiro de equipo sin aviso	*Si, se retiró. *No se retiró.	El supervisor revisa si se retiró algún equipo o no sin ningún aviso.	Gerente de Seguridad
4	Sí, se retiró	Comunicar pérdida de equipo	Mensaje de pérdida	El supervisor comunica al jefe de supervisores sobre la pérdida del equipo(s). En esta actividad se podrá identificar el número de equipos perdidos en el ciclo académico.	Gerente de Seguridad
5	Mensaje de pérdida	Revisar reporte de retiro de equipos	Reporte revisado completamente	El jefe de supervisores revisa de manera detallada los reportes pasados sobre retiros de los equipos a fin de comprobar si el	Administrador del Centro de

				equipo fue retirado sin ningún aviso.	Datos
6	Reporte revisado completamente	Elaborar informe de seguridad	Informe de seguridad	El jefe de supervisores elabora un informe para el área de seguridad de la universidad comunicando la pérdida del equipo y de ese modo se inicien las investigaciones del caso.	Administrador del Centro de Datos
7	Informe de seguridad	Término	--	El jefe de supervisores envía el informe para que el área de seguridad de la universidad se encargue del asunto.	Administrador del Centro de Datos
8	No se retiró	Revocar o cambiar algún equipo	Si es necesario. No es necesario.	El supervisor luego de verificar que no se realizaron retiros sin aviso valida si es necesario realizar alguna reasignación o cambio a algún equipo del centro de datos.	Gerente de Seguridad
9	Si es necesario	Elaborar solicitud de revocación de equipos	Solicitud de revocación de equipos	El supervisor elabora una solicitud de revocación de equipos para que este sea revisado y sea dado por conforme por el jefe de supervisores.	Gerente de Seguridad

10	Solicitud de revocación de equipos	Enviar Solicitud de revocación de equipos	Envío realizado	El supervisor envía la Solicitud de revocación de equipos elaborada.	Gerente de Seguridad
11	Envío completado	Revisar solicitudes para conformidad	Solicitud atendida	El jefe de supervisores revisa y atiende la solicitud.	Administrador del Centro de Datos
12	Solicitud atendida	Validar conformidad	*Si se brindó conformidad. *No se brindó conformidad.	El jefe de supervisores valida si se brindó o no se brindó la conformidad de la solicitud.	Administrador del Centro de Datos
13	* No se brindó conformidad *No es necesario.	Validar disconformidad / revocación	Fue con disconformidad / sin revocación.	El supervisor verifica si se procederá a realizar el reporte dependiendo si no necesito de una revocación o se le fue negada una revocación.	Gerente de Seguridad
14	Si se brindó.	Enviar conformidad de solicitud	Envío de conformidad realizado.	El jefe de supervisores envía la conformidad de la Solicitud de revocación de equipos.	Administrador del Centro de Datos

15	Envío de conformidad realizado.	Enviar simultáneamente	Envío simultáneo realizado	El jefe de supervisores envía la conformidad de la Solicitud de revocación de equipos.	Administrador del Centro de Datos
16	Envío simultáneo realizado	Revisar de conformidad de solicitud de revocación	Solicitud de revocación de equipos revisada	El Gerente General de IT-Expert recibe y revisa la solicitud.	Gerente General
17	Solicitud de revocación de equipos revisada	Comunicar revocación	Comunicación realizada	El Gerente General de IT-Expert se comunica con el gerente de proyectos y recursos.	Gerente General
18	*Comunicación realizada. *No es conforme.	Atender solicitud	Solicitud atendida	El Gerente atiende la solicitud.	Gerente de Proyectos y Recursos.
19	Solicitud atendida	Realizar documento de requerimiento para la revocación de equipo	Documento de requerimientos	El Gerente realiza el documento dependiendo de los requerimientos que esta revocación requiera.	Gerente de Proyectos y Recursos.

20	Documento de requerimientos	Enviar documento de requerimientos	Envío de documento de requerimientos realizado	El gerente envía el documento a ser validado por el gerente general de IT-Expert.	Gerente de Proyectos y Recursos.
21	Envío de documento de requerimientos realizado	Revisar documento de requerimientos	Revisión completada	El Gerente General de IT-Expert revisa el documento de requerimientos elaborado por el gerente de proyectos y recursos.	Gerente General
22	Revisión completada	Validar documento	*Si es conforme. *No es conforme.	El gerente general valida si el documento es conforme o no.	Gerente General
23	Si es conforme	Enviar conformidad de documento de requerimientos	Envío de documento de requerimientos realizado	El gerente general envía el documento con su conformidad.	Gerente General
24	Envío de documento de requerimientos realizado	Revisar conformidad de documento de requerimientos	Recepción y revisión de conformidad de documento de requerimientos completada	El supervisor recibe y revisa el documento.	Gerente de Seguridad

25	*Registro de equipos revocados *Recepción y revisión de conformidad de documento de requerimientos completada	Verificar	Verificación completada	El supervisor verifica que tenga ambos documentos para proceder a realizar	Gerente de Seguridad
26	Verificación completada	Realizar tareas en base a requerimientos	Equipo revocado realizando tareas	El supervisor realiza la revocación en base a los requerimientos.	Gerente de Seguridad
27	*Equipo revocado realizando tareas. *Fue con disconformidad / sin revocación.	Validar tareas previas	Con / sin tareas previas.	El supervisor verifica la información de la revisión de equipos previo a hacer el reporte general de la revisión de equipos.	Gerente de Seguridad
28	Con / sin tareas previas.	Realizar reporte general de la revisión de equipos	Reporte General de la Revisión de Equipos	El supervisor realizar el reporte de la revisión programada. Esta actividad permitirá identificar el número de equipos sin problemas en el ciclo académico así también permitirá calcular el porcentaje de equipos con problemas vs equipos sin problemas al inicio del ciclo.	Gerente de Seguridad

29	Reporte General de la Revisión de Equipos	Enviar reporte general de la revisión de los equipos	Envío del reporte general de la revisión de los equipos	El supervisor envía el reporte al Jefe de supervisores.	Gerente de Seguridad
30	Envío del reporte general de la revisión de los equipos	Revisar el reporte general de la revisión de los equipos	Reporte General de la Revisión de Equipos revisado	El jefe de supervisores procede a revisar el reporte para luego archivarlo.	Administrador del Centro de Datos
31	No se brindó.	Enviar disconformidad de solicitud	Disconformidad enviada	El jefe de supervisores envía la disconformidad al supervisor	Gerente de Seguridad
32	Disconformidad enviada	Revisar disconformidad de solicitud	Disconformidad recibida, no se brindó.	El supervisor recibe la disconformidad	Gerente de Seguridad
33	Envío simultáneo realizado	Revisar conformidad de solicitud de revocación	Conformidad recibida	El supervisor recibe la conformidad.	Gerente de Seguridad
34	Conformidad recibida	Registrar equipo(s) a	Registro de equipos	El supervisor elabora un documento que a futuro le ayudará en el reporte general de la	Gerente de

		ser revocado(s)	revocados	revisión de equipos. Esta actividad permitirá identificar el número de equipos revocados en el ciclo académico.	Seguridad
35	Registro de equipos revocados	Enviar en Simultáneo	Registro de equipos revocados	El Gerente de Seguridad envía el registro de equipos revocados al Gerente Capstone a modo informativo a su vez que pasa a verificar.	Gerente de Seguridad
36	Registro de equipos revocados	Recibir Registro de Equipos a ser revocados	--	El Gerente Capstone recibe el listado de los equipos que serán revocados del centro de datos a modo informativo.	Gerente Capstone
37	Registro de equipos revocados	Fin	--	El proceso se da por concluido el gerente de seguridad revisa el reporte general de la revisión de equipos	Administrador del Centro de Datos

Tabla 41: Revisión de Equipos

Fuente: Elaboración Propia

Diagrama del Proceso

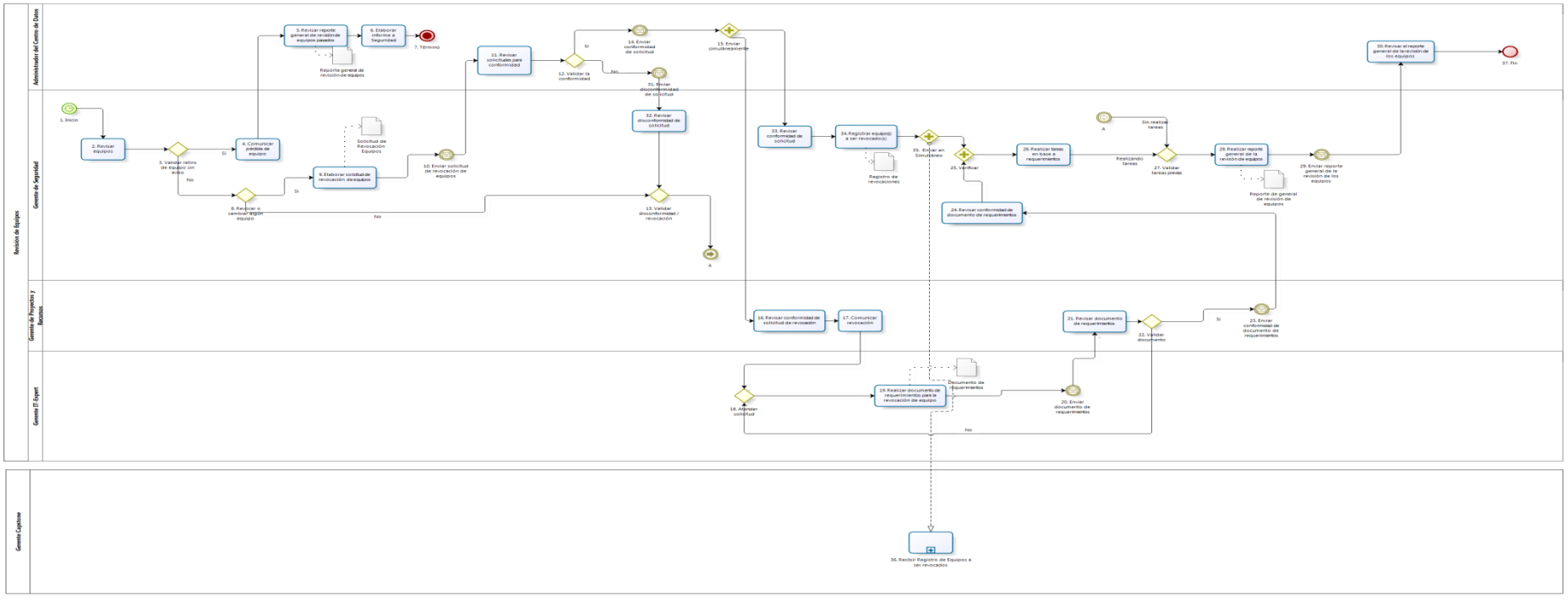


Imagen 14: Revisión de Equipos

Fuente: Elaboración Propia

Definición de Procesos: Control de Protección Ambiental

Propósito del Proceso

El propósito del proceso de Control de Protección Ambiental es monitorear y controlar las operaciones de inspección respecto a la protección ambiental del centro de datos. Dentro de estas están los suministros de energía, la protección de instalaciones y en menor grado el cableado.

Descripción

El proceso de Control de Protección Ambiental se inicia cuando el gerente de seguridad después de revisar su cronograma envía la solicitud a un operador de servicios generales para que este inspeccione los suministros de energía que corresponden al edificio donde se encuentra ubicado el centro de datos. Este una vez que realiza la inspección envía al gerente de seguridad un reporte con los resultados de ésta en la cual también incluye observaciones y/o incidencias. Luego de recibir dicho reporte el gerente de seguridad procede a enviar una solicitud al supervisor de turno del centro de datos para que este realice un reporte respecto a cómo ha estado protegida las instalaciones del centro de datos especificándose si se registró alguna incidencia desde el último reporte realizado. El supervisor envía el reporte al gerente de seguridad. Éste analiza ambos reportes recibidos y realiza su reporte de incidencias el cual es un resumen de ambos reportes. Este reporte es enviado al director de la carrera de Ingeniería de Sistemas de Información el cuál después de revisarlo analiza los resultados y envía al gerente de seguridad un documento donde especifica las observaciones y/o requerimientos que hay que realizar para poder mejorar tanto el suministro de energía como la protección de las instalaciones.

Roles

Roles	Área Funcional	Descripción
Gerente de Seguridad	IT-Expert	Encargado de gestionar y supervisar todo lo relacionado a Seguridad en el Centro de Cómputo.

Administrador del Centro de Datos	IT-Expert	Encargado de turno del centro de datos.
Operador	IT-Expert	Es el encargado de realizar los mantenimientos.
Director de la Carrera	Facultad de Ingeniería	Es el encargado de velar por el bien educativo de la carrera de ingeniería de sistemas.

Entradas del Proceso

Entrada	Descripción	Encargado de Elaboración
Necesidad de inspeccionar los suministros de energía	La realización de esta inspección es importante debido a que ayuda a controlar y monitorear la protección ambiental del centro de datos.	Gerente de seguridad

Salidas del Proceso

Salida	Descripción	Encargado de Elaboración
Documento de requerimientos y/o observaciones revisado	Este documento que fue elaborado por el director de la carrera contiene las observaciones y/o requerimientos que se necesitan para mejorar la protección ambiental del centro de datos.	Director de la Carrera de Ingeniería de Sistemas de información

Caracterización

	Entrada	Actividad	Salida	Descripción	Responsable
1	--	Inicio	Cronograma de la inspección de suministros de energía	El gerente de seguridad, al inicio del ciclo académico debe revisar su cronograma de actividades.	Gerente de Seguridad
2	Cronograma de la inspección de suministros de energía	Redactar solicitud de inspección de suministros de energía	Solicitud de Inspección de Suministros de Energía	El Gerente de Seguridad se encarga de realizar una solicitud a los operadores de servicios generales para que estos realicen las tareas de revisión de los suministros de energía y revisión de cableado respecto al centro de datos. Esta actividad se realiza cada mes.	Gerente de Seguridad
3	Solicitud de Inspección de Suministros de Energía	Enviar solicitud de inspección de suministros de energía	Solicitud de Inspección de Suministros de Energía enviado	El gerente de seguridad envía la solicitud al operador para que este pueda realizar la inspección.	Gerente de Seguridad
4	Solicitud de Inspección de Suministros de	Inspeccionar suministros de	Reporte de Inspección de	El operador envía un reporte de inspección de suministros al gerente de seguridad.	Operador

	Energía enviado	energía	Suministros		
5	Reporte de Inspección de Suministros	Revisar Reporte de Inspección de Suministros	Revisión de Reporte de Inspección de Suministros realizado	El gerente de seguridad revisa el reporte y saca conclusiones respecto a esto	Gerente de Seguridad
6	Revisión de Reporte de Inspección de Suministros realizado	Redactar solicitud de reporte de Protección de Instalaciones	Solicitud de Reporte de Protección de Instalaciones	El gerente de seguridad luego de revisar el reporte de suministros de energía pasa a redactar la solicitud de protección de instalaciones que será enviado al supervisor de turno.	Gerente de Seguridad
7	Solicitud de Reporte de Protección de Instalaciones	Enviar solicitud de reporte de protección de instalaciones	Solicitud de Reporte de Protección de Instalaciones enviado	El gerente de seguridad envía la Solicitud de Reporte de Protección de Instalaciones al supervisor de turno.	Gerente de Seguridad
8	Solicitud de	Revisar Solicitud	Solicitud de	El supervisor recibe la solicitud de reporte de protección	Administrador

	Reporte de Protección de Instalaciones enviado	de reporte de Protección de Instalaciones	Reporte de Protección de Instalaciones revisado	de instalaciones.	del Centro de Datos
9	Solicitud de Reporte de Protección de Instalaciones revisado	Elaborar Reporte de Protección de Instalaciones	Reporte de Protección de Instalaciones	El supervisor realiza el reporte respecto al resultado de la actividad realizada	Administrador del Centro de Datos
10	Reporte de Protección de Instalaciones	Enviar Reporte de Protección de Instalaciones	Reporte de Protección de Instalaciones enviado	El supervisor envía el Reporte de Protección de Instalaciones al gerente de seguridad	Administrador del Centro de Datos
11	Reporte de Protección de Instalaciones	Revisar Reporte de Protección de Instalaciones	Reporte de Protección de Instalaciones revisado	El gerente de seguridad procede a revisar el reporte enviado por el supervisor.	Gerente de Seguridad

12	Reporte de Protección de Instalaciones revisado	Realizar Reporte de Incidencias	Reporte de Incidencias	El gerente de seguridad realiza el reporte de incidencias. En esta actividad se podrá verificar el número de incidencias reportadas en cada ciclo académico en los suministros de energía del centro de datos.	Gerente de Seguridad
13	Reporte de Incidencias	Enviar	Reporte de Incidencias enviado	El gerente de seguridad envía el reporte de incidencias al director de carrera de sistemas.	Gerente de Seguridad
14	Reporte de Incidencias por enviar a Director	Enviar Reporte de Incidencias a Director	Reporte de Incidencias	El gerente de seguridad envía el reporte de incidencias al director de la carrera quien es el encargado del centro de datos	Gerente de Seguridad
15	Reporte de Incidencias	Revisar y redactar documentación	Reporte de Incidencias revisado	El director de la carrera revisa el reporte enviado por el gerente de seguridad y elabora el documento de requerimientos y/o observaciones.	Director de la Carrera
16	*Reporte de Incidencias * Reporte de Incidencias	Revisar	Reporte de Incidencias	El gerente de seguridad recibe el reporte de incidencias revisado por el Director de la Carrera de ingeniería de Sistemas de Información.	Gerente de Seguridad

	revisado				
17	Documento de requerimientos y/o observaciones	Revisión de documento de requerimientos y/o observaciones	Documento de requerimientos y/o observaciones revisado	El gerente de seguridad revisa el documento y toma las medidas para realizar los cambios u observaciones mencionadas	Gerente de Seguridad
18	Documento de requerimientos y/o observaciones revisado	Fin	--	El proceso finaliza cuando el gerente de seguridad revisa el documento de requerimientos y/o observaciones.	Gerente de Seguridad

Tabla 42: Control de Protección Ambiental

Fuente: Elaboración Propia

Diagrama del Proceso

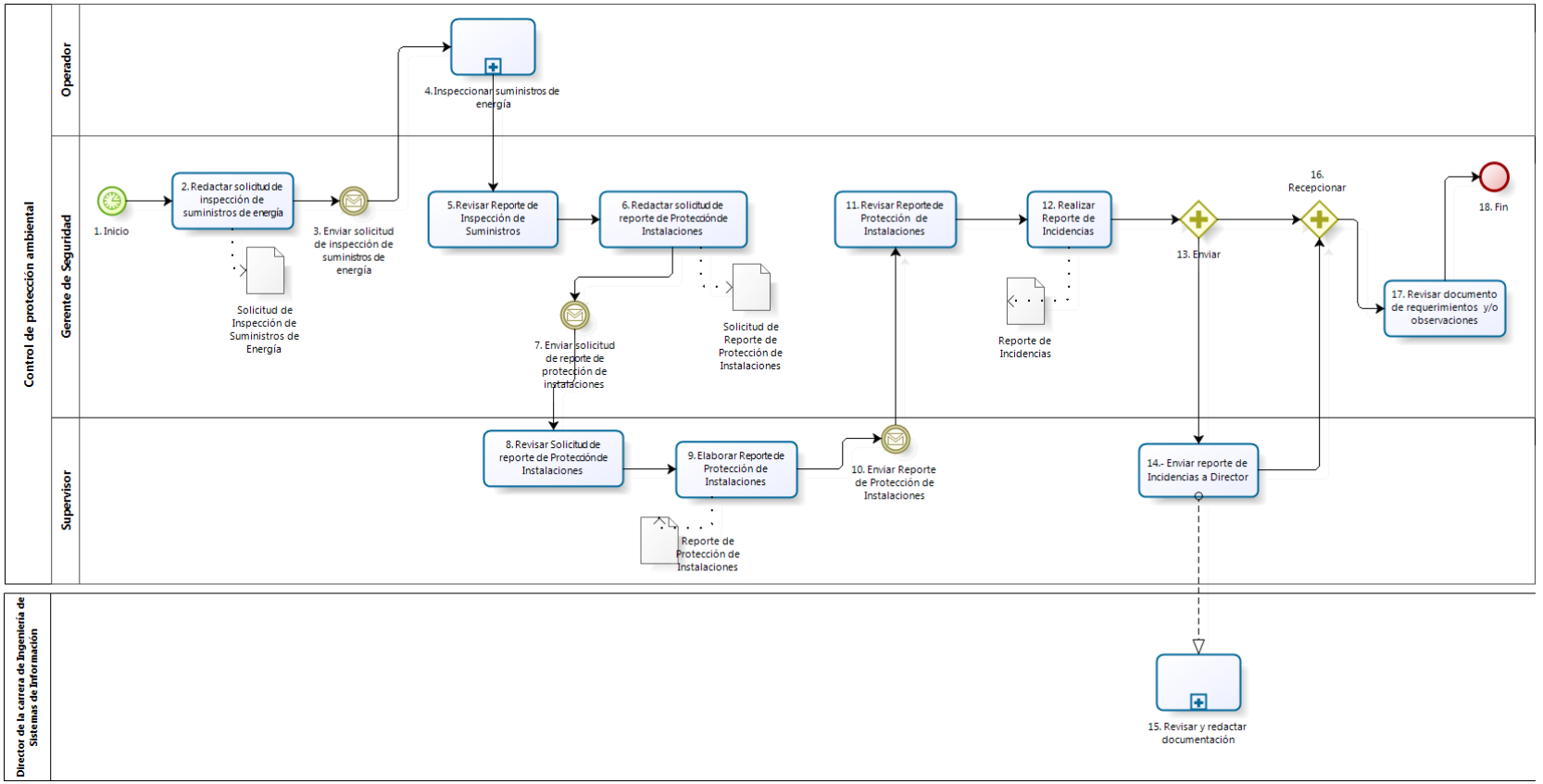


Imagen 15: Control de protección ambiental

Fuente: Elaboración Propia

Definición de Procesos: Gestión de solicitud de accesos

Propósito del Proceso

El propósito del proceso de Gestión de Solicitud de Accesos es definir cuál es la secuencia de actividades a seguir y el flujo adecuado para solicitar acceso físico al centro de datos de la carrera de Ingeniería de Sistemas y Software. Este proceso guarda estrecha relación con las políticas definidas para la gestión de la seguridad física y lógica. Al mismo tiempo, este proceso es clave para el inicio las actividades de pase a producción y despliegue dentro del centro datos.

Descripción

El proceso de Gestión de Solicitud de Accesos se inicia cuando el Gerente de Proyectos y Recursos IT-Expert de la empresa IT-Expert solicita a cada gerente de recursos de las empresas virtuales la relación de alumnos que deben contar con acceso al centro de datos por pertenecer a los cursos de Taller de Desempeño 1, Taller de Desempeño 2, Taller de Proyectos 1 y Taller de Proyectos 2. Luego, esta lista debe ser revisada por el Gerente Proyecto y Recursos, el mismo que visa la relación y solicita su atención por parte del Gerente de Seguridad de IT-Expert. Posterior a ello, el Gerente de Seguridad de IT-Expert procede a revisar la lista, tramita y notifica los cambios.

Roles

Roles	Descripción
Gerente de Proyectos y Recursos.	Es la persona encargada de administrar de los servidores del centro de cómputo, realizar seguimiento a los proyectos de la empresa y atender solicitudes de servicios de TI de las empresas virtuales.
Gerente de Seguridad	Encargado de gestionar y supervisar todo lo relacionado a Seguridad dentro del Centro de Cómputo.

Entradas del Proceso

Entrada	Descripción	Encargado de Elaboración
Listado de recursos por empresa.	Este documento contiene la lista de alumnos con las que contará la empresa virtual a lo largo del ciclo.	Gerencia de Proyectos y Recursos de IT-Expert

Salidas del Proceso

Salida	Descripción	Encargado de Elaboración
Listado de alumnos con accesos	Este documento consiste en tener el listado de alumnos que cuentan con acceso físico al centro de datos, el mismo que se genera a partir de un Excel.	Gerente del Seguridad

Caracterización

	Entrada	Actividad	Salida	Descripción	Responsable
1	-	Inicio	Solicitud de alumnos por empresa virtual	El proceso inicia cuando el gerente de proyectos y recursos de la empresa IT- Expert solicita al resto de empresas virtuales la relación de alumnos a los cuales se les debe tramitar el acceso al centro de datos.	Gerente de Proyectos y Recursos.
2	Solicitud de alumnos por empresa virtual	Generar lista de Alumnos Matriculados	Listado de alumnos por empresa.	El gerente de recursos de cada uno de las empresas virtuales que forman parte de taller de desempeño 1 y 2, y taller de proyecto 1 y 2 crea la lista de alumnos que forman parte de su empresa.	Gerente de Recursos.
3	Listado de alumnos por empresa.	Crear relación de alumnos	Listado de alumnos a dar acceso.	Se prepara el documento que contendrá la relación de alumnos de cada empresa virtual que contarán con acceso físico al centro de datos. Los datos que debe tener este listado es: Código de Alumno, Nombre del Alumno, Empresa, Proyecto.	Gerente de Proyectos y Recursos.
4	Listado de alumnos a	¿Es conforme?	Listado de alumnos a dar	En esta actividad se verifica/analiza si se necesita una revisión de la lista de alumnos por parte del gerente de recursos de cada empresa	Gerente de Proyectos y

	dar acceso.		acceso. Listado de alumnos a dar acceso a revalidar.	virtual. En caso sea necesaria una validación por parte del gerente de recursos de cada empresa se envía un correo con la lista y las observaciones encontradas. En caso no se requiera una verificación adicional se procede a visar la relación y asignar.	Recursos.
5	Listado de alumnos a dar acceso.	Visar y asignar para atención	Solicitud de Atención Lista de alumnos visada.	El gerente de proyectos y recursos de IT-Expert se encarga de revisar que el listado de alumnos contenga todos los datos mencionados en el punto A y que cuente con la conformidad del gerente general de la empresa solicitante.	Gerente de Proyectos y Recursos.
6	Listado de alumnos a dar acceso a revalidar.	Reformular relación de alumnos	Listado de alumnos a dar acceso a revalidar.	El gerente de proyectos y recursos de IT-Expert puede solicitar la revisión de la lista porque esta no cumple con los requisitos mínimos indispensables, mediante un mensaje se envía la relación al gerente de recursos de la empresa virtual correspondiente para su revisión.	Gerente de Proyectos y Recursos.
7	Listado de alumnos a dar acceso a	¿Es conforme?	Listado de alumnos a dar acceso a	El gerente de seguridad, verifica que la relación enviada sea revalidada o visada cumpla con todos los requisitos necesarios antes	Gerente de Seguridad

	revalidar. Solicitud de Atención Lista de alumnos visada.		revalidar. Lista de alumnos visada.	de tramitar los accesos.	
8	Listado de alumnos visado.	Tramitar accesos	Relación de alumnos con accesos.	El responsable de brindar accesos tramita los accesos físicos para los alumnos que figuran en el listado, esta labor consiste en actualizar la información en la base de datos GSFL en la tabla SOL_ACC ingresando todos los datos mencionados en el punto A, para que de esta forma esta información sea explotada desde un Excel con programación VBA.	Gerente del Seguridad
9	Listado de alumnos a dar acceso a revalidar.	Solicitar revisión de lista de alumnos.	Listado de alumnos a dar acceso a revalidar. Reporte de	El gerente de seguridad de IT-Expert puede solicitar la revisión de la lista al gerente de proyectos y recursos porque esta no está acorde a las especificaciones o algún requerimiento mínimo ha sido obviado. Esta revisión se puede dar hasta en tres oportunidades, si se produce	Gerente de Seguridad

			cancelación por iteraciones.	por cuarta vez el proceso se finaliza y se genera el reporte de cancelación por iteraciones.	
10	Relación de alumnos con accesos.	Generar reporte de Accesos.	Reporte de alumnos con acceso.	El gerente de seguridad genera un reporte para en el cual se lista a las personas que cuentan con acceso al centro de datos.	Gerente del Seguridad
11	Reporte de alumnos con acceso. Reporte de cancelación por iteraciones.	Fin	Correo de Notificación	El gerente de seguridad envía un correo informativo en el cual se indica que se han brindado los accesos respectivos, este correo tiene como destinatario al Gerente de Proyecto y Recursos de IT-Expert y a los alumnos involucrados.	Gerente de Seguridad

Tabla 43: Gestión de Solicitud de Accesos

Fuente: Elaboración Propia

Diagrama del Proceso

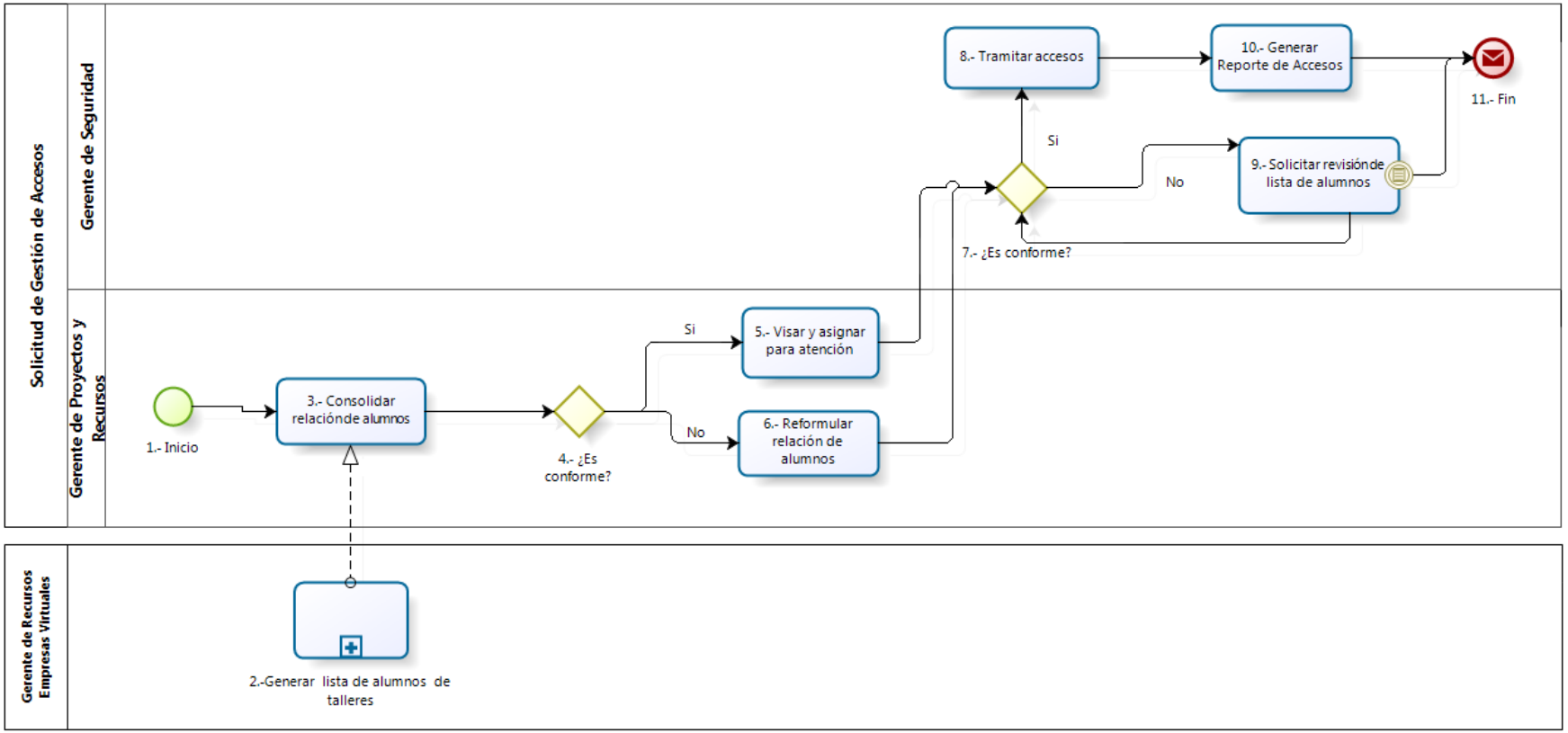


Imagen 16: Gestión de Solicitud de Accesos

Fuente: Elaboración Propia

Política de Seguridad Física

Introducción

La seguridad física brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones del centro de datos de la carrera de Ingeniería de Sistemas de Información, al mismo tiempo previene evitar al máximo el riesgo de accesos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen tres conceptos a tener en cuenta: la protección física de accesos, la protección ambiental y el transporte, protección y mantenimiento de equipamiento y documentación; los cuáles se tocarán de manera detallada en la sección de Conceptos y aspectos específicos sobre la Política de Seguridad Física.

