



FORMULAR UNA PROPUESTA DE MEJORAMIENTO EN LOS SERVICIOS DE LA GESTIÓN DE ACCESOS, PARA QUE LAS RESPUESTAS DE INGRESO A LOS MÓDULOS DEL SISTEMA PEOPLESFT SE OTORGUEN DE UNA FORMA RÁPIDA Y EFECTIVA, BASADOS EN LA NORMA ISO/IEC 20000 Y LA METODOLOGÍA SCRUM EN LA PONTIFICIA UNIVERSIDAD JAVERIANA DE LA CIUDAD DE BOGOTÁ.

PRESENTADO POR:

DIEGO ALEJANDRO SÁENZ GARCÍA (diego.saenzg@campusucc.edu.co)

UNIVERSIDAD COOPERATIVA DE COLOMBIA

FACULTAD INGENIERÍA

INGENIERÍA DE SISTEMAS

BOGOTÁ

2021



FORMULAR UNA PROPUESTA DE MEJORAMIENTO EN LOS SERVICIOS DE LA GESTIÓN DE ACCESOS, PARA QUE LAS RESPUESTAS DE INGRESO A LOS MÓDULOS DEL SISTEMA PEOPLESOFT SE OTORGUEN DE UNA FORMA RÁPIDA Y EFECTIVA, BASADOS EN LA NORMA ISO/IEC 20000 Y LA METODOLOGÍA SCRUM EN LA PONTIFICIA UNIVERSIDAD JAVERIANA DE LA CIUDAD DE BOGOTÁ.

PRESENTADO POR:

DIEGO ALEJANDRO SÁENZ GARCÍA (diego.saenzg@campusucc.edu.co)

Modalidad de grado Seminario de perfeccionamiento
Requisito Parcial para obtener el título de Ingeniero de Sistemas

Director
Yovanny Vela

UNIVERSIDAD COOPERATIVA DE COLOMBIA
FACULTAD INGENIERÍA
INGENIERÍA DE SISTEMAS
BOGOTÁ
2021





NOTA DE ACEPTACIÓN

PRIMER JURADO

SEGUNDO JURADO

Bogotá, Agosto 2021



AGRADECIMIENTOS

Doy gracias a Dios por permitirme llegar hasta donde estoy actualmente y lo que esté por venir en mi vida laboral y académica. Por mis logros hechos, los objetivos alcanzados y las metas completadas.

A mi papá y a mi mamá por explicarme la importancia social y económica que uno puede adquirir cuando uno tiene un título, por la educación que me dieron, por la enseñanza sobre todos los temas de la vida que me dieron en mi niñez y adolescencia.



DEDICATORIA

A los docentes de la Universidad Cooperativa de Colombia, su trabajo de la pedagogía con objetivo de explicar la importancia de los ingenieros de sistemas en un mundo social y laboral que demanda o necesita profesionales mejor preparados con respecto a las áreas tecnológicas e informáticas.

A mis compañeros y compañeras que he conocido y compartido a lo largo de esta carrera académica, los momentos que socializamos sobre temas académicos y extraacadémicos ha hecho de mi vida estudiantil una etapa de mi vida agradable que siempre recordaré con alegría.



CONTENIDO

GLOSARIO	7
RESUMEN.....	8
INTRODUCCIÓN	9
1. DESCRIPCIÓN DEL PROBLEMA.....	10
1.1. PLANTEAMIENTO DEL PROBLEMA.....	10
1.2. OBJETIVOS DEL PROBLEMA.....	11
1.2.1 Objetivo General	11
1.2.2 Objetivos Específicos	11
2. MARCOS DE REFERENCIA.....	12
2.1. MARCO TEÓRICO	12
2.2. MARCO JUDICIAL	16
3. METODOLOGÍA.....	17
4. DIAGNÓSTICO	19
5. DISEÑO DE INGENIERÍA.....	24
CONCLUSIONES	26
RECOMENDACIONES.....	27
BIBLIOGRAFÍA.....	28



GLOSARIO

Acceso: autenticación e identificación de un usuario para administrar o gestionar funciones de un sistema informático.

Aplicación: recurso tecnológico o software creado para una determinada tarea.

Caso: acontecimiento o conjunto de circunstancia para ser analizado.

Cargo: función o rol asignado a una persona que contiene responsabilidades para ser realizadas.

Configuración: son opciones personalizadas de un individuo sobre un sistema.

Gestión de Accesos: es la normativa que permite el acceso a sistemas para usuarios autorizados y prohíbe la entrada a usuarios no autorizados al sistema.

Incidente: acontecimiento repentino y/o impredecible no deseado que se presenta en los procesos de un sistema.

Metodología: es una serie de métodos y técnicas científicas que se aplican sistemáticamente durante un proceso de investigación para alcanzar un resultado válido y eficiente.

Norma ISO/IEC 20000: Norma internacional diseñada para proporcionar un marco coherente para la gestión de los Servicios TI, tanto internos como externos, beneficiando a empleados y clientes.

Planificación: es un proceso estructurado en etapas para obtener un objetivo determinado.

Problema: es un acontecimiento en un sistema que puede producir: lentitud, malestar o fallos.

Proceso: es una secuencia de pasos creada con algún tipo de lógica que se enfoca en lograr algún resultado específico. Inicia por una entrada y finaliza en una salida.

Queja: Disgusto por el trabajo de un sistema informático o el trabajo de un ser humano.

Reclamo: es una expresión de desacuerdo o inconformidad ante un producto o un servicio de una organización.

Scrum: es un marco de trabajo para desarrollo ágil de software.

Servicio: es