Alcance

Esta política aplicará a todo el personal vinculado laboralmente y educativamente con la UPC así también terceros que tengan acceso a los recursos de información del centro de datos de la carrera.

Acrónimos y definiciones

UPS – Sistema de alimentación ininterrumpida (Uninterruptible Power Supply).

TIA – Asociación de la Industria de Telecomunicaciones (Telecomunications Industry Asociation).

Centro de Datos – Centro de datos carrera de Ingeniería de Sistemas en la Universidad Peruana de Ciencias Aplicadas.

Objetivos

Objetivo General

- Brindar las bases para prevenir, asegurar, controlar, monitorear, mantener y supervisar los diversos factores que puedan afectar la disponibilidad del centro de datos de la carrera.

Objetivos Específicos

- Prevenir e impedir el acceso físico no autorizado, además de evitar interrupciones a las actividades educativas, daños o robos de los activos del centro de datos de la carrera.

- Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del centro de datos de la carrera.

- Proteger los equipos del centro de datos en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

Enunciado de la Política

"Los equipos informáticos y áreas aledañas al centro de datos de la carrera, deben cumplir con todas las políticas funcionales y procedimientos de seguridad física, con el fin de evitar el acceso por personas no autorizadas, daño e interferencia a los recursos e infraestructura de información."

Responsabilidades

Es responsabilidad del director de la carrera de Ingeniería de Sistemas de Información e Ingeniería de Software la aprobación de esta política.

Violaciones a la política

En caso se viole la Política de Seguridad Física se dispone de aplicar las siguientes sanciones:

- Suspensión o acceso restringido al centro de datos.

- Reembolso por algún daño causado.

- Suspensión sin pago de salario.

- Demanda civil o penal.

Estas sanciones se encuentran en el Reglamento de Disciplina de la Universidad Peruana de Ciencias Aplicadas.

Conceptos y directrices sobre la Política de Seguridad Física

Protección Física de Accesos

Se debe controlar y proteger tanto dentro de las instalaciones como al momento de acceder los equipos y la información del centro de datos, englobando dos aspectos específicos como son: el control de acceso físico y el desarrollo de las tareas dentro del centro de datos.

Controles de Acceso Físico

El centro de datos debe ser protegido mediante controles de acceso físico a fin de permitir el acceso sólo al personal autorizado. Estos controles deben ser aplicados por el supervisor de turno del centro de datos para así, proteger al centro de datos de accesos no autorizados por lo que soporta el concepto de protección física de accesos.

Recomendaciones y controles adicionales:

Inspeccionar y supervisar a los alumnos y/o visitantes del centro de datos registrando código, nombres, actividad a realizar, fecha y horario del ingreso y egreso. Para esto se necesitará la creación de una base de datos. El mantenimiento de esta base de datos estará a cargo del DBA de la empresa virtual IT-Expert el cual a su vez se encargará de realizar el reporte de esta información dependiendo de lo que requiera del jefe de supervisores del centro de datos. Por otro lado, el supervisor de turno del centro de datos debe velar por que se cumplan los requerimientos de seguridad del centro de datos a las personas que estén ingresando.

Limitar y controlar el acceso al centro de datos a las personas autorizadas, las cuales deberán contar con un código de identificación. El ingreso del personal también debe ser registrado. Estos registros deben ser almacenados en una base de datos.

Revisar y actualizar cada mes los registros de accesos al centro de datos los cuales deben ser documentados y firmados por el encargado principal del centro de datos.

Revisar los registros almacenados en la base de datos sobre los ingresos y egresos hacia el centro de datos de la carrera. Esta actividad debe ser realizada por el DBA de la empresa IT-Expert.

Clasificar en categorías los diferentes tipos de personal que podrán tener acceso al centro de datos, dentro de los cuales deben estar: operadores y usuarios (trabajo regular), mantenimiento y retiro (trabajo periódico) y visitantes (alumnos o terceros) que necesiten utilizar los equipos y la información del centro de datos de manera temporal.

Desarrollo de Tareas en el Centro de datos

Para incrementar la seguridad del centro de datos, se debe establecer controles y lineamientos para el personal que trabaja en él, así como para las actividades de terceros y alumnos que se den dentro de este. Estos lineamientos y controles tienen que estar ligadas específicamente con la protección física de accesos y permisos.

Recomendaciones y controles adicionales:

Dar a conocer al personal la existencia del centro de datos y las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.

El supervisor de turno debe estar al tanto de todo trabajo o actividad llevada a cabo por alumnos y/o terceros.

El supervisor de turno debe mantener cerrado el ingreso e inspeccionar el centro de datos cada intervalo de tiempo cuando este se encuentre desocupado.

El supervisor debe limitar el acceso al centro de datos de alumnos y/o terceros que no se encuentren autorizados, en caso estos cuenten con una autorización, deben ser monitoreados.

El supervisor de turno debe guardar un registro de todos los alumnos y/o terceros con autorización de acceso al centro de datos.

Impedir el ingreso al centro de datos con equipos que registren información visual o auditiva a menos que estos hayan sido debidamente autorizados por el director de la carrera de Ingeniería de Software y Sistemas. Así también prohibir fumar y consumir alimentos y/o bebidas dentro de las instalaciones del centro de datos.

Protección ambiental

Asegura y controla que las instalaciones estén protegidas, que el suministro de energía sea ininterrumpido, el perímetro del centro de datos cuente con las señalizaciones, barreras físicas, mecanismos de control y ubicación correctos.

Perímetro de Seguridad Física

El lugar en el cual el centro de datos de la carrera se encuentra instalado debe estar protegido por diversas barreras y controles físicos a fin de proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado. Este aspecto forma parte del concepto de la protección ambiental que debe ser cubierto por la seguridad física.

Recomendaciones y controles adicionales:

Establecer y documentar claramente el perímetro de seguridad.

Ubicar las instalaciones del centro de datos dentro del perímetro de un edificio o área de construcción físicamente sólida. Las paredes deben ser sólidas y las puertas deben estar protegidas contra accesos no autorizados mediante alarmas, cerraduras y mecanismos de control. En el caso del mecanismo de control, se sugiere implementar un área de recepción atendida por personal, permitiendo el acceso al centro de datos exclusivamente al personal autorizado, registrando cada ingreso y egreso en forma precisa.

Expandir las barreras físicas necesarias (2.7m), desde el piso real hasta el techo real, a fin de crear un espacio ideal para los equipos así como también impedir incendios, humedad e inundación (contaminación ambiental).

Tener identificados claramente todas las puertas de emergencia/incendio de un perímetro de seguridad.

Designar a un responsable de seguridad que se encargue de llevar los registros de los principales equipos a proteger y sus medidas de protección física.

Suministros de energía

Los equipos deben estar protegidos a posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía debe estar de acuerdo con las especificaciones del fabricante o proveedor de cada equipo.

Recomendaciones y controles adicionales:
Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.

Contar con varias líneas de alimentación de energía así también contar con múltiples enchufes para evitar fallas en el suministro de energía en caso de contar sólo con un único punto.

Contar con un UPS para asegurar la continuidad de la disponibilidad de los equipos que sustentan las operaciones críticas del centro de datos así también como de proteger de fallos de suministro. Estos sistemas de alimentación ininterrumpida deben ser implementados de preferencia en los equipos de operaciones críticas, los cuales deben ser determinados por los encargados así también como por los alumnos propietarios de la información. Estos equipos UPS deben ser probados mensualmente para asegurar el correcto funcionamiento de estos.

Ubicar los interruptores de emergencia cerca a las salida(s) del centro de datos con la finalidad de facilitar un corte de energía rápido ante un caso crítico.

Proveer de iluminación de emergencia así también como protección contra descargas eléctricas en el centro de datos y alrededores en caso de producirse una falla en el suministro de energía.

Instalar un generador de respaldo en caso que el generador principal sufra algún desperfecto asegurando que el tiempo de funcionamiento de la UPS permita el encendido manual del mismo. Ambos generadores deben ser inspeccionados y probados mensualmente para asegurar que funcionen correctamente.

Seguridad del cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño,

asegurando que la disponibilidad del centro de datos no se vea afectado de manera crítica.

Recomendaciones y controles adicionales:
Evitar que el cableado de red atraviese vías públicas a fin de protegerlo de daños e interceptaciones.

Tener separados los cables de comunicaciones con los cables de energía a fin de evitar interferencias.

Tener los cables de energía conectadas a tierra.

Proteger el cableado de comunicaciones (red) mediante canaletas.

Utilizar medios de transmisión alternativos.

Protección de las Instalaciones

La selección y el diseño del área del centro de datos debe tener en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre, brindando un protección ambiental dentro del centro de datos.

Recomendaciones y controles adicionales:
Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.

Controlar que las puertas y ventanas del centro de datos permanezcan cerradas en caso de no contar con personal en las instalaciones, asegurando con una protección especial en las ventanas.

Separar las áreas principales del centro de datos a ser atendidas por el personal de aquellos que serán atendidos por terceros.

Almacenar los materiales peligrosos en lugares seguros a distancia, como estantes o aranceles que se encuentren ubicados en el counter de seguridad.

Ubicar el equipamiento de soporte (impresoras, fax, etc.) dentro del centro de datos para evitar comprometer información sensible y su utilización por personal no autorizado.

Transporte, protección, y mantenimiento de los equipos y documentación

Busca controlar, monitorear y supervisar el mantenimiento de los equipos del centro de datos, el retiro de los equipos, la reutilización o desafectación de estos, ubicación y copias de seguridad. Incluye también las políticas de escritorios y pantallas limpias.

Mantenimiento de equipos

El mantenimiento del equipamiento se realizará de manera permanente para asegurar integridad y disponibilidad, previniendo también que la información de los equipos no se vea afectada durante estas actividades.

Recomendaciones y controles adicionales:

Establecer un plan de mantenimiento preventivo, en el cuál se debe incluir la frecuencia con el cual se brindará el servicio así también como la autorización formal de los responsables del centro de datos de la carrera de Ingeniería de Sistemas y Software.

Establecer que sólo el personal de mantenimiento con autorización podrá llevar a cabo reparaciones o brindar mantenimiento en los equipos del centro de datos de la carrera.

Registrar todos los mantenimientos realizados sean preventivos o correctivos así también como los tipos de fallas encontradas o supuestas en estos.

Registrar cualquier retiro por mantenimiento de los equipos del centro de datos de la carrera.

Realizar una copia de resguardo a la información confidencial de cualquier equipo que vaya a ser retirado por mantenimiento eliminando la información en este previo retiro.

Retiro de los equipos e información

El equipamiento, la información y el software no serán retirados del centro de datos sin autorización formal.

Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos del centro de datos, las que serán llevadas a cabo por los encargados del centro de datos. El personal será puesto en conocimiento de la posibilidad de realización de dichas comprobaciones.

Recomendaciones y controles adicionales:
Realizar un chequeo semanal de los equipos del centro de datos a fin de evitar que alguno de ellos haya sido retiro de manera no autorizada.

Registrar fecha, hora, nombre y código de la persona encargada del centro de datos y nombre del tercero que proceda a retirar equipo(s) del centro de datos.

Políticas de escritorios y pantallas limpias

Proteger documentos en papel y dispositivos de almacenamiento removibles en las instalaciones del centro de datos de la carrera, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Recomendaciones y controles adicionales:
Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.

Asegurar que la información crítica del centro de datos esté debidamente guardada en un gabinete bajo llave, especialmente si no hay ningún encargado en el centro de datos.

Proteger mediante contraseñas y/o cerraduras los terminales o computadores personales que se encuentran desatendidos; también debe ser desconectados de la red. En caso de haya una necesidad de acceder a estos equipos debe guardarse un registro con el motivo, fecha, hora y nombre de la persona.

Desafectación o reutilización segura de los equipos

La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento. Todo medio de almacenamiento conteniendo material sensible debe ser destruido físicamente.

Recomendaciones y controles adicionales:

Destruir toda la información de los medios de almacenamiento a ser desafectados de los equipos en caso estos pasen a ser reutilizados o desafectados para que la información sensible no sea filtrada por terceros o personal no autorizado.

Borrar de manera completa la información del medio de almacenamiento que será reutilizado en otros ambientes para evitar que la información sensible llegue a manos de personal no autorizado ni terceros.

Ubicación y protección de los equipos y copias de seguridad

Los equipos del centro de datos deben ser ubicados y protegidos de manera que se minimice el riesgo de amenazas y desastres ambientales así también como accesos no autorizados.

Recomendaciones y controles adicionales:

Ubicar los equipos en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.

Proveer un control de accesos adecuado hacia el centro de datos.

Ubicar los equipos del centro de datos en un lugar donde sea fácil de supervisar.

Tener en cuenta las recomendaciones brindadas por la TIA 942 respecto al subsistema Arquitectónico para minimizar el riesgo de amenazas de: robo, incendios, explosivos, humo, inundaciones o filtraciones de agua, polvo, vibraciones, corte de energía eléctrica y derrumbes.

Revisar cada mes las condiciones ambientales de manera que no afecten el correcto funcionamiento del centro de datos.

Considerar el impacto de las amenazas descritas en el punto d) que tengan lugar en zonas próximas al centro de datos.

Mapeo de procesos con directrices físicas

	SEGURIDAD FISICA										
	Protección Física de Accesos		Protección Ambiental				Transporte, Protección y Mantenimiento de Equipamiento y Documentación				
	Controles de Acceso Físico	Desarrollo de Tareas en el Centro de Datos	Perimetro de Seguridad Física	Suministro de Energía	Seguridad de Cableado	Protección de las Instalaciones	Mantenimiento de Equipos	Retiro de los Equipos e Información	Políticas de Escritorios y Pantallas Limpias	Desafectación o Reutilización de los Equipos	Ubicación y Protección de los Equipos y Copias de Seguridad
Control de Ingresos	X	X									
Gestión de Accesos Físicos	X										
Control de Suministro de Energía y Protección de			X	X	X	X					
Retiro de Equipos							X	X	X	X	X

Imagen 17: Mapeo de procesos con directrices físicas

Fuente: Elaboración Propia

Seguridad a nivel lógico

Diseño de la evaluación y del Checklist

Para poder aplicar las medidas necesarias al igual que en la fase de la gestión de la seguridad física, se debe analizar toda la información disponible pero esta vez que sobre la seguridad lógica. Las fuentes que se tomaron en cuenta para realizar este checklist son la NTP 17799, el Orange Book del ministerio de defensa de Estados Unidos y el libro seguridad informática de Purificación Aguilera.

Conceptos	Aspectos específicos	Pregunta
Control de Acceso	Control de acceso al sistema operativo	Identificación y Autentificación de usuarios
Control de Acceso	Control de acceso al sistema operativo	Los usuarios se identifican al ingresar al sistema
Control de Acceso	Control de acceso al sistema operativo	Los usuarios se autentifican al ingresar al sistema
Control de Acceso	Control de acceso al sistema operativo	Los usuarios tienen asignados roles
Control de Acceso	Control de acceso al sistema operativo	Se han establecido las modalidades de acceso correspondientes
Control de Acceso	Control de acceso al sistema operativo	Se ha definido horario de atención a usuarios
Control de Acceso	Control de acceso al sistema operativo	Se ha implementado una política de encriptación de contraseñas de usuarios
Control de Acceso	Control de acceso al sistema operativo	Se ha definido cuál es el periodo de caducidad de las contraseñas
Control de Acceso	Control de acceso al sistema operativo	Se ha definido cuál es la longitud mínima y los

		caracteres que debe contener una contraseña
Control de Acceso	Control de acceso al sistema operativo	Existe un lista de control de accesos
Control de Acceso	Control de acceso al sistema operativo	Existen etiquetas de seguridad
Control de Acceso	Control de acceso al sistema operativo	Existe un sistema de sincronización de password
Control de Acceso	Control de acceso al sistema operativo	Existe un control sobre los puertos de todos los dispositivos del server
Control de Acceso	Control de acceso al sistema operativo	Existen firewalls que impidan accesos no deseados
Control de Acceso	Control de acceso a las aplicaciones y la información	Identificación y Autentificación de usuarios
Control de Acceso	Control de acceso a las aplicaciones y la información	Los usuarios se identifican al ingresar al sistema
Control de Acceso	Control de acceso a las aplicaciones y la información	Los usuarios se autentifican al ingresar al sistema

Control de Acceso	Control de acceso a las aplicaciones y la información	Los usuarios tienen asignados roles
Control de Acceso	Control de acceso a las aplicaciones y la información	Se han establecido las modalidades de acceso correspondientes
Control de Acceso	Control de acceso a las aplicaciones y la información	Se ha definido horario de atención a usuarios
Control de Acceso	Control de acceso a las aplicaciones y la información	Se ha implementado una política de encriptación de contraseñas de usuarios
Control de Acceso	Control de acceso a las aplicaciones y la información	Se ha definido cuál es el periodo de caducidad de las contraseñas
Control de Acceso	Control de acceso a las aplicaciones y la información	Se ha definido cuál es la longitud mínima y los caracteres que debe contener una contraseña
Control de Acceso	Control de acceso a las aplicaciones y la información	Existe un lista de control de accesos
Control de Acceso	Control de acceso a las aplicaciones y la	Se han definido que puertos puede usar cada aplicación

	información	
Control de Acceso	Control de acceso a las aplicaciones y la información (BD)	Identificación y Autentificación de usuarios
Control de Acceso	Control de acceso a las aplicaciones y la información (BD)	Los usuarios se identifican al ingresar al sistema
Control de Acceso	Control de acceso a las aplicaciones y la información (BD)	Los usuarios se autentifican al ingresar al sistema
Control de Acceso	Control de acceso a las aplicaciones y la información (BD)	Los usuarios tienen asignados roles
Control de Acceso	Control de acceso a las aplicaciones y la información (BD)	Se han establecido las modalidades de acceso correspondientes
Control de Acceso	Control de acceso a las aplicaciones y la información (BD)	Se ha definido horario de atención a usuarios
Control de Acceso	Control de acceso a las aplicaciones y la información (BD)	Se ha implementado una política de encriptación de contraseñas de usuarios

Control de Acceso	Control de acceso a las aplicaciones y la información (BD)	Se ha definido cuál es el periodo de caducidad de las contraseñas
Control de Acceso	Control de acceso a las aplicaciones y la información (BD)	Se ha definido cuál es la longitud mínima y los caracteres que debe contener una contraseña
Control de Acceso	Control de acceso a las aplicaciones y la información (BD)	Existe un lista de control de accesos
Control de Acceso	Control de acceso a las aplicaciones y la información (BD)	Existen firewalls que impidan accesos no deseados
Control de Acceso	Control de acceso a la red	Se han definido los accesos a recursos compartidos
Control de Acceso	Control de acceso a la red	Se han creados grupos con perfiles para manejar los accesos.
Control de Acceso	Responsabilidades de usuarios	Se ha definido cuales son las responsabilidades de los usuarios
Control de Acceso	Responsabilidades de usuarios	Se ha definido cuales son las sanciones de los usuarios por infringir las normas

Control de Acceso	Requisitos de negocio para el control de accesos	Se ha establecido una política donde se definan cuáles son los requisitos mínimos de control de accesos.
Gestión de las comunicaciones y operaciones	Procedimientos y responsabilidades de operación	Se han probado que los equipos procesen la información de forma adecuada
Gestión de las comunicaciones y operaciones	Procedimientos y responsabilidades de operación	Se han definido los procedimientos ante incidencias
Gestión de las comunicaciones y operaciones	Planificación y aceptación del sistema	Se han definido todos los procesos que se llevan a cabo dentro del centro de datos
Gestión de las comunicaciones y operaciones	Planificación y aceptación del sistema	Se lleva a cabo una planificación sobre los servicios que se brindan
Gestión de las comunicaciones y	Planificación y aceptación del sistema	Se llevan a cabo pruebas para asegurar que se va a cumplir con los servicios contratados.

operaciones		
Gestión de las comunicaciones y operaciones	Planificación y aceptación del sistema	Se han definidos SLA's para cada servicio brindado
Gestión de las comunicaciones y operaciones	Protección contra software malicioso	Se han instalado en todos los servidores antivirus
Gestión de las comunicaciones y operaciones	Protección contra software malicioso	Se han habilitado las actualizaciones del antivirus
Gestión de las comunicaciones y operaciones	Protección contra software malicioso	Se realizan escaneos completos para verificar que no esté infectado.
Gestión de las comunicaciones y operaciones	Protección contra software malicioso	Se han habilitado las herramientas de escaneo de virus/malware en tiempo real

Gestión de las comunicaciones y operaciones	Protección contra software malicioso	Se ha implementado un firewall que impida accesos no deseados
Gestión de las comunicaciones y operaciones	Protección contra software malicioso	Se ha probado que el firewall y su configuración
Gestión de las comunicaciones y operaciones	Gestión del respaldo y recuperación	Se ha definido el proceso de respaldo de información
Gestión de las comunicaciones y operaciones	Gestión del respaldo y recuperación	Se ha definido la periodicidad del respaldo de la información
Gestión de las comunicaciones y operaciones	Gestión del respaldo y recuperación	Se ha definido cuál es el proceso adecuado de recuperación de información
Gestión de las comunicaciones y	Gestión de la seguridad en redes	Se han bloqueado los puertos del servidor

operaciones		
Gestión de las comunicaciones y operaciones	Utilización de medios informáticos	Se han bloqueado los puertos USB
Gestión de las comunicaciones y operaciones	Utilización de medios informáticos	Se ha bloqueado el uso de la grabadora de CD/DVD
Gestión de las comunicaciones y operaciones	Utilización de medios informáticos	Se ha bloqueado el uso de disquetera
Gestión de las comunicaciones y operaciones	Monitoreo	Se ha definido que se debe realizar monitoreo sobre el uso de centro de datos
Gestión de las comunicaciones y operaciones	Monitoreo	Se guardan de transacciones sobre las operaciones realizadas en el centro de datos

Gestión de las comunicaciones y operaciones	Monitoreo	Se guardan log de intentos no autorizados
Gestión de las comunicaciones y operaciones	Monitoreo	Se guardan log de fallas en el firewall
Gestión de las comunicaciones y operaciones	Monitoreo	Se guardan log de intentos fallidos
Adquisición, desarrollo y mantenimiento de sistemas	Controles criptográficos	Uso de cifrado para la protección de información sensible para la información transportada en medios removibles
Adquisición, desarrollo y mantenimiento de sistemas	Controles criptográficos	Las contraseñas usan sistemas criptográficos para ser creadas
Adquisición, desarrollo y mantenimiento de sistemas	Controles criptográficos	Control de contraseñas (creación, recuperación, definición)

Adquisición, desarrollo y mantenimiento de sistemas	Seguridad de los archivos de sistema	Se ha implementado algún control software, accesos sobre los archivos del sistema
Adquisición, desarrollo y mantenimiento de sistemas	Seguridad de los archivos de sistema	¿Cuál es el procedimiento para modificar archivos en el disco del sistema?
Adquisición, desarrollo y mantenimiento de sistemas	Seguridad de las aplicaciones	Se controlan las modificaciones en los sistemas del centro de datos
Adquisición, desarrollo y mantenimiento de sistemas	Seguridad de las aplicaciones	Se hace un monitoreo aleatorio de logs transaccionales para verificar el uso adecuado de los sistemas.
Adquisición, desarrollo y mantenimiento de sistemas	Seguridad de los procesos de desarrollo y soporte	Se han definido los ambientes de desarrollo
Adquisición, desarrollo y mantenimiento de sistemas	Seguridad de los procesos de desarrollo y soporte	Se han definido los ambientes de pruebas
Adquisición, desarrollo y mantenimiento de sistemas	Seguridad de los procesos de desarrollo y soporte	Se evalúa los impactos producidos por cambios en el ambiente de pruebas
Adquisición, desarrollo y	Seguridad de los procesos de desarrollo y	Se evalúa los impactos producidos por cambios en el

mantenimiento de sistemas	soporte	ambiente de desarrollo
Adquisición, desarrollo y mantenimiento de sistemas	Seguridad de los procesos de desarrollo y soporte	Se tiene un historial de control de versiones
Adquisición, desarrollo y mantenimiento de sistemas	Seguridad de los procesos de desarrollo y soporte	Se tiene un historial de las peticiones de cambio en los sistemas
Adquisición, desarrollo y mantenimiento de sistemas	Seguridad de los procesos de desarrollo y soporte	Se han documentado todos los cambios y los *rollbacks* necesarios para regresar a una versión anterior.
Adquisición, desarrollo y mantenimiento de sistemas	Gestión de la vulnerabilidad técnica	Existe un documento de análisis de vulnerabilidades
Adquisición, desarrollo y mantenimiento de sistemas	Gestión de la vulnerabilidad técnica	Se han llevado a cabo acciones para mitigar estas vulnerabilidades
Adquisición, desarrollo y mantenimiento de sistemas	Requisitos de seguridad de los sistemas	Se ha establecido una política donde se definan cuáles son los requisitos mínimos de seguridad de los sistemas.

Tabla 44: Checklist a Nivel Lógico

Fuente: NTP17799

Interpretación de Resultados

Al aplicar la evaluación dada por el checklist, se obtuvieron los siguientes resultados:

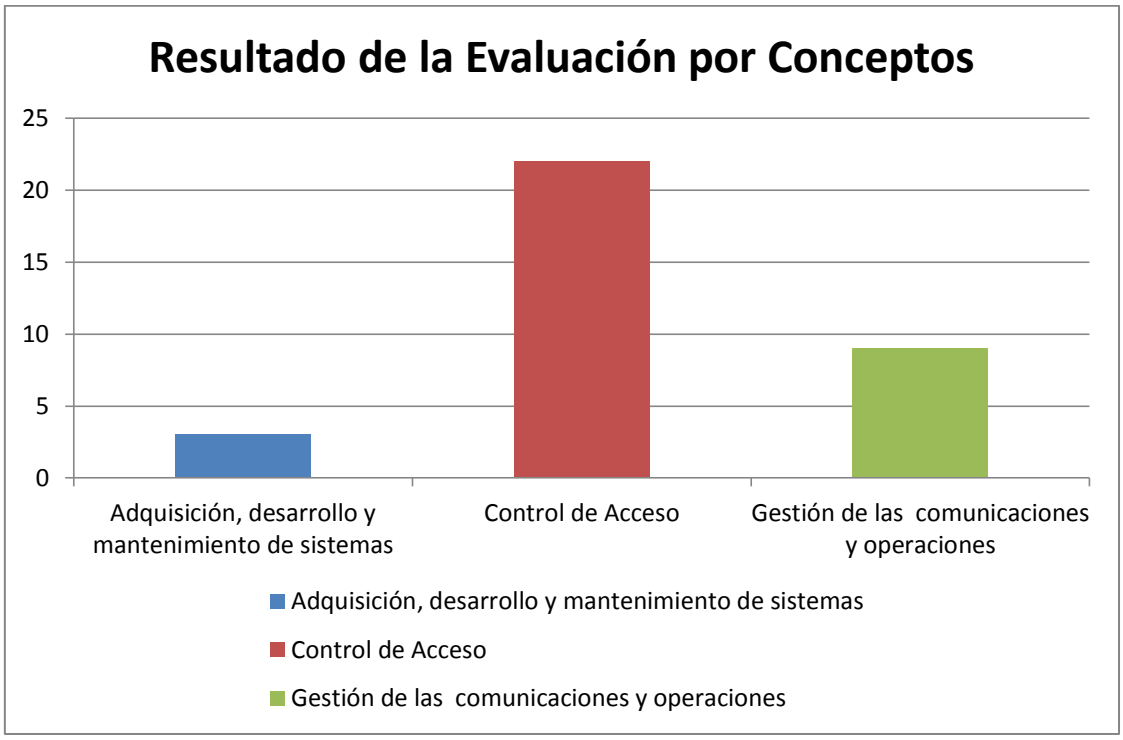


Imagen 18: Resultado de la Evaluación por Conceptos

Fuente: Elaboración Propia

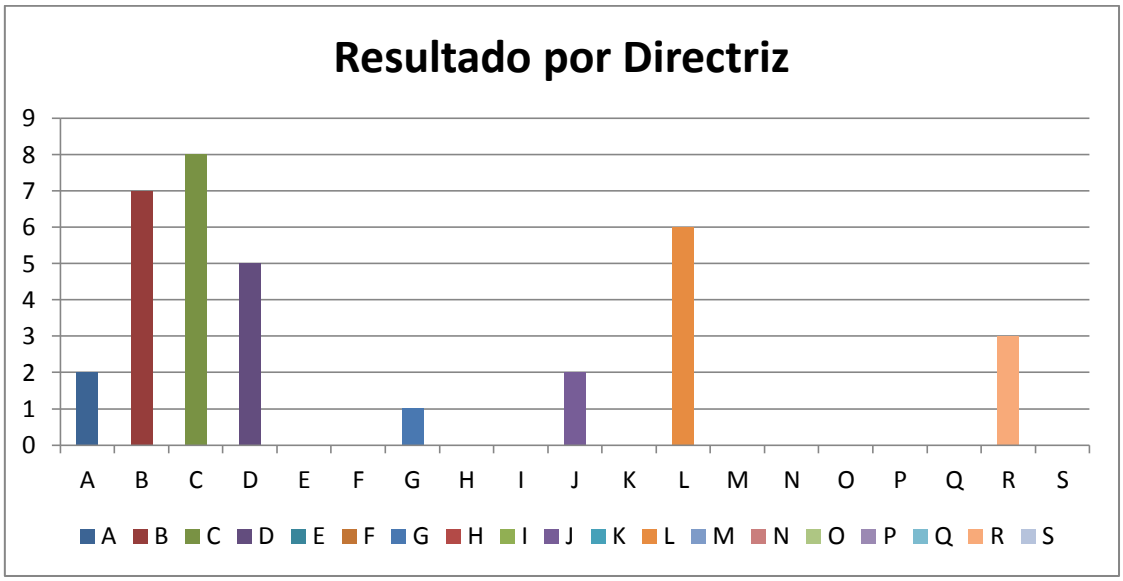


Imagen 19: Resultado por Directriz

Fuente: Elaboración Propia

ID	Directrices
A	Control de acceso a la red
B	Control de acceso a las aplicaciones y la información
C	Control de acceso a las aplicaciones y la información (BD)
D	Control de acceso al sistema operativo
E	Controles criptográficos
F	Gestión de la vulnerabilidad técnica
G	Gestión de la seguridad en redes
H	Gestión del respaldo y recuperación
I	Monitoreo
J	Planificación y aceptación del sistema
K	Procedimientos y responsabilidades de operación
L	Protección contra software malicioso
M	Requisitos de negocio para el control de accesos
N	Requisitos de seguridad de los sistemas
O	Responsabilidades de usuarios
P	Seguridad de las aplicaciones
Q	Seguridad de los archivos de sistema
R	Seguridad de los procesos de desarrollo y soporte
S	Utilización de medios informáticos

Tabla 45: Aspectos Específicos

Fuente: Elaboración Propia

Estos resultados indican que; dentro de la seguridad lógica se han establecido tres conceptos y de estos tres el más desarrollado es el control de accesos, sin embargo existen aspectos específicos que deben ser cubiertos dentro de esta y por otro lado, el concepto menos trabajado es el de adquisición desarrollo y mantenimiento de sistemas pero se debe tomar en consideración que existe un área como servicios generales que se encarga de controlar muchas de estas actividades, las mismas que no pueden ser modificadas o abarcadas por el proyecto.

Procesos de la gestión de la seguridad lógica

Definición de Procesos: Gestión de solicitud de respaldo de información

Propósito del Proceso

El propósito del proceso de Gestión de Solicitud de Respaldo de Información es el de resguardar la información que reside en el centro de datos de la carrera de Ingeniería de Sistemas y Software y en los ambientes de producción y desarrollo. Este proceso surgió debido a la política de seguridad lógica, la cual establece que ante algún incidente o problema que haya sufrido el centro de datos debe existir un repositorio que almacene la información para evitar tiempos de inoperatividad en el servicio.

Descripción

El proceso de Gestión de Solicitud de Respaldo de Información inicia cuando el gerente de proyectos y recursos de la empresa IT-Expert solicita la creación de los archivos de respaldo, esta solicitud puede ser de respaldo de base de datos o de archivos en la carpeta del file server de cada empresa. El gerente de seguridad recibe la solicitud y determina cuál es el tipo de solicitud y procede a crear los archivos de respaldo, resguardando estos en una carpeta asignada para cada tipo de respaldo.

El alcance que tiene las copias de seguridad se limita únicamente a la información que se encuentre en el centro de datos de la carrera de Ingeniería de Sistemas y Software de la UPC, es decir bases de datos en los ambientes de producción y archivos en el file

server[15]. Luego, esta lista debe ser revisada por el Gerente General de la empresa, el mismo que visa la relación y solicita su atención por parte de IT-Expert. Posterior a ello, el Gerente de Proyectos y Recursos procede a revisar la lista y solicita al alumno encargado que tramite y notifique los cambios.

Roles

Roles	Descripción
Gerente de Proyectos y Recursos.	Es la persona encargada de administrar de los servidores del centro de cómputo, realizar seguimiento a los proyectos de la empresa y atender solicitudes de servicios de TI de las empresas virtuales.
Gerente de Seguridad	Encargado de gestionar y supervisar todo lo relacionado a Seguridad tanto dentro como fuera del Centro de Cómputo.

Entradas del Proceso

Entrada	Descripción	Encargado de Elaboración
Lista de carpetas o bases de datos a respaldar	Este documento contiene la lista de carpetas en el file server o nombres de las bases de datos que se encuentran en el centro de datos a ser respaldadas.	Gerencia de Proyectos y Recursos IT-Expert

Salidas del Proceso

Salida	Descripción	Encargado de Elaboración
Informe de	Este documento consiste en el listado de las	Gerente del

trabajo.	carpetas o bases de datos respaldadas, las actividades, incidencias y soluciones que se han seguido a lo largo de proceso.	Seguridad

Caracterización

	Entrada	Actividad	Salida	Descripción	Responsable
1	Listado de carpetas o bases de datos a respaldar.	Inicio	Listado de carpetas o bases de datos a respaldar.	El proceso inicia cuando se le envía un correo al Gerente de Proyectos y Recursos, este correo contiene el listado de carpetas o bases de datos a respaldar, esta solicitud puede ser generada por el Gerente de Recursos de cualquiera empresa virtual.	Gerente de Proyectos y Recursos.
2	Listado de carpetas o bases de datos a respaldar	Solicitar respaldo de información.	Listado de carpetas o bases de datos a respaldar	El Gerente de Proyectos y Recursos. genera el listado de carpetas o bases de datos que deben ser respaldadas	Gerente de Proyectos y Recursos.
3	Listado de carpetas o bases de datos a respaldar	Analizar y verificar solicitud	Listado de carpetas o bases de datos a respaldar Resultado del	El gerente de seguridad analizar y verifica que la solicitud sea factible y que cumpla con los estándares descritos en la política de respaldo	Gerente de Seguridad

			análisis.	de información.	
4	Listado de carpetas o bases de datos a respaldar Resultado del análisis.	Determinar mecanismo de copia.	Manual de mecanismo a seguir.	El gerente de seguridad revisa en base a su análisis preliminar cuál es el manual que debe seguir para realizar esta solicitud.	Gerente de Seguridad
5	Manual de mecanismo a seguir.	¿Qué tipo de solicitud es?	Informe de trabajo. Listado de carpetas o bases de datos a respaldar. Manual de mecanismo a seguir.	Dependiendo del tipo de solicitud (base de datos o carpetas) se debe seguir un determinado flujo que se encuentra en la política de seguridad.	Gerente de Seguridad
6	Listado de carpetas o bases	Determinar e identificar el	Informe de trabajo.	El gerente de seguridad determina cuál es la cantidad y los nombres de	Gerente de

	de datos a respaldar. Manual de mecanismo a seguir. Informe de trabajo.	número de bases de datos para respaldo.	Listado de carpetas o bases de datos a respaldar.	las bases de datos a respaldar.	Seguridad
7	Listado de carpetas o bases de datos a respaldar. Informe de trabajo.	Determinar e identificar el número de carpetas para respaldo.	Informe de trabajo. Listado de carpetas o bases de datos a respaldar	El gerente de seguridad determinar cuál es la cantidad y los nombres de las carpetas a respaldar.	Gerente de Seguridad
8	Informe de trabajo. Listado de	Generar backup de las base de datos.	Informe de trabajo Archivos .bak de respaldo de las base	El gerente de seguridad ejecuta los scripts de respaldo de cada base de datos.	Gerente de Seguridad

	carpetas o bases de datos a respaldar		de datos. Lista de archivos .bak respaldados. Log de procesos de las bases de datos		
9	Informe de trabajo. Listado de carpetas o bases de datos a respaldar	Respaldar información de las carpetas.	Informe de trabajo. Lista de carpetas respaldadas del file server. Listado de carpetas o bases de datos a respaldar.	El gerente de seguridad copia la información contenida en cada carpeta a una ruta específica, esta ruta se encuentra en la política de respaldo de información.	Gerente de Seguridad
10	Informe de trabajo Archivos .bak de respaldo de las	Verificar y supervisar log de backup.	Informe de trabajo. Log de procesos.	El gerente de seguridad debe revisar el log de cada base de datos respaldada y certifica que no exista error alguno.	Gerente de Seguridad

	base de datos. Lista de archivos .bak respaldados. Log de procesos de las bases de datos				
11	Log de procesos. Informe de trabajo.	¿Se encontraron errores en el log?	Informe de trabajo. Listado de carpetas o bases de datos a respaldar. Log de procesos.	En caso se encuentren errores en el log de procesos, se debe realizar nuevamente el proceso de backup de la base o bases que terminaron con error.	Gerente de Seguridad
12	Informe de trabajo. Listado de carpetas o bases de datos a	Determinar Flujo	Informe de trabajo. Listado de carpetas o bases de datos a respaldar	Esta actividad se encarga de discernir si la actividad Generar backup se inició de un flujo normal o de un reproceso se necesita consolidar.	Gerente de Seguridad.

	respaldar. Log de procesos.				
13	Informe de trabajo. Listado de carpetas o bases de datos a respaldar. Lista de carpetas respaldadas del file server.	Consolidar	Listado de carpetas o bases de datos a respaldadas. Copias de las carpetas del file server. Archivos .bak de respaldo de las base de datos.	Como la solicitud puede ser de tres tipos, primero que sea solo respaldo de base de datos, que sea solo respaldo de las carpeta del file server o ambos. El gerente de seguridad debe consolidar la data en una única ubicación.	Gerente de Seguridad
14	Copias de las carpetas del file server. Archivos .bak de respaldo de las	Verificar los archivos generados.	Informe de trabajo. Copias de las carpetas del file server. Archivos .bak de	El gerente debe supervisar que todos los archivos se puedan abrir sin problemas.	Gerente de Seguridad

	base de datos. Listado de carpetas o bases de datos a respaldadas.		respaldo de las base de datos.		
15	Copias de las carpetas del file server. Archivos .bak de respaldo de las base de datos. Informe de trabajo.	Compactar archivos de respaldo.	Archivos compactados. Informe de trabajo. Lista de carpetas respaldadas del file server. Lista de archivos .bak de respaldo de las base de datos.	El gerente de seguridad debe compactar los generados por los respaldos utilizando el compresor instalado en el servidor.	Gerente de Seguridad
16	Lista de carpetas respaldadas del	Guardar los archivos	Informe de trabajo.	El gerente de seguridad debe organizar los archivos generados en	Gerente de Seguridad

	file server. Lista de archivos .bak de respaldo de las base de datos. Informe de trabajo. Archivos compactados.	generados.		las carpetas correspondientes del servidor.	
17	Informe de trabajo.	Ingresar en bitácora.	Bitácora actualizada Informe de trabajo.	El gerente de seguridad debe ingresar la lista de carpetas o base de datos respaldados, la fecha y el estado de los archivos.	Gerente de Seguridad
18	-Bitácora actualizada -Informe de	Fin	Informe de trabajo.	El gerente de seguridad debe enviar un correo al Gerente de Proyectos y Recursos para hacer público que los	Gerente de Seguridad

	trabajo.			respaldos se han llevado a cabo.	

Tabla 46: Gestión de Solicitud de respaldo de información

Fuente: Elaboración Propia

Diagrama del Proceso

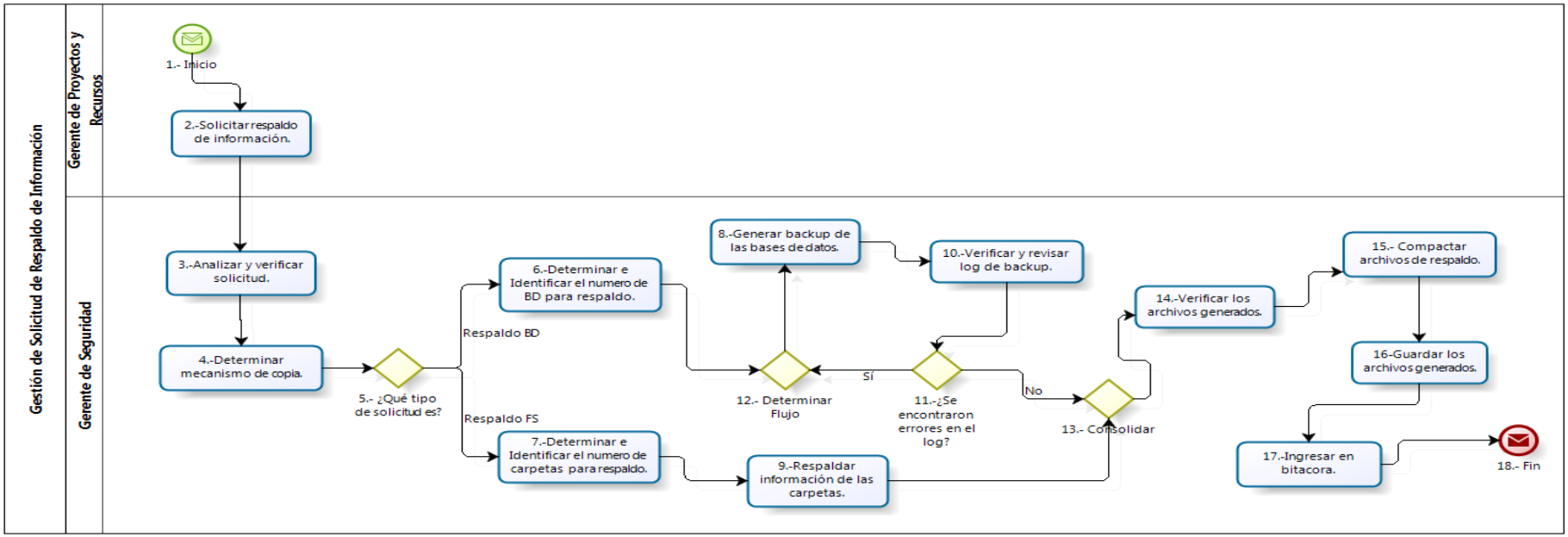


Imagen 20: Gestión de solicitud de respaldo de información

Fuente: Elaboración Propia

Definición de Procesos: Administración de Vulnerabilidades y Parches

Propósito del Proceso

El proceso de Administración de Vulnerabilidades y Parches es el que se encarga de determinar cuáles son las actualizaciones y/o parches que el sistema operativo del servidor necesita tener instalado dentro del centro de datos de la carrera ingeniería de sistemas y software.

Descripción

El proceso de Administración de Vulnerabilidades y Parches inicia cada tres semanas cuando se realiza una revisión de cuáles son las actualizaciones que se encuentran en estado pendiente. Este proceso interactúa con la el análisis de vulnerabilidades que se lleva a cabo en otro proyecto de la empresa IT-Expert.

Roles

Roles	Descripción
Gerente de Proyectos y Recursos.	Administración de los servidores del centro de cómputo. Realizar seguimiento a los proyectos de la empresa Encargado de atender solicitudes de servicios de TI requerido por las empresas virtuales
Gerente del Seguridad	Encargado de gestionar y supervisar todo lo relacionado a Seguridad tanto dentro del Centro de Cómputo.

Entrada del Proceso

Entrada	Descripción	Encargado de Elaboración
Listado de recursos por empresa.	Este documento contiene la lista de alumnos con las que contará la empresa virtual a lo largo del ciclo.	Gerencia de Recursos empresa virtual.

Salidas del Proceso

Salida	Descripción	Encargado de Elaboración
Listado de alumnos con accesos	Este documento consiste en tener el listado de alumnos que cuentan con acceso lógico a la carpeta correspondiente del centro de datos.	Gerente del Seguridad

Caracterización

	Entrada	Actividad	Salida	Descripción	Responsable
0		Inicio	Resultado de la Evaluación de Seguridad.	El gerente de seguridad inicia el proceso de administración de vulnerabilidades en dos momentos, el primero es cuando se ha detectado una nueva vulnerabilidad en el sistema o cuando se inicia cada ciclo académico.	Gerente de Seguridad.
1	Resultado de la Evaluación de Seguridad.	Identificación de vulnerabilidades	Business Impact Analysis.	Proceso que se encarga de elaborar un BIA (Business Impact Analysis) con el objetivo de encontrar vulnerabilidades y/o amenazas que puedan afectar de forma considerable el sistema. Este proceso tiene como información base los resultados de la evaluación desarrollada por el Gerente de Seguridad.	Gerente de Seguridad.
2	Business Impact Analysis	Análisis de vulnerabilidades	Plan de Acción	Proceso que se encarga de elaborar un plan de acción para mitigar los impactos de todas y cada una de las vulnerabilidades y amenazas que fueron detectadas en el BIA.	Gerente de Seguridad.

3	Plan de Acción	¿Es conforme?	Plan de acción Visado. Informe de sustento.	El gerente de recursos y proyectos de IT-Expert se encarga de revisar toda la información con la que se dispone para poder determinar si es provechoso el implementar los cambios sugeridos. Esta es la actividad más crítica dentro del proceso puesto que si el análisis de costo beneficio es incorrecto se puede impactar directamente sobre los servicios brindados. En caso sea adecuado implementar los cambios se crea el plan de acción visado, en caso de no sea recomendable implementar los cambios se crea el informe de sustento.	Gerente de Recursos y Proyectos IT-Expert
4	Plan de Acción Visado.	Implementar Parches.	Informe de implementación	El Gerente de Seguridad se encarga de realizar todas las implementaciones y cambios detallados y requeridos en el documento del plan de acción. Al mismo tiempo el Gerente de Seguridad se encarga de ir registrando todas las incidencias que pueden salir en el proceso con el objetivo de tener mapeadas todas las actividades en caso se necesite hacer un rollback.	Gerente de Seguridad.

5	Informe de Implementación.	Monitorear.	Reporte de Monitoreo	El Gerente de Seguridad debe realizar un monitoreo por tres semanas para asegurar que todos y cada uno de los cambios implementados no han afectado el correcto funcionamiento de los sistemas ni los servicios.	Gerente de Seguridad.
6	Reporte de Monitoreo.	¿Se encontraron fallas?	Reporte de Incidencias. Reporte de Monitoreo.	Si el Gerente de Seguridad encuentra fallas durante el monitoreo debe generar un reporte con la falla encontrada. En caso no se encuentren fallas se crear los reportes de monitoreo.	Gerente de Seguridad.
7	Reporte de Incidencias.	Deshacer los cambios	Reporte de Cambios.	El Gerente de Seguridad utiliza el reporte de Incidencias y el Plan de acción para realizar un rollback de todos los cambios realizados y regresar a un estado seguro.	Gerente de Seguridad.
8	Reporte de Incidencias. Reporte de Monitoreo. Reporte de	Consolidar para Reporte	Reporte de Incidencias. Reporte de Monitoreo. Reporte de	Esta actividad sirve para consolidar todos los documentos necesarios y crear el reporte final. Si se encontraron fallas durante el monitoreo, se utiliza el reporte de cambios para crear el reporte, por otro lado, si no se encontraron fallas se utiliza el reporte de incidencias y de monitoreo para crear el reporte final.	Gerente de Seguridad

	Cambios.		Cambios		
9	Reporte de Incidencias. Reporte de Monitoreo. Reporte de Cambios	Enviar Reporte	Reporte Final	El Gerente de Seguridad genera los reportes necesarios para sustentar el resultado del proceso.	Gerente de Seguridad.
10	Informe de sustento. Reporte Final	Fin	Reporte Final	El Gerente de Seguridad envía un correo al Gerente de Recursos y Proyecto de IT-Expert con el objetivo de informar que el proceso se ha llevado a cabo de forma correcta y que no han surgido problemas.	Gerente de Seguridad.

Tabla 47: Administración de vulnerabilidades y parches

Fuente: Elaboración Propia

Diagrama de Procesos

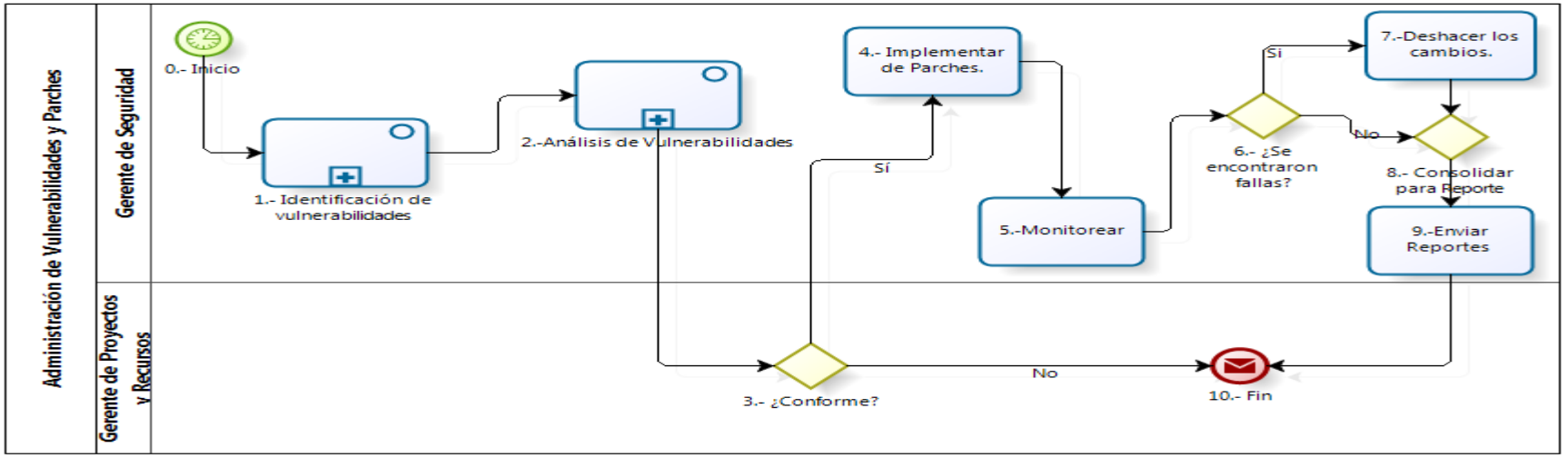


Imagen 21: Administración de vulnerabilidades y parches

Fuente: Elaboración Propia

Definición de Procesos: Gestión de Solicitud de Accesos Lógico

Propósito del Proceso

El propósito del proceso de Gestión de Solicitud de Accesos Lógico es definir cuál es la secuencia de actividades a seguir y el flujo adecuado para solicitar acceso lógico a las carpetas del servidor creadas para cada empresa virtual en el centro de datos de la carrera de Ingeniería de Sistemas y Software. Este proceso guarda estrecha relación con las políticas definidas para la gestión de la seguridad física y lógica.

Descripción

El proceso de Gestión de Solicitud de Accesos se inicia cuando el gerente de recursos de cada empresa virtual genera la relación de alumnos de su empresa que deben tener acceso a las carpetas de cada empresa. Los únicos alumnos que deben tener acceso a dichas carpetas son los alumnos de Taller de Desempeño 1, Taller de Desempeño 2, Taller de Proyectos 1 y Taller de Proyectos 2. Luego, esta lista debe ser revisada por el Gerente General de la empresa, el mismo que visa la relación y solicita su atención por parte de IT-Expert. Posterior a ello, el gerente de proyectos y recursos de IT-Expert revisan la lista y solicita al alumno encargado que tramite y notifique los accesos solicitados.

Roles

Área Funcional	Descripción
Gerente de Proyectos y Recursos.	Alumno encargado de administrar los servidores del centro de cómputo, realizar seguimiento a los proyectos de la empresa y también es el encargado de atender solicitudes de servicios de TI requerido por las empresas virtuales.
Gerente de Seguridad	Encargado de gestionar y supervisar todo lo relacionado a Seguridad dentro del Centro de Cómputo.

Entradas del Proceso

Entrada	Descripción	Encargado de Elaboración
Listado de alumnos por empresa	Este documento contiene la lista de alumnos con las que contará la empresa virtual a lo largo del ciclo.	Gerencia de Recursos empresa virtual.

Salidas del Proceso

Salida	Descripción	Encargado de Elaboración
Listado de alumnos con accesos	Este documento consiste en tener el listado de alumnos que cuentan con acceso lógico a la carpeta correspondiente del centro de datos.	Gerente de Seguridad

Caracterización

	Entrada	Actividad	Salida	Descripción	Responsable
1		Inicio	Listado de alumnos por empresa	El proceso inicia cuando el gerente de proyectos y recursos de la empresa IT- Expert solicita al resto de empresas virtuales la relación de alumnos a los cuales se les debe otorgar acceso lógico a los files server de cada empresa virtual dentro del centro de datos de la carrera de Ingeniería de Sistemas y Software de la UPC.	Gerente de Proyectos y Recursos.
2	Listado de alumnos por empresa	Crear relación de alumnos	Listado de alumnos por empresa	Se prepara el documento que contendrá la relación de alumnos de la empresa que contarán con acceso lógico a las carpetas de cada empresa virtual dentro del centro de datos. Los datos que debe tener este listado es: Código de Alumno, Nombre del Alumno, Empresa.	Gerente de Proyectos y Recursos.
3	Listado de alumnos por empresa	¿Es conforme?	Relación de alumnos revisada.	El gerente de proyectos y recursos de IT-Expert revisan cada relación de alumnos por empresa, verifica que esta sea correcta y que se cumplan con los requisitos mínimos. En caso de ser	Gerente de Proyectos y Recursos.

			Relación de alumnos a revalidar	correcta se pasa a visar la misma. En caso de ser incorrecta se retorna al gerente de recurso de la empresa virtual correspondiente para su atención.	
4	Relación de alumnos a revalidar	Reformular relación de alumnos	Relación de alumnos corregida.	En caso sea necesaria una validación de la lista de alumnos el gerente de recursos de la empresa virtual debe revisar, modificar según corresponda la relación de alumnos y enviarla al gerente de proyectos y recursos para que este verifique nuevamente que todo se encuentre según lo estipulado.	Gerente de Proyectos y Recursos.
5	Relación de alumnos revisada.	Visar y asignar para atención	Relación de alumnos visada.	El gerente de proyectos y recursos visar la relación de alumnos como señal de conformidad y revisión y deriva al gerente de seguridad la relación para que esta sea atendida.	Gerente de Proyectos y Recursos.
6	Relación de alumnos visada. Relación de alumnos corregida.	¿Es conforme?	Relación de alumnos por revisar. Relación de alumnos	Se verifica si se necesita una revisión de la lista de alumnos por parte del gerente de proyectos y recursos. En caso la lista sea correcta se procede a su atención y en caso no serla se solicita una revisión adicional al gerente de recursos de la empresa solicitante.	Gerente de Seguridad

	Relación de alumnos revisada.		visada.		
7	Relación de alumnos por revisar.	Solicitar revisión de lista de alumnos.	Relación de alumnos revisada. Reporte de cancelación por iteraciones.	El gerente de seguridad de IT-Expert puede solicitar la revisión de la lista porque esta no cumple con los requisitos mínimos indispensables. Esta revisión se puede dar hasta en tres oportunidades, si se produce por cuarta vez el proceso se finaliza y se genera el reporte de cancelación por iteraciones.	Gerente de Seguridad
8	Relación de alumnos visada.	Tramitar accesos	Relación de permisos brindados por alumno.	El gerente de seguridad es el responsable de brindar accesos, este tramita los accesos lógicos para los alumnos que figuran en el listado, esta labor consiste en actualizar la información en la base de datos GSFL en la tabla SOL_ACC ingresando todos los datos mencionados en el punto 1, para que de esta forma esta información sea explotada desde un Excel con programación VBA.	Gerente de Seguridad

9	Relación de permisos brindados por alumno.	Notificar accesos.	Reporte de relación permisos - alumnos.	Cuando se haya terminado la actualización de los datos en la base de datos, el gerente de seguridad debe enviar un correo detallando los cambios al responsable del centro de datos y recordándole la ruta donde se encuentra el Excel que genera el reporte de listado de accesos permitidos y también a los alumnos a los cuales se les brindo el acceso correspondiente.	Gerente de Seguridad
10	Reporte de relación permisos - alumnos. Reporte de cancelación por iteraciones.	Fin	Correo de notificación	El gerente de seguridad se encarga de enviar un correo al gerente de recursos de cada empresa virtual con la relación de alumnos que cuentan con acceso a la carpeta compartida.	Gerente de Seguridad

Tabla 48: Gestión de solicitud de accesos lógicos

Fuente: Elaboración Propia

Diagrama del Proceso

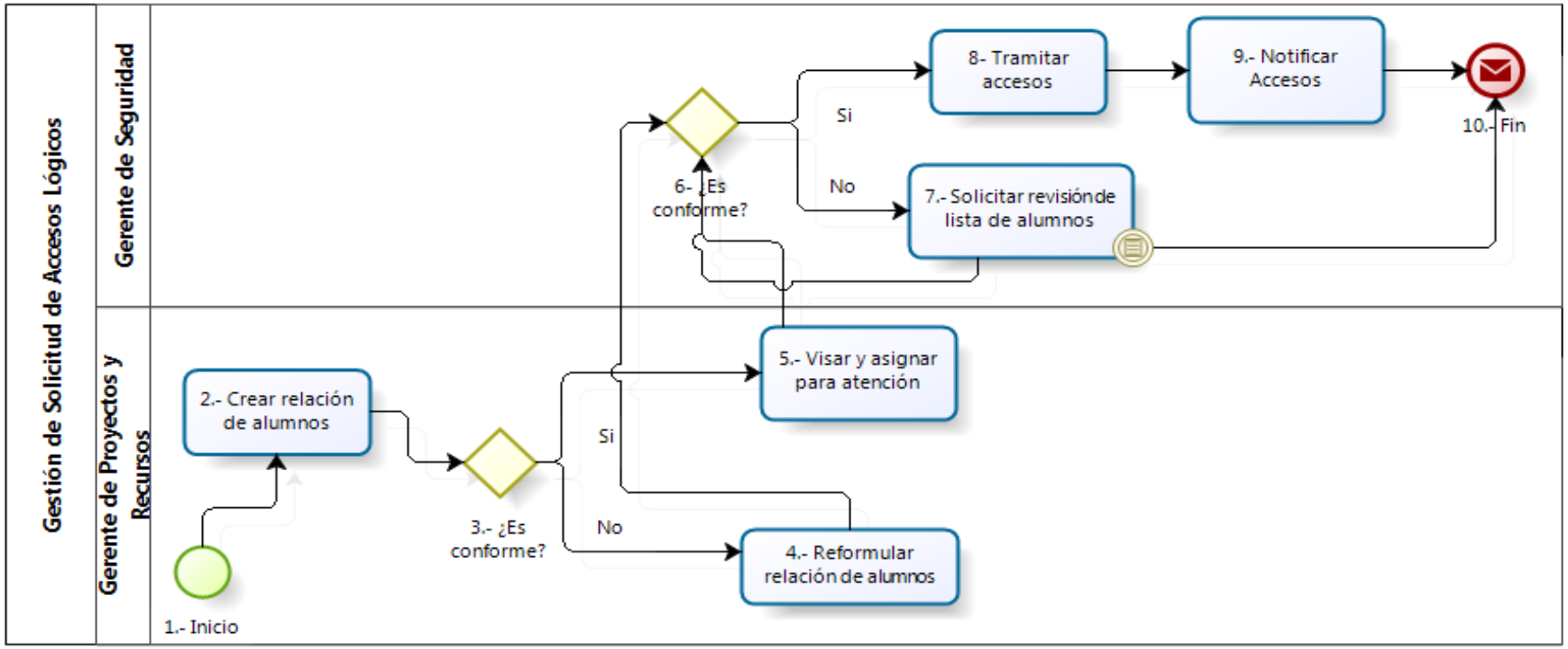


Imagen 22: Gestión de solicitud de accesos lógicos

Fuente: Elaboración Propia

Definición de Procesos: Monitoreo de Componentes

Propósito del Proceso

El proceso de Monitoreo de Componentes consiste en llevar a cabo una serie de actividades para determinar si el funcionamiento de todos los componentes del centro de datos de la carrera de Ingeniería de Sistemas y Software. Por otro lado, este proceso se encarga de supervisar que la carga de trabajo que tiene el centro de datos en la actualidad se encuentra dentro de la capacidad del centro de datos y así evitar incidentes.

Descripción

El proceso de Monitoreo de Componentes inicia cada tres semanas durante el horario de talleres de proyecto (Lunes 4-7 pm y Miércoles de 4-7). Este proceso tiene que evaluar cada uno de los componentes del centro de datos de la carrera.

Roles

Rol	Descripción
Gerente del Seguridad	Encargado de gestionar y supervisar todo lo relacionado a la seguridad dentro del Centro de Cómputo.

Entradas del Proceso

Entrada	Descripción	Encargado de Elaboración
Lista de Métricas por componente del Sistema.	Este documento contiene la lista métricas a calcular para cada uno de los componentes del sistema dentro del centro de datos de la carrera.	Gerencia de Recursos y Proyectos

Salidas del Proceso

Salida	Descripción	Encargado de Elaboración
Reporte Final del Sistema.	Este documento consiste un informe sobre el estado actual del sistema y de cada componente evaluado.	Gerente del Seguridad

Caracterización

	Entrada	Actividad	Salida	Descripción	Responsable
1		Inicio	Lista de Métricas por componente del Sistema.	Este proceso inicia cada tres semanas a partir del inicio de clases de cada ciclo regular y durante los horarios de talleres de desempeño y taller de proyecto.	Gerente de Seguridad.
2	Lista de Métricas por componente del Sistema.	Monitorear particiones.	Reporte de Métricas de Particiones.	En esta actividad el gerente de seguridad se encarga de realizar un monitoreo y control sobre el desempeño de las particiones en cada uno de los servidores del centro de datos de la carrera. Las métricas que debe calcular son Velocidad de Lectura, Velocidad de Escritura, Porcentaje de Uso y Tiempo de Acceso.	Gerente de Seguridad.
3	Reporte de Métricas de Particiones.	¿Se detectaron fallas?	Reporte de Incidencia de Particiones. Reporte de Métricas de	En caso se encuentren fallas se inicia el proceso de Identificación de Problemas y se crea un reporte de incidencia, en caso contrario se procede a realizar el siguiente monitoreo.	Gerente de Seguridad.

			Particiones.		
4	Reporte de Métricas de Particiones. Reporte de Incidencia de Particiones.	Monitorear discos.	Reporte de Métricas de Disco.	En esta actividad el gerente de seguridad se encarga de realizar un monitoreo y control sobre el desempeño de cada uno de los discos duros en los servidores del centro de datos de la carrera. Las métricas que debe calcular son Velocidad de Lectura, Velocidad de Escritura, Porcentaje de Uso y Tiempo de Acceso.	Gerente de Seguridad.
5	Reporte de Métricas de Disco.	¿Se detectaron fallas?	Reporte de Incidencia de Discos. Reporte de Métricas de Disco.	En caso se encuentren fallas se inicia el proceso de Identificación de Problemas y se crea un reporte de incidencia, en caso contrario se procede a realizar el siguiente monitoreo.	Gerente de Seguridad.
6	Reporte de Métricas de Disco.	Monitorear desempeño de la CPU.	Reporte de Métricas de CPU.	En esta actividad el gerente de seguridad se encarga de realizar un monitoreo y control sobre el desempeño de todos los CPU ’s dentro del centro de datos de la carrera. Las métricas que debe calcular son Porcentaje de Uso de Sistema, Porcentaje de	Gerente de Seguridad.

	Reporte de Incidencia de Discos.			Uso de Aplicaciones, Porcentaje de Memoria Utilizado y Porcentaje de CPU utilizado.	
7	Reporte de Métricas de CPU.	¿Se detectaron fallas?	Reporte de Incidencia de CPU.	En caso se encuentren fallas se inicia el proceso de Identificación de Problemas y se crea un reporte de incidencia, en caso contrario se procede a realizar el siguiente monitoreo.	Gerente de Seguridad.
8	Reporte de Métricas de CPU. Reporte de Incidencia de CPU.	Verificar uso de ancho de banda	Reporte de Métricas de ancho de banda.	En esta actividad el gerente de seguridad se encarga de realizar un monitoreo y control sobre el uso del ancho de banda del servidor. Las métricas a calcular son Tiempo de subida de archivos, Tiempo de bajada de archivos, Numero de MB por segundo y Tiempo de respuesta.	Gerente de Seguridad.
9	Reporte de Métricas de ancho de banda.	¿Se detectaron fallas?	Reporte de Incidencia de Ancho de Banda.	En caso se encuentren fallas se inicia el proceso de Identificación de Problemas y se crea un reporte de incidencia, en caso contrario se procede a realizar el siguiente monitoreo.	Gerente de Seguridad.

10	Reporte de Métricas de ancho de banda. Reporte de Incidencia de Ancho de Banda.	Revisar logs de sistemas.	Reporte de Métricas de Logs del Sistema.	En esta actividad el gerente de seguridad se encarga de revisar los logs del sistema para verificar que no se haya presentado algún inconveniente con el sistema.	Gerente de Seguridad.
11	Reporte de Métricas de Logs del Sistema.	¿Se detectaron fallas?	Reporte de Incidencia de Logs.	En caso se encuentren fallas se inicia el proceso de Identificación de Problemas y se crea un reporte de incidencia, en caso contrario se procede a realizar el siguiente monitoreo.	Gerente de Seguridad.
12	Reporte de Incidencia de Logs. Reporte de Métricas de Logs del	Probar equipos de red.	Reporte de Métricas de Red.	En esta actividad el gerente de seguridad se encarga de realizar un monitoreo y control sobre el desempeño de las particiones en cada uno de los servidores del centro de datos de la carrera. La métrica a calcular es el Tiempo de respuesta de Router/Switch, Número de paquetes enviados, Número de paquetes recibidos y Número de paquetes perdidos.	Gerente de Seguridad.

	Sistema.				
13	Reporte de Métricas de Red.	¿Se detectaron fallas?	Reporte de Incidencia de Equipos de Red. Reporte de Problemas. Reporte de Métricas de Red.	En caso se encuentren fallas se inicia el proceso de Identificación de Problemas y se crea un reporte de incidencia, en caso contrario se procede a realizar el siguiente monitoreo.	Gerente de Seguridad.
14	Reporte de Incidencia de Logs. Reporte de Incidencia de Equipos de	Identificación de Problemas.	Plan de Acción. Reporte de Problemas.	Proceso aún no definido por ser parte del proyecto de alumnos de TP1.	Gerente de Seguridad.

	Red. Reporte de Incidencia de Ancho de Banda. Reporte de Incidencia de CPU. Reporte de Incidencia de Discos. Reporte de Incidencia de Particiones.				
15	Reporte de Problemas.	Generar Reporte.	Reporte Final del Sistema.	El gerente de seguridad generar un reporte consolidado los reportes de cada incidencia en caso se haya presentado alguna o crea un reporte con el estado del sistema y las métricas	Gerente de Seguridad.

	Reporte de Métricas de Red.			calculadas en cada actividad de monitoreo.	
16	Reporte Final del Sistema.	Fin	Reporte Final del Sistema.	El reporte es enviado al Gerente de Recursos y Proyectos de IT-Expert y el Gerente General de la empresa IT-Expert	Gerente de Seguridad.

Tabla 49: Monitoreo de Componentes

Fuente: Elaboración Propia

Diagrama de Procesos

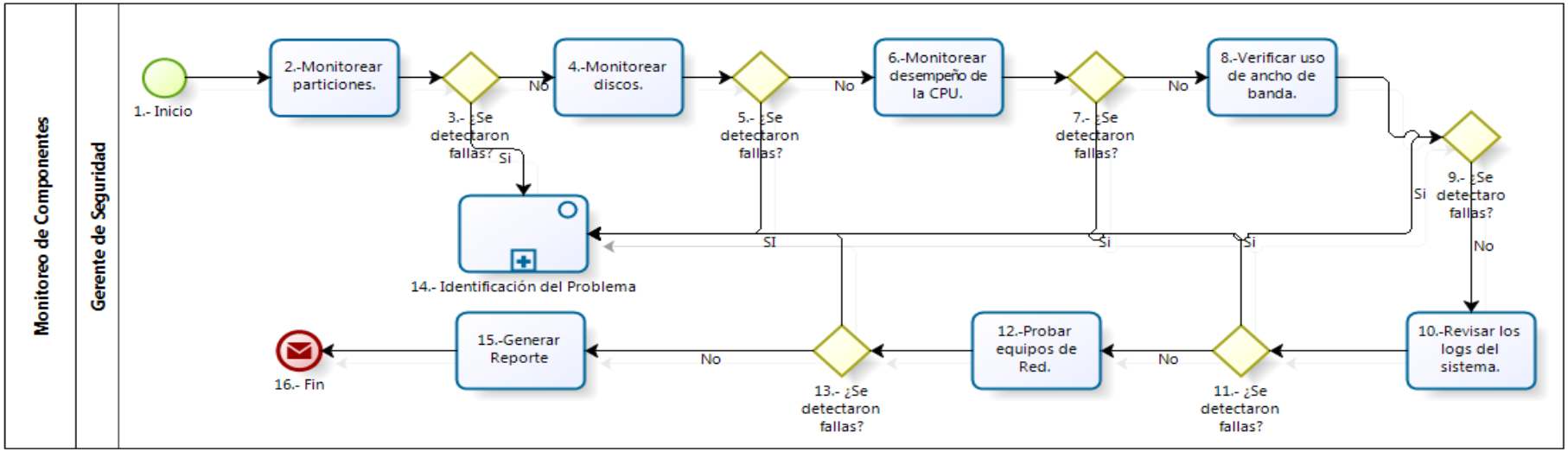


Imagen 23: Monitoreo de Componentes

Fuente: Elaboración Propia

Definición de Procesos: Gestión de Pruebas de Seguridad

Propósito del Proceso

El propósito del proceso de Gestión de Pruebas de Seguridad es determinar cuál es el procedimiento adecuado para llevar a cabo las pruebas de seguridad al interior de las instalaciones del centro de datos y determinar si surgen nuevas incidencias con respecto a la seguridad para que sean atendidas por la Gestión de Problemas y al mismo tiempo para obtener indicadores de desempeño del centro de datos.

Descripción

El proceso de Gestión de Pruebas de Seguridad inicia cada primer día hábil de cada trimestre del ciclo académico. Es aquí cuando el Gerente de Seguridad revisa la bitácora de errores para determinar si han surgido nuevos incidentes que deben ser derivados a la Gestión de Problemas para que esta pueda determinar cuál es la causa del mismo y así aplicar las medidas correctivas necesarias.

El alcance de las pruebas se limita únicamente a los componentes que se encuentren dentro del centro de datos de la carrera de Ingeniería de Sistemas de Información. Las pruebas que se llevarán a cabo han sido determinadas mediante un análisis de seguridad y en estas se deben obtener los siguientes indicadores:

Número de nuevos incidentes.

Número de incidentes repetitivos.

Número de incidentes detectados.

Al final de proceso el Gerente de Seguridad se encarga de notificar al Gerente General de IT-Expert sobre las nuevas incidencias encontradas para que esté al tanto de las mismas y de los posibles riesgos inherentes a estas fallas.

Roles

Roles	Descripción
Gerente de Seguridad	Encargado de gestionar y supervisar todo lo relacionado a Seguridad dentro del Centro de Cómputo.

Entradas del Proceso

Entrada	Descripción	Encargado de Elaboración
Listado de pruebas a realizar	Este documento contiene la lista de pruebas/software a utilizar para determinar si el centro de datos se encuentra en un nivel mínimo aceptable.	Gerencia de Proyectos y Recursos IT-Expert

Salidas del Proceso

Salida	Descripción	Encargado de Elaboración
Informe de Pruebas de Seguridad.	Este documento consiste en el listado de las pruebas realizadas, las incidencias registradas y los posibles impactos de las mismas.	Gerente del Seguridad

Caracterización

	Entrada	Actividad	Salida	Descripción	Responsable
1	-	Inicio	Listado de pruebas a realizar	El proceso inicia por solicitud expresa del gerente de proyectos y recursos de IT-Expert	Gerente de Seguridad
2	Listado de pruebas a realizar	Revisar bitácora de errores	Listado de errores en bitácora.	El gerente de seguridad revisa la relación de incidencias registradas en la bitácora para así determinar si existe un incidente no registrado antes o no.	Gerente de Seguridad
3	Listado de errores en bitácora.	¿Se encontraron nuevas fallas?	Listado de Nuevos Incidentes. Listado de Errores en	Al revisar la bitácora el gerente de seguridad debe analizar si se trata de un nuevo problema o de uno ya conocido, en caso se trate de un nuevo problema se deriva el caso a la Gestión de Problemas para que	Gerente de Seguridad

			bitácora.	lo identifique.	
4	Listado de Nuevos Incidentes.	Gestión de Problemas		El proceso aún no se ha terminado de definir por los alumnos de proyecto 1, sin embargo, este proceso tiene como input la información encontrada en las pruebas de seguridad.	Gerente de Seguridad
5	Listado de Errores en bitácora.	Consolidar	Listado de Errores en bitácora.	Esta actividad sirve para determinar consolidar todos los documentos necesarios de la actividad Realizar las pruebas según manual.	Gerente de Seguridad
6	Listado de Errores en bitácora.	Realizar las pruebas según Manual	Resultado de la Evaluación.	El gerente de seguridad se encarga de llevar a cabo las pruebas descritas en el Manual de Pruebas con el objetivo de identificar el origen de las incidencias encontradas en la bitácora que no	Gerente de Seguridad

				han sido derivadas a la Gestión de Problemas.	
7	Resultado de la Evaluación.	¿Se encontraron fallas?	Listado de Incidencias encontrado durante la Evaluación. Listado de Nuevas Fallas.	En caso de encontrarse fallas se notifican las mismas y se analiza si deben ser enviadas a la Gestión de Problemas o se debe buscar una solución a este incidente.	Gerente de Seguridad
8	Listado de Incidencias encontrado durante la Evaluación.	Registrar Incidencias Encontradas	Listado de fallas registradas.	El gerente de seguridad registra las incidencias encontradas para que estas sirvan de ayuda a futuros problemas que se puedan presentar.	Gerente de Seguridad
9	Listado de Incidencias encontrado durante la	Consolidar	Listado de fallas registradas.	Esta actividad sirve para determinar consolidar todos los documentos necesarios de la actividad Crear informe de pruebas	Gerente de Seguridad

	Evaluación. Listado de Nuevas Fallas. Listado de fallas registradas.			de seguridad	
10	Listado de fallas registradas.	Crear informe de pruebas de seguridad	Informe de Pruebas de Seguridad.	El gerente de seguridad se encarga de crear el informe de pruebas de seguridad para que el Gerente General de IT-Expert esté al tanto de las mismas.	Gerente de Seguridad
11	Informe de Pruebas de Seguridad.	Fin	Correo de Notificación	Se envía el Informe de Pruebas de Seguridad al Gerente de Proyectos y Recursos de la empresa IT-Expert.	Gerente de Seguridad

Tabla 50: Gestión de Pruebas de Seguridad

Fuente: Elaboración Propia

Diagrama del Proceso

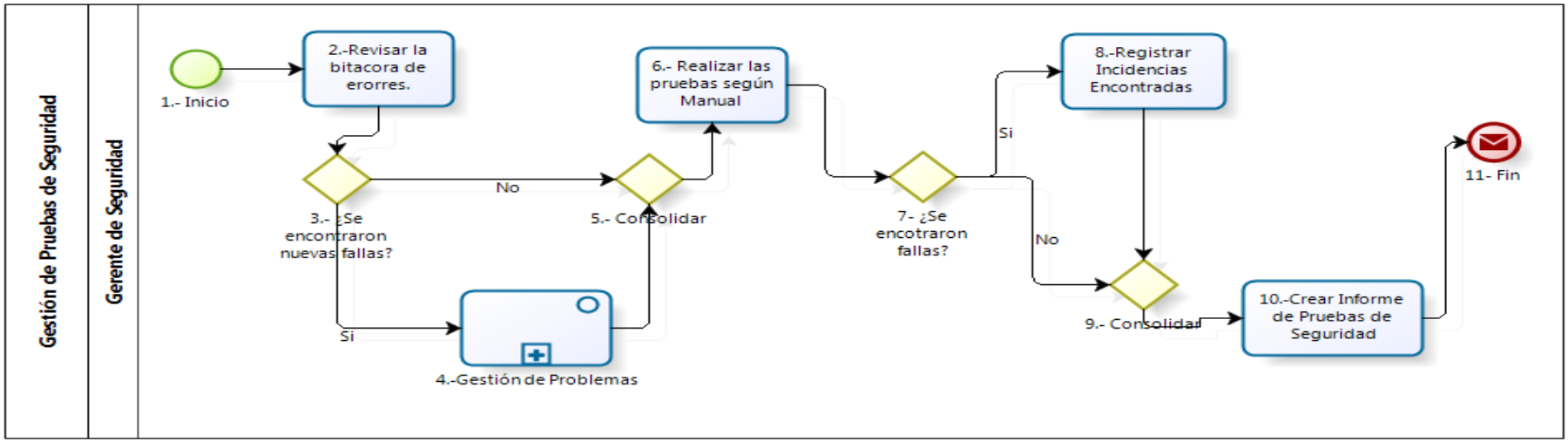


Imagen 24: Gestión de Pruebas de Seguridad

Fuente: Elaboración Propia

Definición de Procesos: Restauración de Backup

Propósito del Proceso

El propósito del proceso de restauración de backup es determinar cuál es el procedimiento adecuado para llevar a cabo la restauración de los archivos que han sido almacenados en un archivo de respaldo.

Descripción

El proceso de restauración de backup inicia cuando le llega al gerente de proyectos y recursos de la empresa virtual IT-Expert una solicitud de restauración de archivos de respaldo. El gerente debe validar y verificar que la solicitud cumpla con los requisitos mínimos para ser atendido. El gerente de seguridad determina qué tipo de solicitud es, es decir si se trata de la restauración de una base de datos o de algún archivo del file server respaldado. El gerente de seguridad debe notificar a la gestión de problemas si se presenta algún problema del cual no tiene conocimiento ni información disponible a lo largo del proceso. Finalmente, el gerente de seguridad envía el informe de restauración para dar por finalizado el proceso.

Roles

Roles	Descripción
Gerente de Seguridad	Encargado de gestionar y supervisar todo lo relacionado a Seguridad dentro del Centro de Cómputo.
Gerente de Proyectos y Recursos	Es la persona encargada de administrar de los servidores del centro de cómputo, realizar seguimiento a los proyectos de la empresa y atender solicitudes de servicios de TI de las empresas virtuales.

Entradas del Proceso

Entrada	Descripción	Encargado de Elaboración
Formato de restauración.	Este documento contiene la lista de archivos y/o bases de datos que deben ser restaurados, este documento debe tener un sustento del porque se necesita la restauración y la conformidad del gerente del recursos de la empresa que solicite el servicio.	Gerencia de Proyectos y Recursos IT-Expert

Salidas del Proceso

Salida	Descripción	Encargado de Elaboración
Informe de Restauración.	Este documento consiste en el listado de los archivos que se han restaurado exitosamente y cuales han sufrido problemas a los largo del proceso y han sido derivados a la gestión de problemas para su atención	Gerente del Seguridad

Caracterización

	Entrada	Actividad	Salida	Descripción	Responsable
1	Formato de restauración.	Inicio	Formato de restauración.	El proceso inicia por solicitud expresa de cualquier empresa virtual a la cual IT-Expert brinda servicios.	Gerente de Proyectos y Recursos.
2	Formato de restauración.	Revisar/Derivar el caso.	Conformidad de atención. Formato de restauración	El gerente de proyectos y recursos de la empresa IT-Expert se encarga de revisar que el formato de restauración cumpla con todas las indicaciones y requisitos presentes en el formato. Una vez verificada la información en el formato, se deriva al gerente de seguridad para su atención.	Gerente de Proyectos y Recursos.
3	Formato de restauración.	Verificar el tipo de solicitud	Listado de archivos a	El gerente de seguridad se encarga de revisar y determinar de qué tipo de solicitud se trata y cuál es el procedimiento	Gerente de Seguridad

	Conformidad de atención.		restaurar. Manual de Restauración.	a seguir. La solicitud de restauración puede ser de dos tipos: Archivos en el File Server o Restauración de Base de Datos.	
4	Listado de archivos a restaurar. Manual de Restauración.	Ejecutar proceso de Restauración de Base de Datos	Listado de archivos restaurados.	El gerente de seguridad sigue el procedimiento detallado en el Manual de Restauración para restaurar la base de datos solicitada.	Gerente de Seguridad
5	Listado de archivos a restaurar. Manual de Restauración.	Restaurar archivos del file server.	Listado de archivos restaurados.	El gerente de seguridad sigue el procedimiento detallado en el Manual de Restauración para restaurar archivos que se encuentren dentro del File Server.	Gerente de Seguridad
6	Listado de archivos restaurados.	Verificar errores/problemas	Resultado de Validación de Archivos	El gerente de seguridad verifica y comprueba que los archivos (base de datos, archivos) que han sido restaurados se	Gerente de Seguridad

			Restaurados. Listado de archivos restaurados.	encuentren de habilitados y no tengan problemas.	
7	Resultado de Validación de Archivos Restaurados.	Gestión de Problemas		El proceso Gestión de Problemas tiene como inputs los posibles errores que aparecen en la restauración de backup. Y el output aún no se tiene definido pues forma parte de un proyecto de alumnos de taller de proyecto1	Gerente de Seguridad
8	Resultado de Validación de Archivos Restaurados. Listado de archivos restaurados.	Consolidar	Resultado de Validación de Archivos Restaurados. Listado de archivos restaurados.	Esta actividad se encarga de unificar y controlar el inicio de la actividad Crear Informe de Restauración ya que está puede iniciarse desde la Gestión de Problemas en caso se hayan presentado problemas nuevos o iniciar directamente dado que no se encontraron nuevos problemas.	Gerente de Seguridad

9	Resultado de Validación de Archivos Restaurados. Listado de archivos restaurados.	Crear informe de restauración.	Informe de Restauración	El gerente de seguridad se encarga de crear el informe de restauración en el cual se detalla cuáles son los archivos restaurados y cuál es el estado de los mismos.	Gerente de Seguridad
10	Informe de Restauración	Fin		Se envía el Informe de Restauración al Gerente de Proyectos y Recursos de la empresa IT-Expert.	Gerente de Seguridad

Tabla 51: Restauración de Backup

Fuente: Elaboración Propia

Diagrama del Proceso

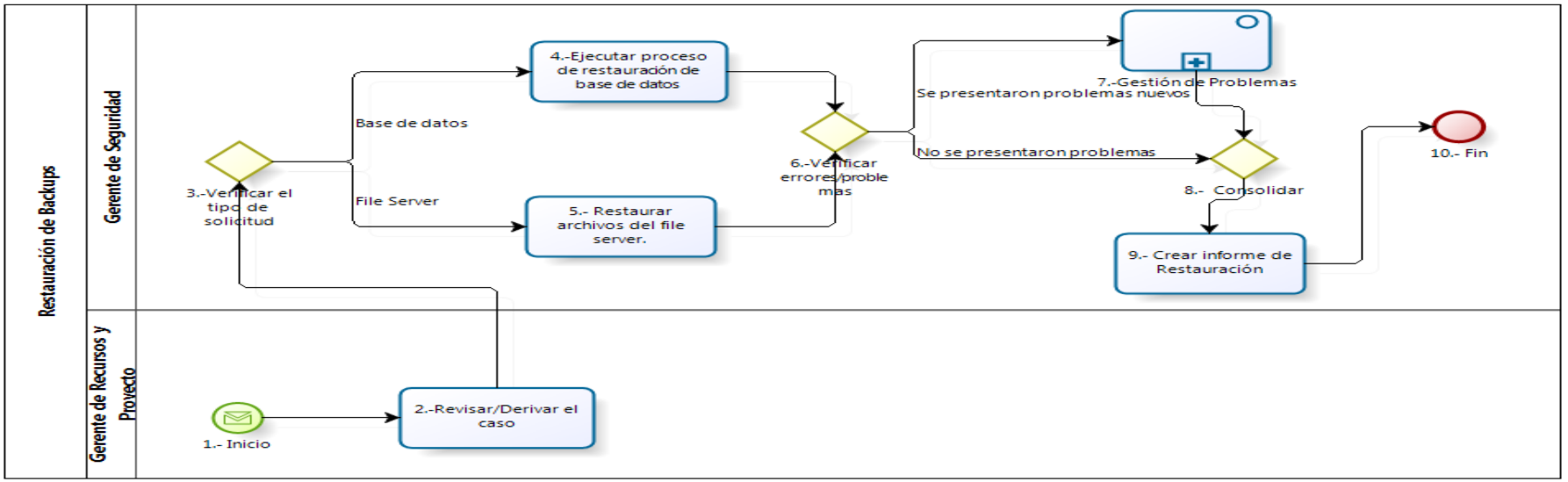


Imagen 25: Restauración de Backup

Fuente: Elaboración Propia

Definición de Procesos: Control de Vulnerabilidades Técnicas

Propósito del Proceso

El propósito del proceso de control de vulnerabilidades técnicas es el de definir, controlar y monitorear a los recursos que desempeñan un rol en el manejo de las vulnerabilidades técnicas de los sistemas del centro de datos.

Descripción

El proceso de Control de vulnerabilidades técnicas se inicia cuando el gerente de seguridad define los roles y responsabilidades en base a los diferentes sistemas y aplicativos desplegados en el centro de datos de la carrera. Una vez definido esto se envía el documento al Gerente General y este lo delega al Gerente de Proyectos y Recursos para que este asigne dichos roles entre los recursos de la empresa virtual IT-Expert. El recurso envía su conformidad al Gerente de Proyectos y Recursos, el cuál será revisado por este y enviado de vuelta al gerente de seguridad para que este defina la línea de tiempo, evaluación de parches y determine el monitoreo y evaluación de las vulnerabilidades con cada recurso responsable por los sistemas del centro de datos.

Roles

Roles	Área Funcional	Descripción
Gerente General	IT-Expert	Encargada de monitorear el avance y la presentación de los entregables, además de realizar las coordinaciones necesarias entre el Jefe de Proyecto y el Comité de Proyectos.
Gerente de Proyectos y Recursos	IT-Expert	Encargado de supervisar y administrar todos los proyectos de la empresa IT-Expert.
Recurso	IT-Expert	Alumno de IT-Expert que se encuentra cursando los cursos de Taller de

		Desempeño o Taller de Proyectos.
Gerente de Seguridad	IT-Expert	Encargado de gestionar y supervisar todo lo relacionado a Seguridad tanto dentro como fuera del Centro de Cómputo.

Entradas del Proceso

Entrada	Descripción	Encargado de Elaboración
Necesidad de control de vulnerabilidades técnicas de los sistemas del centro de datos	Al inicio del ciclo académico el gerente de seguridad tendrá que definir los roles y responsabilidades respecto a los sistemas del centro de datos.	Gerente de Seguridad

Salidas del Proceso

Salida	Descripción	Encargado de Elaboración
Documento de monitoreo y evaluación de las vulnerabilidades técnicas	Este documento indica el plan a seguir para el control, monitoreo y evaluación de los sistemas del centro de datos respecto a sus vulnerabilidades técnicas.	Gerente de Seguridad

Caracterización

	Entrada	Actividad	Salida	Descripción	Responsable
1	--	Inicio	Necesidad de control de vulnerabilidades técnicas de los sistemas del centro de datos.	Inicia el proceso.	Gerente de Seguridad
2	Necesidad de control de vulnerabilidades técnicas de los sistemas del centro de datos	Definir roles y responsabilidades	Documento de roles y responsabilidades sobre el control de vulnerabilidades técnicas	Cada período académico el jefe de seguridad de turno define los roles y responsabilidades sobre los sistemas del centro de datos. Esto se da cada inicio de ciclo académico.	Gerente de Seguridad
3	Documento de roles y responsabilidades sobre el control de vulnerabilidades técnicas	Enviar documento	Documento de roles y responsabilidades enviado	El jefe de seguridad envía el documento al gerente general de la empresa virtual IT-Expert.	Gerente de Seguridad

4	Documento de roles y responsabilidades enviado	Revisar documento de roles y responsabilidades	Recepción y revisión de documento de roles y responsabilidades revisado	El gerente general de la empresa virtual IT-Expert revisa el documento.	Gerente General
5	Recepción y revisión de documento de roles y responsabilidades revisado	Enviar documento	Envío de documento de roles y responsabilidades revisado enviado	El gerente general de la empresa virtual IT-Expert envía al gerente de proyectos y recursos el documento.	Gerente General
6	Envío de documento de roles y responsabilidades revisado enviado	Revisar documento de roles y responsabilidades	Recepción y revisión de documento de roles y responsabilidades revisado	El gerente de proyectos y recursos revisa el documento.	Gerente de Proyectos y Recursos
7	Recepción y revisión de documento de roles y responsabilidades revisado	Enviar documento	Envío de documento de roles y responsabilidades revisado enviado	El gerente de proyectos y recursos envía a los recursos de la empresa tanto a Helpdesk como a Service Desk el documento.	Gerente de Proyectos y Recursos
8	Envío de documento de roles y	Revisar documento de roles y	Revisión de documento de roles y	El recurso revisa el documento de roles y	Recurso

	responsabilidades revisado enviado	responsabilidades	responsabilidades revisado	responsabilidades a detalle.	
9	Revisión de documento de roles y responsabilidades revisado	Enviar conformidad	Conformidad de recurso	El recurso envía su conformidad respecto al rol y responsabilidad asignado.	Recurso
10	Conformidad de recurso	Revisar conformidades	Conformidad de Gerente de proyectos y recursos	El gerente se encarga de revisar las conformidades y de informar al jefe de seguridad sobre esto.	Gerente de Proyectos y Recursos
11	Conformidad de Gerente de proyectos y recursos	Definir línea de tiempo	Documento de definición de línea de tiempo	El jefe de seguridad elabora el documento de definición de línea de tiempo respecto a los sistemas del centro de datos enfocándose en las vulnerabilidades técnicas potenciales y relevantes.	Gerente de Seguridad
12	Documento de definición de línea de tiempo	Definir evaluación de parches	Documento de evaluación de parches	El jefe de seguridad elabora el documento de evaluación de parches con los aplicativos actuales con los que cuenta el centro de datos, indicando en este cuáles serán los pasos por	Gerente de Seguridad

				cada aplicativo para ejecutar la actividad en caso sea requerida. En esta actividad se podrá verificar el número de parches definidos por aplicativo en el ciclo académico.	
13	Documento de evaluación de parches	Monitorear y evaluar las vulnerabilidades técnicas	Documento de monitoreo y evaluación de las vulnerabilidades técnicas	El jefe de seguridad se encarga de realizar un monitoreo y evaluación acompañado de los recursos asignados a cada sistema o aplicativo a realizar una pequeña evaluación sobre las vulnerabilidades técnicas. Esta actividad se realiza cada inicio y fin de ciclo académico. En esta actividad se podrá identificar el número de vulnerabilidades técnicas evaluadas y monitoreadas durante el ciclo académico.	Gerente de Seguridad
14	Documento de monitoreo y evaluación de las vulnerabilidades técnicas	Fin	--	El proceso finaliza cuando el gerente de seguridad revisa el documento de monitoreo y evaluación de las vulnerabilidades técnicas.	Gerente de Seguridad

Tabla 52: Control de Vulnerabilidades Técnicas

Fuente: Elaboración Propia

Diagrama del Proceso

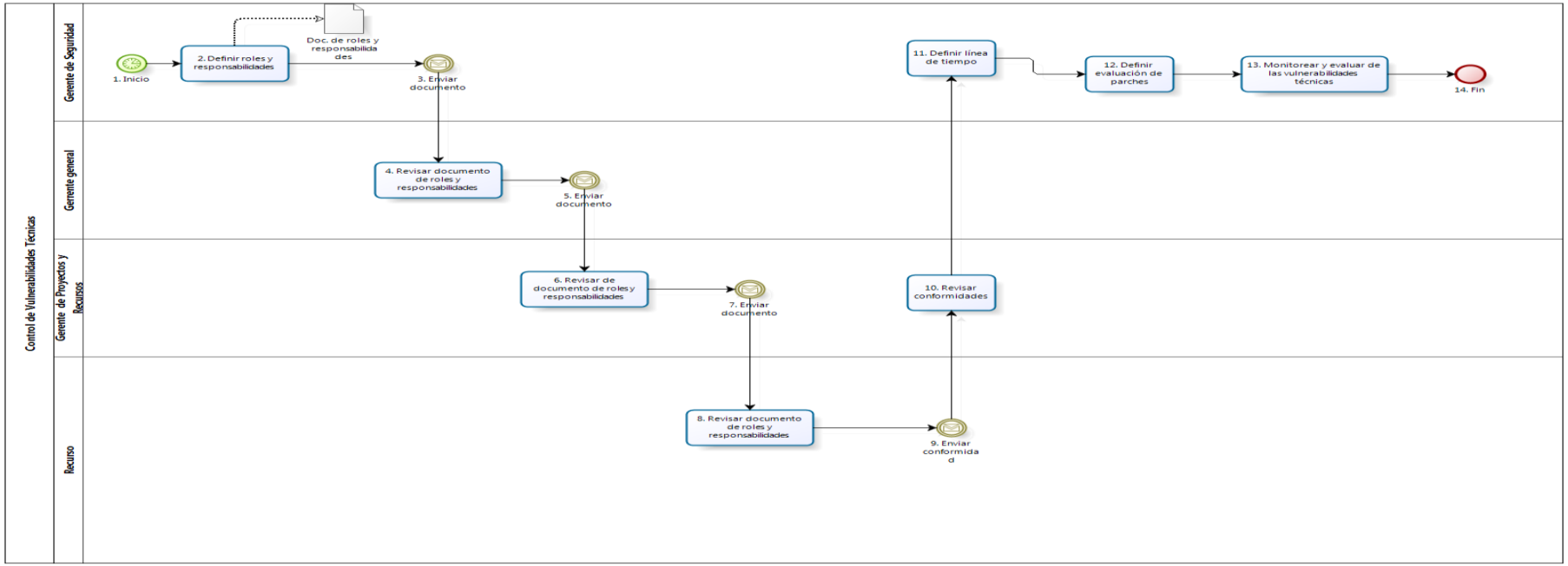


Imagen 26: Control de Vulnerabilidades Técnicas

Fuente: Elaboración Propia

Definición de Procesos: Gestión de Claves

Propósito del Proceso

El propósito del proceso de Gestión de Claves es el de monitorear a lo largo del ciclo académico en curso el proceso de atención de registro, re inicialización y control de las contraseñas de los recursos de las empresas virtuales específicamente las de la empresa virtual IT-Expert. Este proceso es clave para mantener protegido los datos de los aplicativos del centro de datos de la facultad.

Descripción

El proceso de Gestión de Claves se inicia cuando se inicia el ciclo académico en curso y el Gerente de Proyectos y Recursos de la empresa virtual IT-Expert elabora el documento con el consolidado de los recursos con sus roles, así también con los perfiles en los aplicativos con los que cuenta el centro de datos. Este documento es enviado y validado por Service Desk, en caso no pase la validación se envía el documento al Gerente de Proyectos y Recursos para que corrija los errores, por otro lado, si pasa la validación, se envía a Helpdesk para que este identifique a los encargados de cada aplicativo y se asignen las contraseñas a los recursos que lo requieren, informando a estos sobre su contraseña y haciéndoles recordar que tienen que cambiarla a una de su preferencia personal. Al final del ciclo se reinicializan las contraseñas a todos los recursos por parte de los encargados de los aplicativos.

Roles

Roles	Descripción
Gerente de Proyectos y Recursos.	Administración de los servidores del centro de cómputo. Realizar seguimiento a los proyectos de la empresa Encargado de atender solicitudes de servicios de TI requerido por las empresas virtuales

Gerente del Seguridad	Encargado de gestionar y supervisar todo lo relacionado a Seguridad tanto dentro como fuera del Centro de Cómputo.
Encargado - Helpdesk	Recurso de la empresa virtual IT-Expert que se encargan de atender solicitudes delegadas por Service Desk.
Encargado - Service Desk	Recurso de la empresa virtual IT-Expert que se encargan de atender validar y delegar solicitudes o requerimientos de los usuarios.

Entradas del Proceso

Entrada	Descripción	Encargado de Elaboración
Inicio de Ciclo Académico	Se elabora el documento con el mapeo de recursos, roles, perfiles y aplicativos para que Service Desk y Helpdesk puedan brindar las contraseñas a los recursos de la empresa.	Gerente de Proyectos y Recursos

Salidas del Proceso

Salida	Descripción	Encargado de Elaboración
Reporte de problemas. Encuesta de ciclo final.	Al finalizar el ciclo los recursos de Helpdesk elaborarán un reporte indicando si se tuvo inconvenientes con las contraseñas en algún aplicativo (como borrado aleatorio, etc.) así como también la aplicación de una encuesta en la cual se verificará si la gestión de las contraseñas fue óptima.	Helpdesk

Caracterización

	Entrada	Actividad	Salida	Descripción	Responsable
1	--	Inicio	Lista de alumnos matriculados	Se Inicia el proceso obteniendo la lista de alumnos matriculados en los cursos de TDP1, TDP2, TP1 y TP2 en el presente ciclo académico.	Gerente de Proyectos y Recursos
2	Lista de alumnos matriculados	Elaborar documento de recursos, roles y aplicativos	Documento de recursos, roles y aplicativos	El Gerente de recursos elabora el documento con el fin de mapear los recursos con los roles que desempeñarán en el ciclo académico así como también con los aplicativos que estos usaran a lo largo del ciclo.	Gerente de Proyectos y Recursos
3	Documento de recursos, roles y aplicativos	Enviar documento	Documento de recursos, roles y aplicativos enviado	El Gerente envía el documento a Service Desk para que este valide el documento y lo delegué.	Gerente de Proyectos y Recursos
4	*Documento de recursos, roles y aplicativos *enviado*. * Documento de recursos, roles y	Identificar si es corrección o primera entrega	Documento de recursos, roles y aplicativos identificado	El encargado de Service Desk identifica si es una corrección o una primera entrega, ya que en caso sea una primera entrega se valida todo el documento y si es una corrección se validan las correcciones únicamente.	Encargado - Service Desk

	aplicativos *corregido*.				
5	Documento de recursos, roles y aplicativos identificado	Revisar documento de recursos, roles y aplicativos	Documento de recursos, roles y aplicativos recibido	Service Desk Revisa el documento para validarlo.	Encargado - Service Desk
6	Documento de recursos, roles y aplicativos recibido	Validar documento de recursos, roles y aplicativos	Conforme. No conforme.	Service Desk valida el documento.	Encargado - Service Desk
7	No conforme	Enviar no conformidad	Documento de recursos, roles y aplicativos no conforme enviado	Service Desk envía el documento sin conformidad al Gerente de Proyectos y Recursos para que este realice las correcciones necesarias.	Encargado - Service Desk
8	Documento de recursos, roles y aplicativos no	Corregir documento de recursos, roles y	Documento de recursos, roles y aplicativos	El Gerente realiza las correcciones necesarias al documento.	Gerente de Proyectos y Recursos

	conforme enviado	aplicativos	corregido		
9	Documento de recursos, roles y aplicativos corregido	Enviar documento corregido	Documento de recursos, roles y aplicativos corregido y enviado	El Gerente envía el documento a Service Desk para que este valide el documento y lo delegué.	Gerente de Proyectos y Recursos
10	Conforme	Enviar documento	Documento de recursos, roles y aplicativos enviado	Service Desk delega la solicitud a Helpdesk.	Encargado - Service Desk
11	Documento de recursos, roles y aplicativos enviado	Revisar documento de recursos, roles y aplicativos	Documento de recursos, roles y aplicativos recibidos	Helpdesk Revisa el documento y asigna a un recurso para que atienda la solicitud	Encargado - Helpdesk
12	Documento de recursos, roles y aplicativos recibidos	Revisar relación de recursos encargados	Relación de recursos revisado	Helpdesk revisa la relación de recursos encargados de los aplicativos	Encargado - Helpdesk
13	Relación de	Identificar	Recurso	Dependiendo del aplicativo Helpdesk identifica a los encargados de los aplicativos y les delega la lista de los	Encargado -

	recursos revisado	recurso para tarea	identificado	recursos que necesitarán que se les cree una contraseña nueva o que se les reinicie la contraseña	Helpdesk
14	*Recurso identificado * No conformidad enviada	Verificar procedencia	Procedencia verificada	El encargado de Helpdesk verifica la procedencia ya que si es un recurso que recién se ha de asignar es porque hay que realizar todo el registro en cambio, si proviene del gerente de recursos es porque solo hay que realizar las correcciones realizadas por éste.	Encargado - Helpdesk
15	Procedencia verificada	Registrar o corregir contraseña	Contraseña registrada / corregida	El recurso registra la contraseña para el recurso de IT-Expert que usará el aplicativo y en caso ya cuenta con una contraseña desde el ciclo pasado se procederá a reiniciar la contraseña. En esta actividad se podrá identificar el número de contraseñas registradas y corregidas en el ciclo académico así como también el número de contraseñas mal registradas y mal corregidas en el ciclo académico.	Encargado - Helpdesk
16	Contraseña registrada / corregida	Enviar información de registro	Información enviada	Se envía un correo a todos los recursos a los cuales se les ha registrado una contraseña y se les recuerda que tienen que cambiar esa contraseña y colocar una propia.	Encargado - Helpdesk

17	Información enviada	Recepción de información de contraseñas	Información de contraseñas recibida	El Gerente recibe la información de las contraseñas registradas.	Gerente de Proyectos y Recursos
18	Información de contraseñas recibida	Verificar información de registro de contraseñas	*Conforme. *No conforme.	El Gerente verifica que las contraseñas brindadas sean las mismas que las solicitadas en el documento de recursos, roles y aplicativos. En esta actividad se podrá identificar el porcentaje de contraseñas registradas y corregidas de manera correcta versus las contraseñas que fueron mal registradas en el ciclo académico.	Gerente de Proyectos y Recursos
19	No conforme.	Enviar no conformidad	No conformidad enviada	El Gerente envía la no conformidad de la información de las contraseñas para que el encargado de Helpdesk revise sus errores de ingreso.	Gerente de Proyectos y Recursos
20	Conforme	Enviar conformidad	Conformidad enviada	El Gerente envía su conformidad con la tarea realizada por el encargado de Helpdesk.	Gerente de Proyectos y Recursos
21	Conformidad enviada	Registrar en la BD	Registros realizados	El encargado de Helpdesk se encarga de registrar la información en la base de datos. En esta actividad se podrá identificar Número de registros de contraseñas en la	Encargado - Helpdesk

				Base de datos a lo largo del ciclo académico.	
22	Registros realizados	Reiniciar contraseñas	Registros realizados revisados	Al finalizar el ciclo académico se procede a reiniciar todas las contraseñas de los recursos de la empresa virtual IT-Expert. Por lo que el encargado revisa los registros realizados en el presente ciclo académico.	Encargado - Helpdesk
23	Registros realizados revisados	Reiniciar contraseñas	Contraseñas reiniciadas	Se reinician las contraseñas al finalizar el ciclo académico y se realiza un informe detallando esta actividad.	Encargado - Helpdesk
24	Contraseñas reiniciadas	Fin	--	El proceso finaliza cuando el encargado reinicia las contraseñas de los usuarios del ciclo académico que esta por culminar.	Encargado - Helpdesk

Tabla 53: Gestión de Claves

Fuente: Elaboración Propia

Diagrama del Proceso

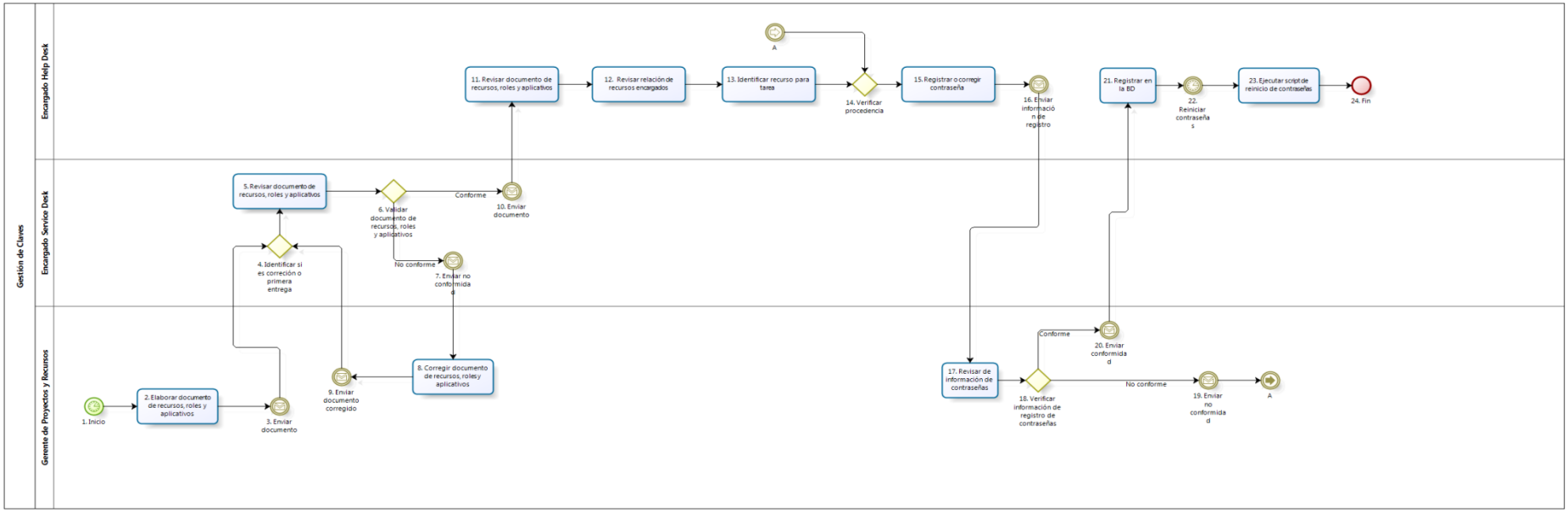


Imagen 27: Gestión de Claves

Fuente: Elaboración Propia

Definición de Procesos: Revisión e Instalación de Software

Propósito del Proceso

El propósito del proceso de Revisión e instalación de software es la de controlar y proteger el centro de datos de la instalación de cualquier software que no cuente con los requisitos necesarios que indican que es seguro y así no poner en riesgo la seguridad de la información del centro de datos.

Descripción

El proceso de Revisión e instalación de software se inicia cuando nace una solicitud de parte de un recurso de la empresa virtual IT-Expert tiene la necesidad de instalar un aplicativo, por lo que envía una solicitud en donde detalla la información del aplicativo. Esta solicitud es enviada a Service Desk donde se atiende y se valida el formato de ésta. En caso la validación sea correcta, la solicitud es enviada al gerente de seguridad de Helpdesk el cual se encargará de evaluar y validar la información del software a ser instalado así como también ver si es factible la instalación del mismo en el centro de datos, reuniéndose con el recurso de la empresa virtual para afinar detalles sobre la instalación del aplicativo.

Roles

Roles	Área Funcional	Descripción
Gerente de Seguridad	IT-Expert	Es el encargado de velar por la seguridad del centro de datos.
Recurso IT-Expert	IT-Expert	Es el recurso de la empresa virtual IT-Expert el cual puede estar cursando los cursos de taller de desempeño o proyecto.
Service Desk	IT-Expert	Es el encargado de controlar y monitorear las solicitudes de los usuarios.

Entradas del Proceso

Entrada	Descripción	Encargado de Elaboración
Necesidad de Instalación de un nuevo software en el centro de datos	La necesidad de instalar un nuevo software en el centro de datos siempre es una necesidad para los recursos de las diferentes empresas virtuales de la carrera especialmente de la empresa virtual IT-Expert.	Recurso IT-Expert

Salidas del Proceso

Salida	Descripción	Encargado de Elaboración
Software instalado correctamente registrado.	El software es registrado debidamente en la base de datos donde están registrados los aplicativos que están desplegados en el centro de datos.	Jefe de Seguridad - Helpdesk

Caracterización

	Entrada	Actividad	Salida	Descripción	Responsable
1	--	Inicio	Necesidad de Instalación de un nuevo software en el centro de datos	Se inicia el proceso al necesitarse la instalación de un nuevo software en el centro de datos.	Recurso IT-Expert
2	Necesidad de Instalación de un nuevo software en el centro de datos	Redactar solicitud de instalación de software en el centro de datos	Solicitud de instalación de nuevo software en el centro de datos	Un recurso de la empresa virtual IT-Expert redacta una solicitud de instalación de un nuevo software en el centro de datos en vista a una necesidad.	Recurso IT-Expert
3	Solicitud de instalación de nuevo software en el centro de datos	Enviar solicitud	Solicitud de instalación de nuevo software en el centro de datos enviado	El recurso de la empresa IT-Expert envía la solicitud a Service Desk.	Recurso IT-Expert
4	Solicitud de instalación de nuevo software en el centro	Revisar	*Solicitud de instalación de nuevo software en el centro	Un recurso de Service Desk se encarga de revisar la solicitud, en	Service Desk

	de datos	solicitud	de datos aceptada. *Solicitud de instalación de nuevo software en el centro de datos rechazada.	caso de aceptar se delega el pedido. En caso que no se acepta, se rechaza la solicitud.	
5	Solicitud de instalación de nuevo software en el centro de datos rechazada.	Enviar solicitud rechazada	Solicitud de instalación de nuevo software en el centro de datos rechazada enviada.	El recurso de Service Desk envía la respuesta a la solicitud del usuario.	Service Desk
6	Solicitud de instalación de nuevo software en el centro de datos rechazada enviada. *Solicitud de instalación de nuevo software en el centro de datos aceptada enviada revisada rechazada enviada.	Término	--	Al ser rechazada la solicitud se envía una respuesta al usuario explicándole la razón del rechazo dando por finalizado el proceso. El usuario en caso desee reenviar otra solicitud tendrá que iniciar el proceso nuevamente.	Recurso IT-Expert
7	Solicitud de instalación de nuevo software en el centro de datos aceptada	Enviar solicitud aceptada	Solicitud de instalación de nuevo software en el centro de datos aceptada enviada.	El recurso de Service Desk delega la solicitud la solicitud hacia Helpdesk	Service Desk

8	Solicitud de instalación de nuevo software en el centro de datos aceptada enviada.	Revisar solicitud de instalación de software en el centro de datos	Solicitud de instalación de nuevo software en el centro de datos aceptada enviada recibida	El jefe de seguridad quien es el encargado de velar por la seguridad del centro de datos recibe la solicitud y procede a revisarla.	Gerente de Seguridad
9	Solicitud de instalación de nuevo software en el centro de datos aceptada enviada revisada	Validar solicitud de instalación	*Solicitud de instalación de nuevo software en el centro de datos aceptada enviada revisada aceptada. *Solicitud de instalación de nuevo software en el centro de datos aceptada enviada revisada rechazada.	El jefe de seguridad quien es el encargado de velar por la seguridad del centro de datos revisa la solicitud y realiza un estudio en el cual ve si el software a instalar cuenta con todos los requisitos necesarios de seguridad. Esta actividad permitirá identificar el número de vulnerabilidades básicas con las que cuentan los aplicativos rechazados en el ciclo académico así también el porcentaje de aplicativos aceptados vs rechazados en el ciclo académico.	Gerente de Seguridad

10	*Solicitud de instalación de nuevo software en el centro de datos aceptada enviada revisada rechazada.	Enviar solicitud rechazada	Solicitud de instalación de nuevo software en el centro de datos aceptada enviada revisada rechazada enviada.	El jefe de seguridad envía su respuesta al usuario detallando el motivo del rechazo.	Gerente de Seguridad
11	*Solicitud de instalación de nuevo software en el centro de datos aceptada enviada revisada aceptada.	Enviar solicitud aceptada	Solicitud de instalación de nuevo software en el centro de datos aceptada enviada revisada aceptada enviada	El jefe de seguridad envía su respuesta al usuario indicándole el día en que se llevará a cabo la reunión para ver detalles sobre la instalación	Gerente de Seguridad
12	Solicitud de instalación de nuevo software en el centro de datos aceptada enviada revisada aceptada enviada	Revisar respuesta	Solicitud de instalación de nuevo software en el centro de datos aceptada enviada revisada aceptada enviada revisada.	El usuario recibe y revisa la respuesta enviada por el jefe de seguridad.	Recurso IT-Expert
13	Solicitud de instalación de nuevo software en el centro de datos aceptada enviada revisada aceptada enviada	Establecer reunión	Acta de reunión	El usuario se reúne con el jefe de seguridad especificando los detalles de la instalación del software en el centro de datos.	Recurso IT-Expert

	revisada.				
14	Acta de reunión. *Software instalado de manera incorrecta.	Instalar software en el centro de datos	Software instalado	El jefe de seguridad se encarga de realizar la instalación del software en el centro de datos.	Gerente de Seguridad
15	Software instalado	Validar instalación del software	*Software instalado correctamente. *Software instalado de manera incorrecta.	El usuario verifica si el software fue instalado de manera correcta.	Recurso IT-Expert
16	Software instalado correctamente.	Registrar nuevo software en la lista de aplicativos del centro de datos	Software instalado correctamente registrado.	El jefe de seguridad registra el nuevo software a detalle dentro del registro donde se encuentran todos los aplicativos que cuenta el centro de datos. Esta actividad permitirá identificar el número de aplicativos instalados en el ciclo académico.	Gerente de Seguridad
17	Software instalado	Fin	--	El proceso finaliza al concretarse la instalación del software y a su vez	Gerente de

	correctamente registrado.			este es registrado.	Seguridad

Tabla 54: Revisión e Instalación de Software

Fuente: Elaboración Propia

Diagrama del Proceso

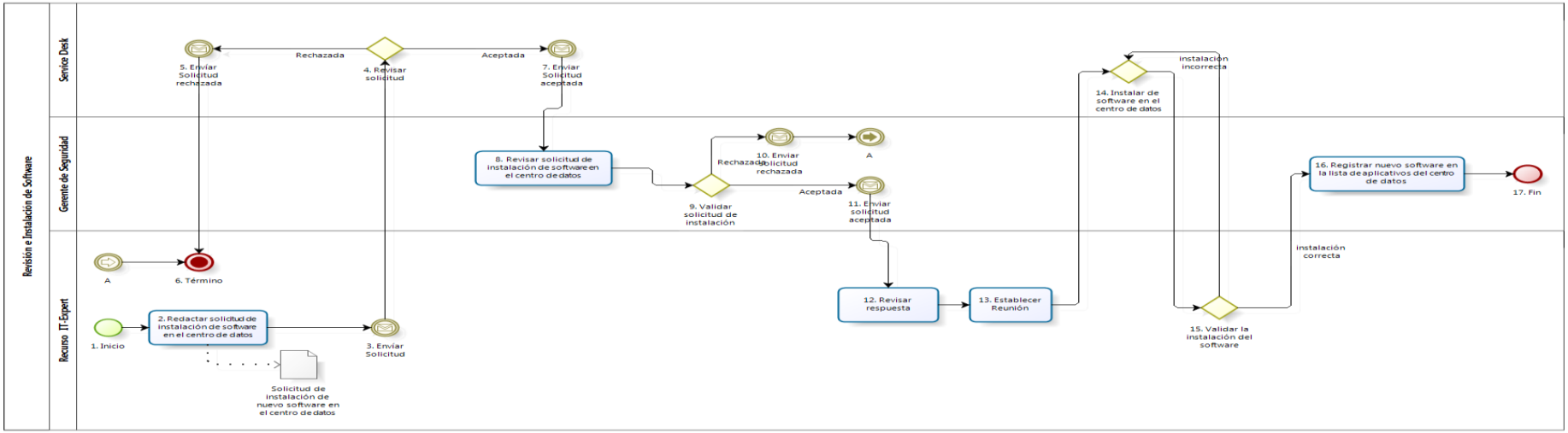


Imagen 28: Revisión e instalación de Software

Fuente: Elaboración Propia

Política de Seguridad Lógica

Introducción

La seguridad lógica brinda el marco para proteger a la información en el uso de aplicativos y sistemas durante las operaciones en el centro de datos de la facultad de Ingeniería. También, previene evitar al máximo el riesgo de accesos no autorizados, mediante el establecimiento de controles de accesos.

Se distinguen tres conceptos a tener en cuenta: gestión de comunicaciones y operaciones, control de accesos y la adquisición y mantenimiento de sistemas; los cuáles se tocan de manera detallada en los puntos: 3.7.8.1, 3.7.8.2 y 3.7.8.3 en este mismo documento.

Alcance

Esta política aplicará a todo el personal vinculado laboralmente y educativamente con la UPC así también terceros que tengan acceso a los recursos de información del data center de la universidad.

Acrónimos y definiciones

Data Center – Centro de datos de la carrera de Ingeniería de Sistemas y Software de la Universidad Peruana de Ciencias Aplicadas.

Objetivos

Objetivo General

- Establecer las políticas básicas que normarán la infraestructura destinada a brindar seguridad lógica de los sistemas del centro de datos.

Objetivos Específicos

Asegurar las operaciones de los recursos de tratamiento de información se realicen de manera segura y correcta en el centro de datos.

Controlar los accesos a la información de los sistemas del centro de datos.

Asegurar que los sistemas a ser adquiridos, desplegados y/o mantenidos cuenten con la seguridad requerida para evitar intrusiones y pérdida de información.

Enunciado de la Política

"Los sistemas y aplicativos del centro de datos de la facultad de Ingeniería, deben cumplir con todas las políticas funcionales y procedimientos de seguridad lógica, con el fin de evitar el acceso por personas no autorizadas, daño e interferencia a los recursos de información."

Responsabilidades

Es responsabilidad del director de las carreras de Ingeniería de Sistemas de Información e Ingeniería de Software la aprobación de esta política.

Violaciones a la política

En caso se viole la Política de Seguridad Lógica se dispone de aplicar las siguientes sanciones:

- Suspensión o acceso restringido al data center.
- Reembolso por algún daño causado.
- Suspensión sin pago de salario.
- Demanda civil o penal.

Estas sanciones se encuentran en el Reglamento de Disciplina de la Universidad Peruana de Ciencias Aplicadas.

Conceptos y directrices sobre la Política de Seguridad Lógica

Gestión de Comunicaciones y Operaciones

Se debe asegurar la operación correcta y segura de los recursos que tratan la información. Todos estos recursos deben tener responsabilidades y procedimientos establecidos de modo que las operaciones sean las indicadas y ante incidencias las respuestas sean ejecutadas sin problemas.

Protección contra software malicioso

Los sistemas del centro de datos deben estar protegidos contra software malicioso. Todos los usuarios de los sistemas deben conocer los peligros de este software y los

encargados u administradores de estos deben controlar y prevenir mediante medidas especiales, detectando y evitando su ingreso a los sistemas.

Recomendaciones y controles adicionales:
El Gerente de Seguridad debe implementar procedimientos de recolección de información referido a nuevos virus o software maliciosos.

El Gerente de Seguridad debe solicitar la instalación y actualización cada ciclo de software de detección y reparación de virus. Este software debe tener las opciones para explorar tanto los sistemas del centro de cómputo como los medios externos que estén conectados a estos sistemas. Así también debe contar con la opción de revisión de archivos adjuntos de correos electrónicos. Finalmente debe verificar cualquier código malicioso en las páginas web.

El Gerente de Seguridad debe establecer un plan de continuidad en caso se presente apropiado para la recuperación de ataques de virus. Esto incluye tanto data como software de los sistemas del centro de datos.

Gestión de respaldo y recuperación

Se debe mantener la integridad y la disponibilidad de los sistemas de información. Para esto, se deben establecer procesos rutinarios para generar respaldos hacienda copias de seguridad (backup).

Recomendaciones y controles adicionales:
El DBA debe almacenar los respaldos en una localización diferente a la del centro de datos, a fin de, estos se no se vean afectados a daños en caso se de algún problema o incidente en el centro de datos.

El DBA debe probar los medios de respaldo cada inicio de ciclo de estudios, para que estos sean de confianza en caso de emergencias.

El DBA debe definir el nivel necesario de recuperación de la información.

Se debe comprobar y verificar a cada inicio de ciclo académico que el proceso de recuperación es eficaz y cumple con tiempos dentro de lo aceptable.

Gestión de seguridad en redes

Se debe asegurar la protección de la infraestructura de apoyo e información en las redes.

Recomendaciones y controles adicionales:

El Gerente de Seguridad debe solicitar cada inicio de ciclo académico un reporte de los servicios de red, electricidad y sistemas de ventilación al área de soluciones generales a fin de poder planificar, en caso se necesite, nuevas adquisiciones referidas a estos servicios y además tener un control sobre estos elementos que brindan una protección ambiental al centro de datos.

Utilización de medios de información

Evitar daños a los sistemas del centro de datos causados por medio de información internos como externos, a fin de que no se vea afectada la disponibilidad de estos. Estos medio deben ser controlados y físicamente protegidos.

Recomendaciones y controles adicionales:

Todo medio de información interno debe ser almacenado por medio del Supervisor en los lugares en los cuales el fabricante recomienda.

Todo medio de información externo debe ser registrado al ingresar al centro de datos y previo a realizarse alguna actividad con este, debe ser explorado por el software de detección de virus a fin de evitar daños en los sistemas. Esta actividad debe ser supervisada por el Supervisor.

Monitoreo

Toda actividad de procesamiento de información no autorizada debe ser detectada. Todos los sistemas con los que cuenta el centro de datos deben ser monitoreados por sus respectivos administradores, teniendo siempre un registro de los usuarios y las operaciones que estos realizaron en el sistema, a fin de asegurar la identificación de los problemas.

Recomendaciones y controles adicionales:

El nivel de monitoreo requerido debe ser determinado por una evaluación de riesgos. Los resultados de esta evaluación de riesgos deben ser analizados por el Gerente de Seguridad del centro de datos con el propósito de establecer los procedimientos para el uso del monitoreo.

Los administradores de los sistemas/aplicativos del centro de datos deben monitorear lo siguiente: accesos autorizados, intentos de accesos no autorizados, operaciones privilegiadas, alertas o fallas del sistema y cambio o intentos de cambio en la configuración de los sistemas del centro de datos. Todo esto en base a la evaluación de riesgos previamente analizada por el Gerente de Seguridad.

Control de Accesos

Se debe controlar el acceso a la información de los sistemas del centro de datos. Solo los usuarios con autorización deben de poder acceder a los sistemas del centro de datos indicados.

Requisitos de negocio para el control de accesos

El Gerente de Seguridad debe establecer, documentar y revisar una política de control de accesos basándose en los requerimientos de seguridad de los sistemas del centro de datos. Debe establecer las reglas y derechos de cada usuario o grupo de usuario.

Recomendaciones y controles adicionales:

Esta política debe contemplar: requisitos de seguridad de los aplicativos, información relativa a las aplicaciones y los riesgos de esta información y perfiles de acceso de usuarios estandarizados.

Especificar las reglas a cumplir siempre con las reglas opcionales.

Responsabilidades de los usuarios

Los usuarios de los sistemas del centro de datos deben ser conscientes de sus responsabilidades en el mantenimiento de la eficacia de las medidas de control de acceso en particular respecto al uso de contraseñas y la seguridad del material puesto a su disposición.

Recomendaciones y controles adicionales:

Todos los usuarios deben ser informados acerca de: mantener la confidencialidad de las contraseñas, seleccionar contraseñas de buena calidad con una longitud mínima de caracteres, cambiar las contraseñas en cada cierto tiempo evitando usar contraseñas

antiguas, cambiar las contraseñas temporales que se asigna al ingresar por primera vez al sistema y no compartir contraseñas de usuarios individuales.

Cerrar sesión de los sistemas del centro de datos al terminar de realizar las actividades de turno, evitando dejar sesiones de usuario activas.

Todos los equipos del centro de datos deben protegerse o bloquearse después de estar 5 minutos inactivos de uso. Esto se aplica para todos los equipos sin excepción.

Gestión de acceso de usuarios

Los usuarios adecuados deben tener accesos autorizados a los sistemas de información del centro de datos. Se debe cubrir todo el ciclo de vida de estos accesos, desde el registro inicial hasta la baja de los usuarios que no requieran dichos accesos.

Recomendaciones y controles adicionales:

El Gerente de Proyectos y Recursos debe aprobar el listado de los accesos y contraseñas de los usuarios que se brindan en el ciclo académico en curso.

Se debe brindar identificadores únicos a los usuarios, de esta forma puede vincular a los usuarios y responsabilizarles de sus acciones.

Se debe garantizar que se provea acceso a los sistemas del centro de datos hasta que se complete el proceso de gestión de claves.

La eliminación inmediata de las autorizaciones (claves) de acceso al finalizar el ciclo académico en curso.

El administrador del sistema de información del centro de datos debe realizar una revisión periódica de estos accesos.

Control de acceso a la red

Se debe controlar el acceso a los servicios de red, usando mecanismos adecuados de identificación para los usuarios así también como un control de accesos de los usuarios a los servicios de información.

Recomendaciones y controles adicionales:

Se debe restringir la capacidad de conexión de los usuarios por medio de filtros. Las aplicaciones más comunes a ser restringidas deben ser: correo electrónico, acceso interactivo, acceso a las aplicaciones y transferencia de archivos.

Control de acceso al sistema operativo

Se debe evitar accesos no autorizados a los equipos del centro de datos. Mediante herramientas de seguridad que permitan restringir el acceso a los sistemas de los equipos y también que estas herramientas sean capaces de registrar todas las acciones involucradas con el acceso a los equipo.

Recomendaciones y controles adicionales:

No se deben mostrar mensajes de ayuda durante el proceso de conexión.

Limitar los intentos fallidos de conexión.

No mostrar la contraseña ingresada, de preferencia mostrar caracteres simbólicos.

Se debe restringir los tiempos de conexión, de preferencia si el sistema operativo se encuentra sin actividad por 10 minutos, se debe considerar re-autentificarse después de este tiempo.

Control de acceso a las aplicaciones y la información

Se debe restringir el acceso lógico a los sistemas de aplicaciones solo a los usuarios que cuenten con accesos autorizados. Para esto las aplicaciones del centro de datos deben controlar el acceso de los usuarios a la información, protegerse de accesos no autorizados y no comprometer la seguridad de otros sistemas en caso comparta información.

Recomendaciones y controles adicionales:

Controlar los derechos de acceso de los usuarios y otras aplicaciones (lectura, escritura, borrado y ejecución).

Adquisición y mantenimiento de sistemas

Los sistemas a del centro de datos a ser adquiridos deben tener requisitos de seguridad establecidos por el Gerente de Seguridad, así también contar con controles

criptográficos básicos como es el caso de las claves o contraseñas. Finalmente establecer una gestión de vulnerabilidades técnicas que sea efectiva.

Requisitos de seguridad de los sistemas

Se debe asegurar que los sistemas de información del centro de datos sean seguros, que cuenten con mecanismos de seguridad propios.

Recomendaciones y controles adicionales:

Se debe tener en cuenta que los requisitos y controles de seguridad deben reflejar el valor de los equipos de información, además de, prever el posible daño al centro de datos en caso de fallas o ausencia de seguridad.

En caso de adquirir productos comprados, estos deben ser probados formalmente y contra con un proceso de adquisición. Tener en cuenta los requisitos de seguridad establecidos.

Controles criptográficos

Se debe proteger la confidencialidad, autenticidad e integridad de la información de los aplicativos en el centro de datos.

Recomendaciones y controles adicionales:

Se debe usar sistemas y técnicas criptográficas para proteger la información sometida a riesgo, específicamente en este caso las contraseñas.

Generar claves para distintas aplicaciones.

Almacenar claves, así también en la forma como el usuario la obtuvo.

Cambiar o actualizar las claves así también como los procedimientos para realizar dichas actividades.

Las claves deben ser revocadas al finalizar el ciclo académico. Específicamente las claves de los usuarios no privilegiados de los aplicativos

Seguridad de los archivos del sistema

Se debe asegurar los archivos de los aplicativos de los sistemas del centro de datos.

Recomendaciones y controles adicionales:

El oficial de seguridad debe controlar la instalación de software en los sistemas del centro de datos.

Gestión de la vulnerabilidad técnica

Se debe reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas. Debe establecerse una gestión de vulnerabilidades técnicas de manera efectiva y sistemática con métricas tomadas para confirmar su efectividad.

Recomendaciones y controles adicionales:

Se deben definir los roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas, incluyendo el monitoreo de vulnerabilidades, la evaluación de vulnerabilidades, el parchado y cualquier otra responsabilidad coordinada.

Se debe definir una línea de tiempo para reaccionar ante notificaciones de vulnerabilidades técnicas relevantes.

Los parches deben ser probados y evaluados antes de que sean instalados con el fin de asegurar que sean efectivos. En caso no existan parches, se debe considerar otros controles como apagar los servicios y capacidades relacionadas a la vulnerabilidad y aumento en la precaución de la vulnerabilidad.

Los sistemas en alto riesgo deben ser tratados primero.

Mapeo de procesos con directrices lógicas

	SEGURIDAD LOGICA															
	Gestión de Comunicaciones y Monitoreo					Control de Accesos						Adquisición, Desarrollo y Mantenimiento de Sistemas				
	Protección contra Software Malicioso	Gestión de Respaldo y Recuperación	Gestión de Seguridad en Redes	Utilización de Medios de Información	Monitoreo	Requisitos de Negocios para el Control de Accesos	Responsabilidades de Usuarios	Gestión de Acceso de Usuarios	Control de Acceso a la Red	Control de Acceso al Sistema Operativo	Control de Acceso a las Aplicaciones y la Información	Requisitos de Seguridad de los Sistemas	Controles Criptográficos	Seguridad de los Archivos del Sistema	Seguridad de los Procesos Soporte	Gestión de la Vulnerabilidad Técnica
Administración de Vulnerabilidades y Parches	X										X					
Monitoreo de Componentes				X	X											
Gestión de Solicitud de Accesos Lógico						X	X	X	X	X				X		
Gestión de Pruebas de Seguridad															X	
Restauración de Backup		X														
Control de Vulnerabilidades Técnicas			X													X
Gestión de Claves													X			
Revisión e Instalación de Software												X		X		

Imagen 29: Mapeo de procesos con directrices lógicas

Fuente: Elaboración Propia

Página dejada en blanco intencionalmente

CAPÍTULO 4: CONTINUIDAD Y CIERRE DEL PROYECTO

En el presente capítulo se presentará el resultado del assessment realizado al centro de datos de la carrera de Ingeniería de Sistemas y Software. Por otro lado, se presentará el planteamiento de continuidad del proyecto con el objetivo que este siga a lo largo del tiempo a pesar que los dueños del proyecto no sigan a cargo del mismo. Finalmente, se presentarán las conclusiones a las que se llegó a lo largo de la investigación y del proyecto.

Continuidad del Proyecto

Todo proyecto basado de ITIL tiene que considerar e incluir la mejora continua del proceso. El proyecto Gestión de la Seguridad Física y Lógica no escapa a esta realidad, motivo por el cual se ha diseñado la siguiente estructura para mantener el proyecto a lo largo del tiempo.

- Definir interacciones entre proyectos
- Definir el rol del Oficial de Seguridad
- Assessment de Seguridad
- Crear el manual de responsabilidades del Oficial de Seguridad
- Proceso de Mantenimiento de Políticas y Controles de Seguridad

Interacciones con otros Proyectos

Si se considera que el flujo adecuado del proyecto debe ser el propuesto por Osiatis, se puede apreciar que la Gestión de la Seguridad guarda relación por la Gestión de la Continuidad, Gestión de Cambios, Gestión de Incidentes, Gestión de Configuraciones, Gestión de Capacidad, Gestión de Niveles de Servicio.

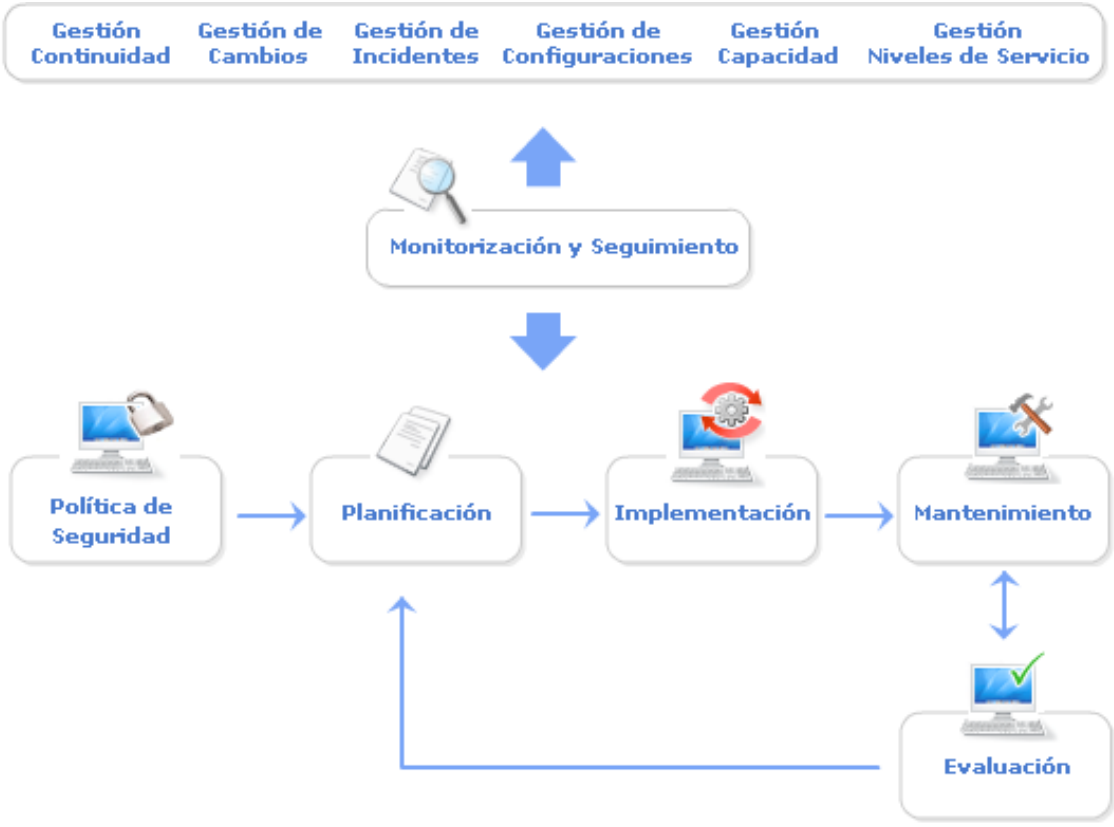


Imagen 30: Procesos ITIL

Fuente: Osiatis.com

Para cada interacción se debe definir cuál es el requerimiento de entrada y salida, al final del análisis el resultado fue el siguiente:

Imagen 31: Procesos ITIL - Primer Nivel

Fuente: Osiatis.com

La Gestión de Niveles de Servicios, nos brinda:

- Los requisitos de seguridad establecidos en los SLA ’s, OLA ’s y UC ’s.

Y el proyecto GSFL apoya en:

- Supervisar el cumplimiento de los mismos.

La Gestión de Incidentes, nos brinda:

- Los incidentes clasificados como incidentes de seguridad.

Y el proyecto GSFL apoya en:

- Recuperar el servicio, con los conocimientos de seguridad que se posee.
- Actualizar la política de seguridad y/o pruebas necesarias para prevenir los incidentes reportados.

La Gestión de la Capacidad, nos brinda:

- La capacidad de los recursos de TI.
- Recursos suficientes para la provisión del servicio de TI.

Y el proyecto GSFL apoya en:

- Enviar métricas para calcular los tiempos de inoperatividad del servicio.
- Actualizar la política de seguridad y/o pruebas necesarias para prevenir tiempos de inoperatividad.

La Gestión de la Problemas, nos brinda:

- Causas de los problemas detectados.
- Solución de los problemas detectados.

Y el proyecto GSFL apoya en:

- Actualizar la política de seguridad y/o pruebas necesarias para prevenir que aparezcan estos problemas.

La Gestión de Cambios, nos brinda:

- Relación de cambios a implementar con un estudio de impacto.
- Y el proyecto GSFL apoya en:
- Aprobación de los RFC.
- Programar pruebas sobre los cambios.
- Analizar criticidad de activos nuevos.

- En conjunto con la Gestión de Continuidad Servicios TI, se elabora el *plan de recuperación y el plan de prevención*

La Gestión de la Seguridad le brinda a la Gestión de Versiones:

- Los requerimientos de seguridad establecidos para cada nivel de servicio.

El Centro de Servicios, nos brinda:

- Los nuevos incidentes de seguridad.
- Protocolos de seguridad que están fallando.

Y el proyecto GSFL apoya en:

- Realizar pruebas de seguridad.
- Actualizar la política de seguridad.

Al finalizar este análisis se puede diagramar el proyecto de Gestión de la Seguridad (considerando la mejora continua) de la siguiente forma:

Imagen 32: Rueda de Continuidad

Fuente: Elaboración Propia

En la fase del mantenimiento se encuentra la mejora continua de la gestión de la seguridad.

Definición de Rol y Manual de Funciones

Información del Rol

Definición

El Oficial de Seguridad es el responsable de asegurar la confidencialidad, integridad y disponibilidad de los activos, información, datos y servicios de tecnología de la información dentro de la empresa IT-Expert y el centro de datos de la carrera Ingeniería de Sistemas de Información.

Usualmente está involucrado con la Gestión de la Seguridad que tiene un alcance más amplio que el de los servicios de TI e incluye manejo de documentos, accesos al centro de datos, entre otros.

Funciones

El Oficial de Seguridad dispone de funciones en los diferentes procesos diseñados e implementados por el proyecto GSFL, a continuación se mostrará estas funciones por proceso:

Proceso Control de ingresos

El oficial de seguridad debe asegurarse que los ingresantes al centro de datos cumplan con ciertos requisitos dependiendo si tienen permisos de ingreso o no, como por ejemplo, presentación de DNI/TIU, presentación de permiso de autorización de ingreso y presentación de permiso de ingreso de dispositivos tecnológicos, también asegurarse de registrar cualquier tipo de dispositivo tecnológico que este ingresando con el ingresante confiscando aquellos no permitidos y registrando aquellos que no están permitidos. Finalmente debe registrar la información del ingresante como: nombre, DNI, Código del TIU Universitario, fecha, hora de ingreso, hora de salida, cantidad de dispositivos tecnológicos, detalle de los dispositivos tecnológicos y duración de visita.

Proceso Revisión de Equipos

El proceso de Revisión de Equipos se inicia cuando el Oficial de Seguridad de turno debe realizar según el cronograma la revisión de equipos del centro de datos. Dentro de esta actividad el oficial de seguridad verifica si se ha retirado algún equipo sin autorización así como también si se necesita desasignar algún equipo del cuál su garantía este por expirar. En caso de pérdida el oficial de seguridad debe comunicar al jefe de supervisores este tema siendo el mismo jefe el que verifique revisando reportes generales de revisión de equipos pasados en caso haya habido una equivocación por parte de alguno de los supervisores que realizaron los reportes pasados; si no es así entonces realiza un informe para el área de seguridad de la universidad con el fin de que investiguen sobre el extravío del equipo. Por otro lado, en el caso de una des asignación, el oficial de seguridad debe realizar una solicitud al administrador del centro de datos para que este de su conformidad respecto del equipo o equipos a ser desafectado o desafectados.

Proceso Control de Protección Ambiental

El proceso de Control de Protección Ambiental se inicia cuando el Administrador del centro de datos después de revisar su cronograma envía la solicitud a un operador de servicios generales para que este inspeccione los suministros de energía que corresponden al edificio donde se encuentra ubicado el centro de datos. Este una vez que realiza la inspección envía al oficial de seguridad un reporte con los resultados de ésta en la cual también incluye observaciones y/o incidencias. Luego de recibir dicho reporte el Administrador del centro de datos procede a enviar una solicitud al supervisor de turno del centro de datos para que este realice un reporte respecto a cómo ha estado protegida las instalaciones del centro de datos especificándose si se registró alguna incidencia desde el último reporte realizado. El oficial de seguridad envía el reporte al Administrador del centro de datos. Éste analiza ambos reportes recibidos y realiza su reporte de incidencias el cual es un resumen de ambos reportes. Este reporte es enviado al director de la carrera de Ingeniería de Sistemas de Información el cuál después de revisarlo analiza los resultados y envía al gerente de seguridad un documento donde especifica las observaciones y/o requerimientos que hay que realizar para poder mejorar tanto el suministro de energía como la protección de las instalaciones.

Proceso Revisión e instalación de software

El proceso de Revisión e instalación de software se inicia cuando nace una solicitud de parte de un recurso de la empresa virtual IT-Expert tiene la necesidad de instalar un aplicativo, por lo que envía una solicitud en donde detalla la información del aplicativo. Esta solicitud es enviada a Service Desk donde se atiende y se valida el formato de ésta. En caso la validación sea correcta, la solicitud es enviada al Oficial de Seguridad el cual se encargará de evaluar y validar la información del software a ser instalado así como también ver si es factible la instalación del mismo en el centro de datos, reuniéndose con el recurso de la empresa virtual para afinar detalles sobre la instalación del aplicativo. El oficial de seguridad luego de que el recurso de la empresa verifique que se ha instalado correctamente procederá a registrar dicho software en la Bases de datos donde se registran la información de los aplicativos del centro de datos. Se registra: nombre, siglas, sistemas operativos con los que trabaja, tamaño, funcionalidad, problemas de instalación (en caso sucedió), fecha de instalación, duración de la instalación, responsable de la instalación y responsable del aplicativo.

Proceso Control de Vulnerabilidades Técnicas

El proceso de Control de vulnerabilidades técnicas se inicia cuando el oficial de seguridad define los roles y responsabilidades en base a los diferentes sistemas y aplicativos desplegados en el centro de datos de la carrera. Una vez definido esto se envía el documento al Gerente General y este lo delega al Gerente de Proyectos y Recursos para que este asigne dichos roles entre los recursos de la empresa virtual IT-Expert. El recurso envía su conformidad al Gerente de Proyectos y Recursos, el cuál será revisado por este y enviado de vuelta al oficial de seguridad para que este defina la línea de tiempo, evaluación de parches y determine el monitoreo y evaluación de las vulnerabilidades con cada recurso responsable por los sistemas del centro de datos.

Proceso Gestión de Claves

En este proceso, el oficial de seguridad tiene que realizar las revisiones de que las claves están cumpliendo con las políticas de la seguridad lógica establecidas para el centro de datos.

Proceso Gestión de Solicitud de Accesos

El proceso de Gestión de Solicitud de Accesos se inicia cuando el Gerente de Proyectos y Recursos IT-Expert de la empresa IT-Expert solicita a cada gerente de recursos de las

empresas virtuales la relación de alumnos que deben contar con acceso al centro de datos por pertenecer a los cursos de Taller de Desempeño 1, Taller de Desempeño 2, Taller de Proyectos 1 y Taller de Proyectos 2. Luego, esta lista debe ser revisada por el Gerente Proyecto y Recursos, el mismo que visa la relación y solicita su atención por parte del Oficial de Seguridad de IT-Expert. Posterior a ello, el Gerente de Seguridad de IT-Expert procede a revisar la lista, tramita y notifica los cambios.

Proceso Gestión de solicitud de respaldo de información

El proceso de Gestión de Solicitud de Respaldo de Información inicia cuando el gerente de proyectos y recursos de la empresa IT-Expert solicita la creación de los archivos de respaldo, esta solicitud puede ser de respaldo de base de datos o de archivos en la carpeta del file server de cada empresa. El oficial de seguridad recibe la solicitud y determina cuál es el tipo de solicitud y procede a crear los archivos de respaldo, resguardando estos en una carpeta asignada para cada tipo de respaldo.

El alcance que tiene las copias de seguridad se limita únicamente a la información que se encuentre en el centro de datos de la carrera de Ingeniería de Sistemas y Software de la UPC, es decir bases de datos en los ambientes de producción y archivos en el file server. Luego, esta lista debe ser revisada por el Gerente General de la empresa, el mismo que visa la relación y solicita su atención por parte de IT-Expert. Posterior a ello, el Gerente de Proyectos y Recursos procede a revisar la lista y solicita al alumno encargado que tramite y notifique los cambios.

Proceso Administración de Vulnerabilidades y Parches

El proceso de Administración de Vulnerabilidades y Parches inicia cada tres semanas cuando se realiza una revisión de cuáles son las actualizaciones que se encuentran en estado pendiente. Este proceso interactúa con la el análisis de vulnerabilidades que se lleva a cabo en otro proyecto de la empresa IT-Expert. El oficial de Seguridad se encarga de identificar vulnerabilidades, analizar las vulnerabilidades identificadas y luego comunicarse con el Gerente de Procesos y Recursos para poder implementar parches.

Al ser implementados estos parches se encarga de monitorear durante 3 semanas el aplicativo para asegurarse que no se ha afectado el correcto funcionamiento de los

sistemas y servicios. En caso de encontrar fallas se deshacen los cambios por medio de un rollback. Si después del monitoreo todo fue correcto, se enviará un reporte al Gerente de Proyectos y Recursos.

Proceso Gestión de Solicitud de Procesos Lógicos

El proceso de Gestión de Solicitud de Accesos se inicia cuando el gerente de recursos de cada empresa virtual genera la relación de alumnos de su empresa que deben tener acceso a las carpetas de cada empresa. Los únicos alumnos que deben tener acceso a dichas carpetas son los alumnos de Taller de Desempeño 1, Taller de Desempeño 2, Taller de Proyectos 1 y Taller de Proyectos 2. Luego, esta lista debe ser revisada por el Gerente General de la empresa, el mismo que visa la relación y solicita su atención por parte de IT-Expert. Posterior a ello, el gerente de proyectos y recursos de IT-Expert revisan la lista y solicita al alumno encargado que tramite y notifique los accesos solicitados.

Proceso Monitoreo de Componentes

El oficial de Seguridad se encarga del proceso de Monitoreo de Componentes. Este inicia cada tres semanas durante el horario de talleres de proyecto (Lunes 4-7 pm y miércoles de 4-7). Este proceso tiene que evaluar cada uno de los componentes del centro de datos de la carrera.

Proceso Gestión de Pruebas de Seguridad

El proceso de Gestión de Pruebas de Seguridad inicia cada primer día hábil de cada trimestre del ciclo académico. Es aquí cuando el Oficial de Seguridad revisa la bitácora de errores para determinar si han surgido nuevos incidentes que deben ser derivados a la Gestión de Problemas para que esta pueda determinar cuál es la causa del mismo y así aplicar las medidas correctivas necesarias.

El alcance de las pruebas se limita únicamente a los componentes que se encuentren dentro del centro de datos de la carrera de Ingeniería de Sistemas de Información. Las pruebas que se llevarán a cabo han sido determinadas mediante un análisis de seguridad y en estas se deben obtener los siguientes indicadores:

- Número de nuevos incidentes.
- Número de incidentes repetitivos.
- Número de incidentes detectados.

Al final de proceso el Oficial de Seguridad se encarga de notificar al Gerente General de IT-Expert sobre las nuevas incidencias encontradas para que esté al tanto de las mismas y de los posibles riesgos inherentes a estas fallas.

Proceso de Restauración de Backup

El proceso de restauración de backup inicia cuando le llega al gerente de proyectos y recursos de la empresa virtual IT-Expert una solicitud de restauración de archivos de respaldo. El gerente debe validar y verificar que la solicitud cumpla con los requisitos mínimos para ser atendido. El oficial de seguridad determina qué tipo de solicitud es, es decir si se trata de la restauración de una base de datos o de algún archivo del file server respaldado. El oficial de seguridad debe notificar a la gestión de problemas si se presenta algún problema del cual no tiene conocimiento ni información disponible a lo largo del proceso. Finalmente, el oficial de seguridad envía el informe de restauración para dar por finalizado el proceso.

Proceso Control de Vulnerabilidades Técnicas

El proceso de Control de vulnerabilidades técnicas se inicia cuando el gerente de seguridad define los roles y responsabilidades en base a los diferentes sistemas y aplicativos desplegados en el centro de datos de la carrera. Una vez definido esto se envía el documento al Gerente General y este lo delega al Gerente de Proyectos y Recursos para que este asigne dichos roles entre los recursos de la empresa virtual IT-Expert. El recurso envía su conformidad al Gerente de Proyectos y Recursos, el cuál será revisado por este y enviado de vuelta al gerente de seguridad para que este defina la línea de tiempo, evaluación de parches y determine el monitoreo y evaluación de las vulnerabilidades con cada recurso responsable por los sistemas del centro de datos.

Assessment de Seguridad

Con el objetivo verificar que los cambios sugeridos por el proyecto se hayan llevado a cabo, que se estén cumpliendo las políticas, las recomendaciones y se respeten los

niveles mínimos requeridos se ha creado un listado de preguntas para que sirvan como assessment de la gestión de la seguridad en el centro de datos. Al mismo tiempo, esta evaluación ayuda a que ciclo a ciclo se retroalimente la gestión de la seguridad con los resultados de las evaluaciones, los resultados de las incidencias, los nuevos requerimientos y los nuevos riesgos detectados.

El assessment se diseñó a partir de diversas recomendaciones de seguridad, las mismas que se encuentran en las diversas fuentes bibliográficas consultadas por el proyecto.

Assessment de Seguridad.

Control	Si	No	N/A	Comentarios
¿Existen métodos físicos para prevenir el acceso no autorizado a la información?	Ξ			
¿Existen métodos para prevenir que las personas dañen información?			Ξ	No existe un área de procesamiento de información al interior del centro de datos.
¿Existen métodos físicos para prevenir que las personas interfieran con la información?			Ξ	No existe un área de procesamiento de información al interior del centro de datos.
¿Se tiene la información sensible y crítica de la organización en un área asegurada?	Ξ			
¿Se han definido perímetros de seguridad para proteger información sensible y crítica?	Ξ			
¿Se utilizan controles de entrada para	Ξ			

proteger la información sensible y crítica?			
¿Se toma en cuenta los riesgos de seguridad y se aseguran los perímetros de seguridad en realidad para reducir el riesgo de seguridad?	Ξ		
¿Toman en cuenta la seguridad de los requisitos de los activos de información y se aseguran de cumplimiento?	Ξ		
¿Se puede reducir el riesgo y cumplir con los requisitos de seguridad, asegurando que los perímetros de seguridad son lo suficientemente fuertes?		Ξ	Se pueden implementar más mejoras a nivel físico incurriendo en costo.
¿Las barreras de seguridad física y perímetros libres de no tienen carencias físicas ni debilidades?		Ξ	Se debe implementar mejores barreras pero esta implementación incurre en costo.
¿Sus sistemas de detección de intrusos cubren todos centros de comunicaciones y	Ξ		El control viene dado por el encargado del

las salas de informática?			centro de datos
¿Sus sistemas de detección de intrusos cumplir con todas las normas regionales, nacionales o internacionales?		Ξ	
¿Utiliza con llave para proteger a las oficinas de su organización la información y la información de las instalaciones de procesamiento		Ξ	No se cuenta con área de procesamiento de información, sin embargo, el acceso al centro de datos es controlado por el staff y siempre se encuentra bajo llave.
¿Registra la fecha y hora los visitantes entrar o salir de las zonas seguras?	Ξ		Se ha diseñado una base de datos que contiene esta data
¿Se supervisa a todos los visitantes a las zonas seguras a menos que su acceso fue previamente aprobado?	Ξ		El encargado del centro de datos debe permanecer durante la presencia de personal externo.
¿Se permite el acceso a áreas seguras sólo si el acceso ha sido autorizado y los visitantes tienen una específica razón por	Ξ		Los únicos que pueden brindar acceso son los gerentes generales de cada empresa virtual.

la cual deben tener acceso			
¿Utiliza los controles de autenticación (por ejemplo, control de acceso tarjeta y el PIN) para validar y autorizar el acceso?		Ξ	
¿Mantiene registros de seguridad de todos los accesos a las zonas seguras	Ξ		Se guarda un historial de los accesos (entrada y salida)
¿Revisa los derechos de acceso a las áreas de seguridad de forma regular?	Ξ		Antes de brindar accesos se debe comprobar que los accesos hayan sido otorgados a la persona que desee ingresar.
¿Se actualiza los derechos de acceso a las áreas de seguridad de forma regular	Ξ		Existe un proceso que se encarga del mantenimiento de los accesos tanto físicos como lógicos.
¿Se revocan los derechos de acceso a las áreas de seguridad en caso sea necesario hacerlo?	Ξ		Cada ciclo se revoca los accesos para que sean tramitados nuevamente.
¿Utiliza métodos físicos para proteger sus		Ξ	Se ha recomendado implementar CTVC para

instalaciones de los daños que causados por el hombre pueden causar		detectar cambios de temperatura abruptos dentro del centro de datos.
¿Utiliza métodos físicos para proteger sus instalaciones de los daños que pueden causar incendios?	Ξ	Se ha recomendado implementar alarmas para detectar cambios de temperatura abruptos dentro del centro de datos.
¿Cómo se protegen sus instalaciones de los daños fuga de agua desde el techo, desde abajo, o de la oficina de al lado podría causar?	Ξ	Se ha recomendado implementar sensores de humedad y fuga de agua a fin de evitar que esto afecte el funcionamiento del centro de datos. Cabe resaltar que el mantenimiento de las instalaciones agua/desagüe depende única y exclusivamente de Servicios Generales.
¿Cómo se protegen sus instalaciones de los daños un incendio en un edificio vecino podría causar?	Ξ	No existen instalaciones alrededor
¿Usted supervisará todas las actividades en las áreas de seguridad?	Ξ	El personal encargado del centro de datos debe verificar todas las actividades realizadas dentro

			de este.
¿Cómo se previene el uso no autorizado de equipo de video dentro de las áreas de seguridad?	Ξ		Se supervisan todas las actividades desarrolladas dentro del centro de datos.
¿Se tiene el control de puntos de acceso público a fin de evitar personas no autorizadas?		Ξ	Las personas externas a la universidad solo pueden ingresar con autorización de servicios generales y siempre bajo la supervisión del encargado del centro de datos.
¿Se previene de daños a los equipos de su organización?	Ξ		Se ha diseñado el proceso de Revisión de Equipos para evitar este tipo de inconvenientes. Cabe mencionar que el mantenimiento no puede ser modificado por el proyecto ya que está a disposición de Servicios Generales y el área de sistemas de la universidad.
¿Cómo se previene la pérdida de los equipos de su organización?	Ξ		No se puede retirar ningún equipo del centro de datos sin la autorización del área de sistemas y/o director de la carrera.

¿Cómo se previene el robo de equipo de su organización?	Ξ		No se puede retirar ningún equipo del centro de datos sin la autorización del área de sistemas y/o director de la carrera.
¿Se protegen los equipos contra amenazas físicas?	Ξ		Toda actividad es supervisada por el encargado del centro de datos.
¿Se protegen los equipos contra las amenazas ambientales?	Ξ		Se ha diseñado el proceso Control de Protección Ambiental.
¿Cómo se protege su equipo para evitar interrupciones en el trabajo?	Ξ		Se tiene un generador de respaldo que brinda energía de respaldo a todo el pabellón donde se encuentra el centro de datos, sin embargo, se está recomendando que se instale y compre un UPS y un generador para el centro de datos.
¿Es usted el proteger a su equipo a través de la eliminación adecuada?	Ξ		Se ha especificado en la política cuál es el procedimiento correcto para desechar equipos.
¿Utiliza los controles especiales para proteger las instalaciones de apoyo?		Ξ	No existen instalaciones de apoyo.

¿Se utilizan controles para minimizar los riesgos de radiación electromagnética?		Ξ	
¿Se protegen los equipos ante descargas eléctricas de rayos?		Ξ	
¿El equipo de aire acondicionado instalado en el centro de datos cubre la demanda del mismo?	Ξ		En la evaluación realizada se detectó que el aire acondicionado no cumple con los requerimientos mínimos por la TIA para alcanzar el nivel adecuado, motivo por el cual se ha recomendado la adquisición de uno nuevo.
¿Los lideres o personal de seguridad de información dentro de la organización tienen la experiencia y habilidades necesarias?	Ξ		El personal contratado ha sido evaluado para cubrir la plaza y tiene conocimiento de las funciones que le corresponden y cuáles son sus responsabilidades.
¿Existe una persona u área dentro de la organización que tengo como tarea principal la seguridad de información?	Ξ		Se ha creado un rol dentro de la organización llamado oficial de seguridad, este rol va acorde a las sugerencias de ITIL.

¿Las funciones de seguridad de información tiene la autoridad necesaria para gestionar y asegurar el cumplimiento acorde al plan de seguridad?		Ξ	Debido a la interacción con Servicios Generales y el área de sistemas de la universidad, se deben respetar las autonomías y los límites establecidos por ellos.
¿Las funciones de seguridad de información tienen los recursos necesarios para gestionar y asegurar el cumplimiento acorde al plan de seguridad?		Ξ	El oficial de seguridad no cuenta con presupuesto para realizar cambios masivos y/o requeridos por el centro de datos.
¿La responsabilidad de cada agrupación de componente claramente asignada, arquitectura, redes, comunicaciones, procesos y auditoria?		Ξ	No se tiene información sobre los límites entre Servicios Generales y el área de Sistemas de la Universidad.
¿Se reporta constantemente la función de la seguridad de información a los líderes de la empresa?	Ξ		
¿La organización tiene documentación sobre los aspectos de la seguridad de	Ξ		

información?			
¿La organización tiene identificados los activos críticos y las funciones que dependen de ellos?	Ξ		
¿Se tiene redactada una estrategia de seguridad de información?	Ξ		
¿Se han asignado costos a cada activo por perdidas de los equipos?		Ξ	No se ha tenido acceso al costo de cada activo.
¿La estrategia de seguridad tiene definida un de revisión y actualización periódica?	Ξ		

Tabla 55: Assessment de Seguridad

Fuente: Elaboración Propia

CONCLUSIONES

Tal como se analizó en el primer capítulo, una vez concluida la evaluación se puede determinar que los niveles de seguridad del centro de datos salieron con un puntaje inferior al deseado. Al mismo tiempo, en cada aspecto evaluado se encontró por lo menos una característica no atendida lo que evita que se le pueda asignar el nivel Tier2.

El en capítulo uno, se concluyó que el estándar TIA 942 y las recomendaciones brindadas por el Orange Book son muy ambiciosas para el centro de datos analizado, motivo por el cual, se crearon checklist (físico/lógico) para alcanzar un nivel mínimo recomendable. Si se establece que el estado óptimo es el recomendado por estas fuentes se incurriría en un costo superior al millón de dólares americanos.

Como se afirmó en el primer capítulo después de realizada la evaluación e interpretación de TIA 942, se puede afirmar que dicho estándar no es suficiente para representar el verdadero estado de un centro de datos, debido al alto grado de especialización en la seguridad física y su baja gestión de la seguridad lógica. No obstante, a partir de esta publicación se puede obtener los mejores estándares de seguridad física y ser complementados con otros que se enfoquen en la seguridad lógica.

Tal cual se demostró en evaluación de seguridad lógica, no existe documentación sobre ninguna de las responsabilidades de los encargados del centro de datos.

No existe una clara segregación de funciones entre el personal encargado del centro de datos y área de sistemas de la universidad.

Como quedó demostrado al revisar las mejores prácticas de gestión de la seguridad, es necesario definir los procesos que se encargan de manejar la seguridad a nivel físico y lógico con las directrices de seguridad.

Al revisar toda la documentación que ha sido utilizada para la construcción de este proyecto, se puede concluir que no existe un único estándar que asegure una gestión adecuada de la seguridad. Sin embargo, de cada uno de estos se puede rescatar cada

requisito y formar un estándar que conlleve a una gestión global de la seguridad en un centro de datos.

RECOMENDACIONES

En el capítulo 3, luego de realizar la interpretación de resultados de la evaluación física del centro de datos se detectó que, éste, debe invertir en la compra e implementación de activos que brinden soporte a la seguridad a nivel físico. Las vulnerabilidades detectadas pueden ser cubiertas mediante la adquisición.

En base a lo desarrollado en nuestro proyecto en lo que respecta a seguridad lógica, es posible desarrollar aplicativos específicos para el tema desarrollado. Estos pueden ser futuros proyectos de tesis para los alumnos de Ing. De Software dentro del centro de estudios.

Lo desarrollado en este documento puede ser usado para evaluar un centro de datos cualquiera, por otro lado la política desarrollada y los procesos establecidos si pueden ser aplicados en centro de datos dentro de un centro de estudios mientras que el resultado de la evaluación sea un nivel TIER 1.

El centro de datos debe realizar evaluaciones al inicio de cada ciclo, debido a que a lo largo del tiempo se van implementando cambios por los proyectos vigentes.

El centro de datos debe establecer un benchmarking con una periodicidad establecida (no mayor a un año), comparándose contra instituciones estatales y bancarias debido a que éstas son las que más se han enfocado en el desarrollo de la gestión de la seguridad.

Se recomienda para futuros proyectos intentar acceder a la información de la infraestructura del centro de datos que administra actualmente el área de servicios generales, ya que con esa información se podría brindar recomendaciones según los estándares a implementar y modificar el diseño de la misma.

BIBLIOGRAFÍA

DELTA ASESORES (2011) Métricas de Proyectos
http://www.deltaasesores.com/articulos/autores-invitados/iaap/3009-metricas-en-proyectos
(Consulta: 04 de Abril del 2011)

ENTERPRISE UNIFIED PROCESS (EUP)
2009 (http://www.enterpriseunifiedprocess.com/)
(Consulta 13 de abril 2011)

INDECOPI (2007) EDI. Tecnología de la información. Código de buenas prácticas para la gestión del a seguridad de información. Lima, Perú

Institute Technology Infrastructure Library (ITIL) (2007) ITIL Overview and Benefits (Consulta 13 de abril 2011)
(http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx)

MOLINAS, Lucio (2011) Seguridad
http://www.pol.una.py/descargas/category/35-4.html?download=317%3A.-.
(Consulta: 04 de Abril del 2011)

REAL ACADEMIA ESPAÑOLA DE LA LENGUA
http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=estándar
(Consulta: 04 Abril del 2011)

OSIATIS (2011) ITIL-Gestión de Servicios TI (consulta 14 de abril de 2011) (http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_seguridad/vision_general_gestion_de_la_seguridad/vision_general_gestion_de_la_seguridad.php)

QUALITAS (2011) ISO 27001
(consulta 15 de abril de 2011) (http://qualitas.com.pe/normas/iso-27001)

RODRÍGUEZ Cuervo, Alejandro (2011) Acercamiento al surgimiento y desarrollo de la seguridad informática.
http://revista.iplac.rimed.cu/index.php?option=com_content&task=view&id=201&Itemid=29
(Consulta: 04 de Abril del 2011)

TE CONNECTIVITY (2011) TIA-942 White Paper - Data Centre Standards Overview
http://www.adckrone.com/eu/en/webcontent/support/PDFs/enterprise/Generic/102264BE.pdf
(Consulta: 04 de Abril del 2011)
Telecommunications Industry Association (TIA) (2005) TIA-942 Telecommunications Infrastructure Standard for Data Center. Arlington, U.S.A

UNIVERSIDAD DE CIENCIAS EXACTAS Y NATURALES Y AGRIMENSURA (2011)
¿Qué es seguridad?
http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/SEGUNIX012.htm
(Consulta: 04 de Abril del 2011)

UNIVERSIDAD DE VALENCIA (2011) Instalación y configuración segura de sistemas Unix
http://www.uv.es/sto/cursos/icssu/html/ar01s04.html
(Consulta: 04 de Abril del 2011)

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA (2011) Texto - Guía: Organización, Dirección y Administración de Centros de Cómputo
http://www.utpl.edu.ec/eva/descargas/material/184/G18901.6.pdf
(Consulta: 04 de Abril del 2011)

ANEXOS

ANEXO 1

Gestión De Seguridad Física y Lógica para un Centro de Datos

Project Charter

Especialidad	**Vacante(s)s/Nombres**
Ing. Sistemas de Información	2
Ing. De Software	0

Historial de revisiones			
Versión	***Fecha***	***Autores:***	***Descripción del cambio***
1.8	09/04/2011	Gino Puppi B. Jack Flores E.	Desarrollo del Project Charter

Uno de los principales problemas que acontece a los alumnos que forman parte de las empresas virtuales, es el hecho de no poder acceder al centro de cómputo y/o no contar con los niveles de acceso correspondientes a nivel BD, aplicaciones y SO.

Con el objetivo de brindar una solución a esta problemática, se concibió el proyecto "Gestión de la Seguridad Lógica y Física", el cual tiene como principal objetivo el crear un estándar a utilizar en el centro de cómputo de la carrera.

El proyecto tiene sus ejes centrales en el uso de estándares internacionales y nacionales como la TIA 942 y la NTP 17799.

Al finalizar el proyecto, se logrará diseñaran y definirán los procesos y el estándar adecuado para el centro de datos.

Objetivos del negocio

El objetivo principal de IT-Expert es administrar los recursos tecnológicos de las carreras de Sistemas de Información y de Software brindando servicios tecnológicos de manera efectiva para la gestión adecuada de la información de las empresas virtuales de la UPC, así como la adecuada asesoría y/o consultoría en los temas de su competencia.

Objetivo General

Diseñar los procesos, controles y procedimientos (estándar) para gestionar la seguridad física (seguridad ambiental, control de acceso, monitoreo, estándares, etc.) y la seguridad lógica (permisos en aplicativos, compartidos, bases de datos, roles, etc.) en el centro de cómputo de la carrera.

Objetivos específicos

O.E.1: Evaluar el estado actual del Centro de cómputo de la carrera.

O.E.2: Definir los procesos que regirán a la gestión de seguridad lógica y física para las empresas virtuales.

O.E.3: Integrar los conceptos de la NTP 17799 y la TIA 942, para la creación de un estándar a usar en el centro de cómputo de la carrera.

Indicadores de éxito

I.1: Aprobación del estándar de seguridad lógico y físico para el centro de datos y los laboratorios por parte de un especialista en el campo de TI.

I.2 Certificado de calidad emitido por la empresa QA evidenciando la conformidad con la documentación sobre los procesos sugeridos.

I.4 Conformidad por parte de los gerentes generales de las empresas virtuales acerca de los procesos definidos para la gestión de la seguridad física y lógica.

Alcance del proyecto

El alcance del proyecto incluirá:

- Evaluación de la situación actual del Centro de datos de la carrera con base en los niveles del Tier.
- Sugerencia de las implementaciones necesarias en el Centro de datos la carrera para lograr el nivel 2 de Tier.
- Desarrollo de los diagramas de procesos y diagrama de primer nivel acordes al EBM.
- Definición de controles que deben cumplirse para llegar al TIER determinado y no generen conflictos con los sistemas desplegados.
- Creación de un estándar personalizado, para el control de la seguridad lógica y física en las empresas virtuales.
- El proyecto solo involucrará al centro de cómputo y laboratorios de la carrera de Ing. De Sistemas de Información y Software.
- Al finalizar el proyecto se realizará una encuesta con el objetivo de determinar el nivel de satisfacción de los usuarios respecto a la seguridad del sistema.

El Alcance del proyecto NO incluirá:

- La creación de un software.
- La adquisición o implementación de algún componente de hardware o software.

  El comité de proyectos asignará un asesor especialista en IT, el cual guiará el desarrollo del proyecto y compartirá sus conocimientos sobre tecnologías de información y en base a estos conocimientos se basarán los entregables del presente proyecto.
- Se contará con el apoyo de alumnos de Taller de Desempeño Profesional 1 y 2.
- Se contará con el apoyo de la empresa QA para el aseguramiento de la calidad de los entregables según los plazos pactados por ambas partes.
- No se podrá modificar las fechas de entrega determinadas por el comité de proyectos.
- No se contará con recursos de QA capacitados disponibles para validar el estándar creado.
- No se cuenta con presupuesto aprobado para este proyecto.

Equipo del proyecto

Comité de proyectos	Jorge Cabrera Berrios; Rosario Villalta Riega María Hilda Bermejo; Carlos Raymundo
Gerente General IT-Expert	William Romero
Jefe de proyecto	Gino Puppi B.
Equipo del Proyecto	Jack Flores E.
Equipo de Apoyo	Recursos por parte de la empresa IT-Expert Recursos validadores de la empresa QA.

Stakeholder	Descripción	Tipo	Impacto	Acción
Comité de Proyectos	Son los encargados de aprobar el proyecto, brindan las pautas sobre las cuales se debe llevar a cabo.	Externo	Alto	Mantener Contacto
William Romero	Gerente de IT-Expert, brinda los requerimientos claves acerca del proyecto.	Interno	Alto	Mantener Contacto
Encargados del Proyecto	Alumnos que brindarán toda la información acerca del proyecto.	Interno	Alto	(No Aplica)
Usuarios	Alumnos matriculados en los talleres de desempeño y proyecto	Externo	Bajo	Monitorear
Luis Mamani	Es el encargado de brindar sugerencias en base a su experiencia para ser aplicadas en el proyecto.	Interno	Medio	Mantener Informado
Gerente del Proyecto	Es el actor principal del proyecto, se encarga de manejar la información y controlar el cumplimiento de los requerimientos de los clientes.	Interno	Alto	Mantener Contacto
Empresa QA	Es la encargada de asegurar el nivel de calidad del proyecto, inspeccionando los documentos relacionados a este.	Externo	Medio	Mantener Informado
Encargados del Centro de Computo	Son los encargados de administrar el Data Center.	Externo	Bajo	Monitorear

Se ha determinado que para los Stakeholders que tienen un impacto “Alto” se ha a seguir una estrategia de contacto continuo, ya que estos tienen un gran poder e interés dentro del proyecto. Por otro lado, para los Stakeholders de impacto “Medio” se va a seguir una estrategia de mantenerlos informados, puesto que estos tienen un gran poder pero un interés bajo. Finalmente, con los Stakeholders que tienen un impacto “Bajo” se va a seguir una estrategia de monitoreo ya que de ellos se va a extraer información relevante al proyecto pero estos no tienen ni poder ni interés en el mismo.

Fases	Actividades	Duración (Sem)
0 Planificación	**Formulación y Aprobación del Charter del Proyecto.**	1
	Evaluar las condiciones del Centro de Computo de la Carrera (Nivel Físico). Evaluar los servidores (capacidad, tiempo de respuesta, procesador, etc.). Evaluar los laboratorios destinados a proyecto (modem, router, PC). Validación de los estándares utilizados para el control de accesos y centro de computo.	3
	Generar el reporte de Incidencias y estado final del sistema.	
	Presentación avance del proyecto a la fecha.	1
1 Seguridad Física	Diagramar/Modelar los procesos existentes sobre la seguridad lógica y física del sistema.	2
	Realizar un checklist entre lo recomendado por la norma TIA y lo presente en el sistema (Data Center, Laboratorios).	1
	Diseñar nuevos procesos y optimizar los necesarios para que soporten la metodología de trabajo de la empresa.	2
	Creación de los diagramas para los procesos de la Gestión Seguridad Lógica y Física..	1
	Enviar a QA los procesos que serán validados .	2
	Elaboración de la memoria parcial del proyecto.	2
2 Seguridad Lógica	**Elaboración y presentación del plan de trabajo.**	1
	Evaluar los productos software ya desplegados y los que se encuentren la cartera de proyectos del ciclo para determinar el impacto y las limitantes que plantean sobre los controles de seguridad en el centro de computo.	2
	Visión general del diseño, Infraestructura del distema de cableado.	1
	Topologías y espacios de telecomunicaciones y Sistema de cableado en el data center y exteriores.	1
3 Assesment y Cierre del Proyecto	Presentación del avance del proyecto a la fecha.	1
	Actualización de un estándar para el centro de computo y los diagrama de procesos.	2
	Elaboración de la memoria final del proyecto. **Actualizar estándar a su última versión.**	2
	Presentación final de la memoria del proyecto.	1

* Hitos y entregables en color gris

Enfoque de Trabajo

Se han considerado cuatro fases que se respetarán y guiarán el desarrollo del presente proyecto: *Evaluación del Sistema, Definición de Procesos, Diseño de las Directivas y Cierre de Proyecto.*

En la fase de *Evaluación del Sistema,* se evaluará al sistema actual (centro de cómputo y laboratorios) para determinar en qué nivel de seguridad se encuenta.

En la fase *Definición de Procesos,* se diseñaran los procesos actuales y/o se crearan los procesos necesarios para dar soporte a la gestión de seguridad.

En la fase de *Diseño de las Directivas,* se evaluará las restricciones impuestas por los proyectos desplegados y se diseñaran todos los controles de acuerdo al estándar TIA 942 y la NTP 17799.

En la fase Cierre del Proyecto, se realizará la entrega del informe final al Comité Organizativo para su sustentación del proyecto.

Riesgos

El contrato de validación y verificación firmado con QA caduque antes del fin de la inspección y de las pruebas.

La inspección y pruebas realizadas por parte de QA sean incorrectas.

Disponibilidad de tiempo de los usuarios finales, para las reuniones de captura de requerimientos (niveles de seguridad, accesos, roles, etc.) y reuniones de control del avance del proyecto.

La aceptación o continuidad del proyecto estará a cargo del comité de proyectos.

Los Stakeholders no definan las expectativas de los requerimientos mínimos.

Aprobación IT-Expert	**Comité de proyectos**			**Fecha**

ANEXO 2

GESTIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA

Plan de Proyecto

Sección 1. Resumen del Proyecto

Descripción del Proyecto

Uno de los principales problemas que acontece a los alumnos que forman parte de las empresas virtuales, es el hecho de no poder acceder al centro de cómputo y/o no contar con los niveles de acceso correspondientes a nivel BD, aplicaciones y SO. Al mismo tiempo no se tiene la seguridad que sus proyectos son resguardados bajo algún criterio o parámetro de seguridad.

Con el objetivo de brindar una solución a esta problemática, se concibió el proyecto "Gestión de la Seguridad Lógica y Física", el cual tiene como principal objetivo el crear un estándar a utilizar dentro del sistema de las empresas virtuales y el centro de cómputo de la carrera.

El proyecto tiene sus ejes centrales en el uso de estándares internacionales y nacionales como la TIA 942 y la NTP 17799. Adicionalmente, la empresa se rige por el uso de ITIL V3.0 el mismo que será utilizado en la gestión de la configuración para este proyecto.

Al finalizar el proyecto, se logrará diseñar los procesos y el estándar adecuado para las empresas virtuales dentro de la carrera.

1.2 Objetivos

1.2.1 Objetivos del negocio

El objetivo principal de IT-Expert es administrar los recursos tecnológicos de las carreras de Sistemas de Información y de Software brindando servicios tecnológicos de manera efectiva para la gestión adecuada de la información de las empresas virtuales de la UPC, así como la adecuada asesoría y/o consultoría en los temas de su competencia.

1.2.2 Objetivo General

Diseñar los procesos, controles y procedimientos (estándar) para gestionar la seguridad física (seguridad ambiental, control de acceso, monitoreo, estándares, etc.) y la seguridad lógica (permisos en aplicativos, compartidos, bases de datos, roles, etc.) en el centro de cómputo de la carrera.

1.2.3 Objetivos específicos

O.E.1: Evaluar el estado actual del Centro de cómputo de la carrera.

O.E.2: Definir los procesos que regirán a la gestión de seguridad lógica y física para las empresas virtuales.

O.E.3: Integrar los conceptos de la NTP 17799 y la TIA 942, para la creación de un estándar a usar en el centro de cómputo de la carrera.

1.3 Alcance

Inclusiones del Proyecto
Evaluación de la situación actual del Centro de datos de la carrera con base en los niveles del Tier.
Desarrollo de los diagramas de procesos y diagrama de primer nivel acordes al EBM.
Definición de controles que deben cumplirse para llegar al TIER determinado y no generen conflictos con los sistemas desplegados.
Creación de un estándar personalizado, para el control de la seguridad lógica y física en las empresas virtuales.
El proyecto solo involucrará al centro de cómputo y laboratorios de la carrera de Ing. De Sistemas de Información y Software.
Al finalizar el proyecto se realizará una encuesta con el objetivo de determinar el nivel de satisfacción de los usuarios respecto a la seguridad del sistema.

Exclusiones del Proyecto
La creación de un software.
La adquisición o implementación de algún componente de hardware o software.

1.4 Asunciones

El comité de proyectos asignará un asesor especialista en IT, el cual guiará el desarrollo del proyecto y compartirá sus conocimientos sobre tecnologías de información y en base a estos conocimientos se basarán los entregables del presente proyecto.

Se contará con el apoyo de alumnos de Taller de Desempeño Profesional 1 y 2.

Se contará con el apoyo de la empresa QA para el aseguramiento de la calidad de los entregables según los plazos pactados por ambas partes.

Sección 2. Organización del Proyecto

2.1 Estructura del Proyecto

Rol	Responsable
Comité de Proyectos	Jorge Cabrera; Rosario Villalta; Carlos Raymundo.
Gerente General IT-Expert	William Romero.
Gerente de Proyecto	Gino Puppi B.
Equipo de Proyecto	Jack Flores E.
Equipo de Apoyo	Alumnos de IT-Expert.

2.2 Stakeholders

Describir a los Stakeholders del proyecto y cuál es su función.

Función del Stakeholder	Stakeholder
Comité de Proyectos	Son los encargados de aprobar el proyecto, brindan las pautas sobre las cuales se debe llevar a cabo.
William Romero	Gerente de IT-Expert, brinda los requerimientos claves acerca del proyecto.
Encargados del Proyecto	Alumnos que brindarán toda la información acerca del proyecto.
Usuarios	Alumnos matriculados en los talleres de desempeño y proyecto.
Luis Mamani	Es el encargado de brindar sugerencias en base a su experiencia para ser aplicadas en el proyecto.
Gerente del Proyecto	Es el actor principal del proyecto, se encarga de manejar la información y controlar el cumplimiento de los requerimientos de los clientes.
Empresa QA	Es la encargada de asegurar el nivel de calidad del proyecto, inspeccionando los documentos relacionados a este.
Encargados del Centro de Cómputo	Son los encargados de administrar el Centro de datos

Sección 3. Estructura de Trabajo

3.1 Métodos, Herramientas, y Técnicas

Métodos:

- Se tendrá referencia al marco de recomendaciones de ITIL.
- Se tendrá una referencia a la NTP 17799 y la TIA 942.
- Se tendrá una referencia a la metodología EUP.
- Lenguaje de modelamiento BPMN.
- Se tendrá una referencia al ISO 27000.

Herramientas:

- Microsoft Office 2007.
- Bizagi Process Modeler.
- SQL 2008.

3.2 Actividades e Hitos

Hito	**Fecha Estimada de Termino**
Formulación y Aprobación del Charter del Proyecto	25/03/11
Checklist de evaluación del Centro de datos	04/04/11
Reporte de Incidencias respecto a la Arquitectura del Centro de datos	18/04/11
Reporte de Incidencias respecto al Sistema Eléctrico del Centro de datos	23/05/11
Reporte de Incidencias respecto a las Telecomunicaciones Centro de datos	30/05/11
Reporte de Incidencias respecto al Sistema Mecánico del Centro de datos	13/06/11
Reporte de Incidencias del Sistema	15/06/11
Informe de estado del Centro de datos	22/06/11
Políticas, Controles y Normas	04/07/11
Elaboración y presentación del plan de trabajo	*Ciclo 2011-02*
Auditoría interna.	*Ciclo 2011-02*
Elaboración de la memoria final del proyecto	*Ciclo 2011-02*
Actualización del estándar a su versión final	*Ciclo 2011-02*

Sección 4. Riesgos

Riesgos
El contrato de validación y verificación firmado con QA caduque antes del fin de la inspección.
La inspección realizada por parte de QA sea incorrecta.
Disponibilidad de tiempo de los usuarios finales, para las reuniones de captura de requerimientos (niveles de seguridad, accesos, roles, etc.) y reuniones de control del avance del proyecto.
La aceptación o continuidad del proyecto estará a cargo del comité de proyectos.
Indecisión por parte de los Stakeholders para definir los requerimientos mínimos.

Sección 5. Historial de Revisión

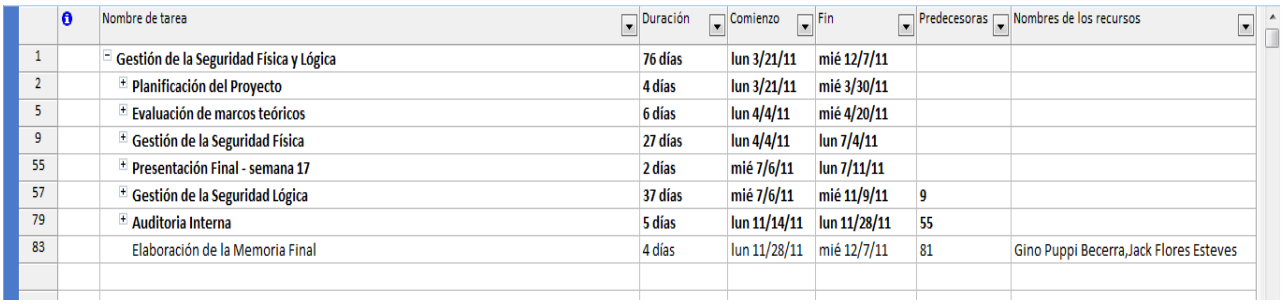
Versión	Nombre	Descripción	Fecha
1.0	Plan de Proyecto	Creación del documento	03/04/11
1.1	Plan de Proyecto	Modificación según sugerencias de William Romero	04/04/11
1.2	Plan de Proyecto	Modificación según sugerencias de Luis Mamani	10/04/11

Sección 6. Aprobación

Nombre	Cargo	Firma	Fecha
Jorge Cabrera	Director de las carreras de Computación		
Rosario Villalta	Coordinadora de Ing. De Sistemas de Información.		
William Romero	Gerente General de IT-Expert		
Luis Mamani	Asesor de Proyecto		

ANEXO 3

Cronograma Proyecto GSFL



	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
1	Gestión de la Seguridad Física y Lógica	76 días	lun 3/21/11	mié 12/7/11		
2	Planificación del Proyecto	4 días	lun 3/21/11	mié 3/30/11		
5	Evaluación de marcos teóricos	6 días	lun 4/4/11	mié 4/20/11		
9	Gestión de la Seguridad Física	27 días	lun 4/4/11	lun 7/4/11		
55	Presentación Final - semana 17	2 días	mié 7/6/11	lun 7/11/11		
57	Gestión de la Seguridad Lógica	37 días	mié 7/6/11	mié 11/9/11	9	
79	Auditoria Interna	5 días	lun 11/14/11	lun 11/28/11	55	
83	Elaboración de la Memoria Final	4 días	lun 11/28/11	mié 12/7/11	81	Gino Puppi Becerra,Jack Flores Esteves

Cronograma Proyecto GSFL 2011-01

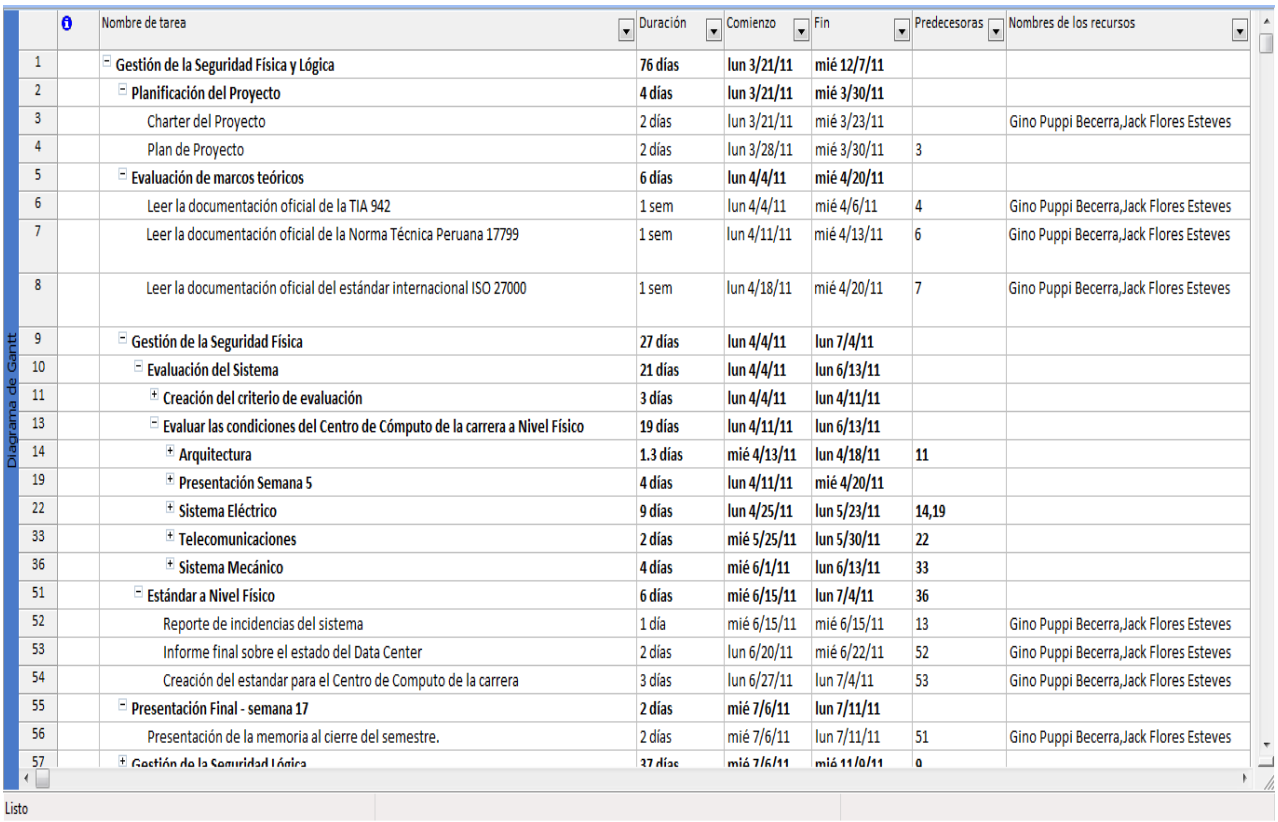


Diagrama de Gantt

	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
1	Gestión de la Seguridad Física y Lógica	76 días	lun 3/21/11	mié 12/7/11		
2	Planificación del Proyecto	4 días	lun 3/21/11	mié 3/30/11		
3	Charter del Proyecto	2 días	lun 3/21/11	mié 3/23/11		Gino Puppi Becerra,Jack Flores Esteves
4	Plan de Proyecto	2 días	lun 3/28/11	mié 3/30/11	3	
5	Evaluación de marcos teóricos	6 días	lun 4/4/11	mié 4/20/11		
6	Leer la documentación oficial de la TIA 942	1 sem	lun 4/4/11	mié 4/6/11	4	Gino Puppi Becerra,Jack Flores Esteves
7	Leer la documentación oficial de la Norma Técnica Peruana 17799	1 sem	lun 4/11/11	mié 4/13/11	6	Gino Puppi Becerra,Jack Flores Esteves
8	Leer la documentación oficial del estándar internacional ISO 27000	1 sem	lun 4/18/11	mié 4/20/11	7	Gino Puppi Becerra,Jack Flores Esteves
9	Gestión de la Seguridad Física	27 días	lun 4/4/11	lun 7/4/11		
10	Evaluación del Sistema	21 días	lun 4/4/11	lun 6/13/11		
11	Creación del criterio de evaluación	3 días	lun 4/4/11	lun 4/11/11		
13	Evaluar las condiciones del Centro de Cómputo de la carrera a Nivel Físico	19 días	lun 4/11/11	lun 6/13/11		
14	Arquitectura	1.3 días	mié 4/13/11	lun 4/18/11	11	
19	Presentación Semana 5	4 días	lun 4/11/11	mié 4/20/11		
22	Sistema Eléctrico	9 días	lun 4/25/11	lun 5/23/11	14,19	
33	Telecomunicaciones	2 días	mié 5/25/11	lun 5/30/11	22	
36	Sistema Mecánico	4 días	mié 6/1/11	lun 6/13/11	33	
51	Estándar a Nivel Físico	6 días	mié 6/15/11	lun 7/4/11	36	
52	Reporte de incidencias del sistema	1 día	mié 6/15/11	mié 6/15/11	13	Gino Puppi Becerra,Jack Flores Esteves
53	Informe final sobre el estado del Data Center	2 días	lun 6/20/11	mié 6/22/11	52	Gino Puppi Becerra,Jack Flores Esteves
54	Creación del estandar para el Centro de Computo de la carrera	3 días	lun 6/27/11	lun 7/4/11	53	Gino Puppi Becerra,Jack Flores Esteves
55	Presentación Final - semana 17	2 días	mié 7/6/11	lun 7/11/11		
56	Presentación de la memoria al cierre del semestre.	2 días	mié 7/6/11	lun 7/11/11	51	Gino Puppi Becerra,Jack Flores Esteves
57	Gestión de la Seguridad Lógica	37 días	mié 7/6/11	mié 11/9/11	9	

Listo

Cronograma Proyecto GSFL 2011-02

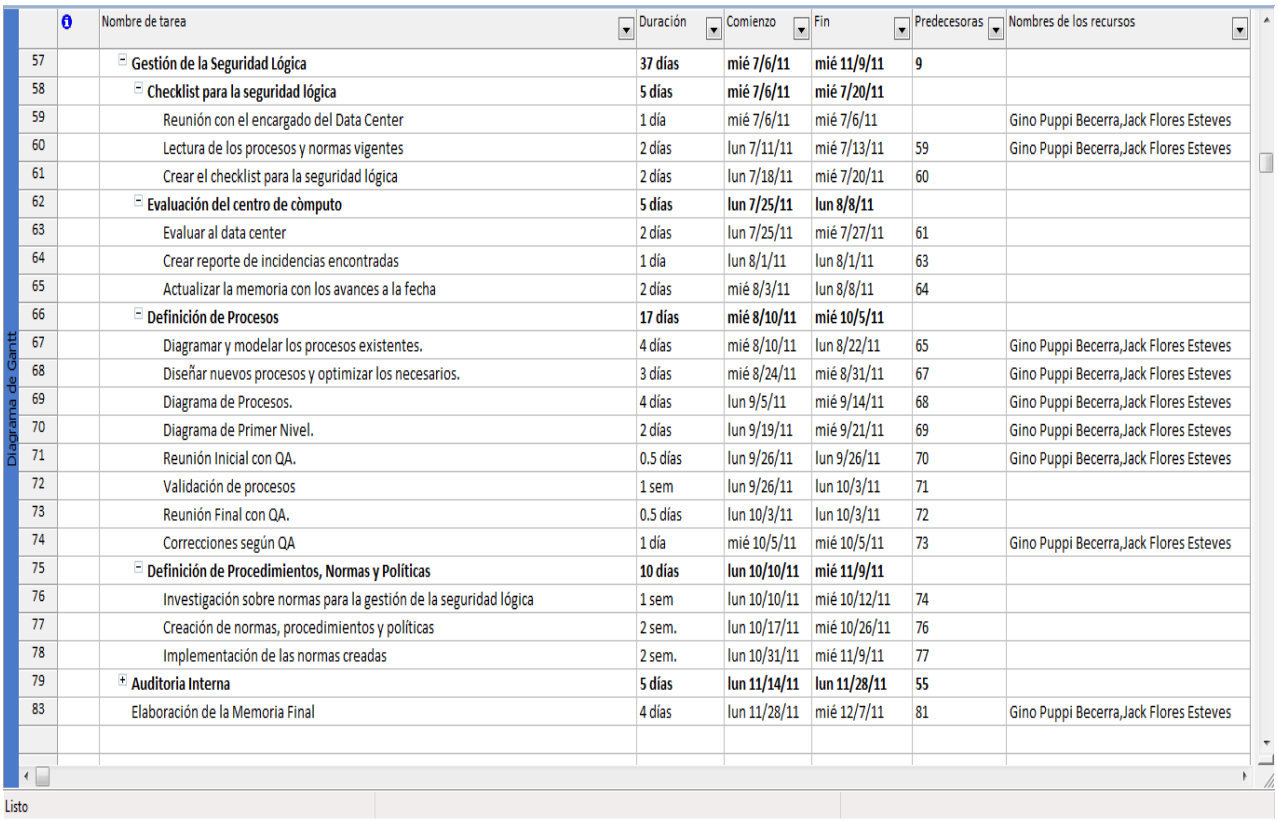


Diagrama de Gantt

	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
57	**Gestión de la Seguridad Lógica**	**37 días**	**mié 7/6/11**	**mié 11/9/11**	**9**	
58	**Checklist para la seguridad lógica**	**5 días**	**mié 7/6/11**	**mié 7/20/11**		
59	Reunión con el encargado del Data Center	1 día	mié 7/6/11	mié 7/6/11		Gino Puppi Becerra,Jack Flores Esteves
60	Lectura de los procesos y normas vigentes	2 días	lun 7/11/11	mié 7/13/11	59	Gino Puppi Becerra,Jack Flores Esteves
61	Crear el checklist para la seguridad lógica	2 días	lun 7/18/11	mié 7/20/11	60	
62	**Evaluación del centro de còmputo**	**5 días**	**lun 7/25/11**	**lun 8/8/11**		
63	Evaluar al data center	2 días	lun 7/25/11	mié 7/27/11	61	
64	Crear reporte de incidencias encontradas	1 día	lun 8/1/11	lun 8/1/11	63	
65	Actualizar la memoria con los avances a la fecha	2 días	mié 8/3/11	lun 8/8/11	64	
66	**Definición de Procesos**	**17 días**	**mié 8/10/11**	**mié 10/5/11**		
67	Diagramar y modelar los procesos existentes.	4 días	mié 8/10/11	lun 8/22/11	65	Gino Puppi Becerra,Jack Flores Esteves
68	Diseñar nuevos procesos y optimizar los necesarios.	3 días	mié 8/24/11	mié 8/31/11	67	Gino Puppi Becerra,Jack Flores Esteves
69	Diagrama de Procesos.	4 días	lun 9/5/11	mié 9/14/11	68	Gino Puppi Becerra,Jack Flores Esteves
70	Diagrama de Primer Nivel.	2 días	lun 9/19/11	mié 9/21/11	69	Gino Puppi Becerra,Jack Flores Esteves
71	Reunión Inicial con QA.	0.5 días	lun 9/26/11	lun 9/26/11	70	Gino Puppi Becerra,Jack Flores Esteves
72	Validación de procesos	1 sem	lun 9/26/11	lun 10/3/11	71	
73	Reunión Final con QA.	0.5 días	lun 10/3/11	lun 10/3/11	72	
74	Correcciones según QA	1 día	mié 10/5/11	mié 10/5/11	73	Gino Puppi Becerra,Jack Flores Esteves
75	**Definición de Procedimientos, Normas y Políticas**	**10 días**	**lun 10/10/11**	**mié 11/9/11**		
76	Investigación sobre normas para la gestión de la seguridad lógica	1 sem	lun 10/10/11	mié 10/12/11	74	
77	Creación de normas, procedimientos y políticas	2 sem.	lun 10/17/11	mié 10/26/11	76	
78	Implementación de las normas creadas	2 sem.	lun 10/31/11	mié 11/9/11	77	
79	**Auditoria Interna**	**5 días**	**lun 11/14/11**	**lun 11/28/11**	**55**	
83	Elaboración de la Memoria Final	4 días	lun 11/28/11	mié 12/7/11	81	Gino Puppi Becerra,Jack Flores Esteves

Listo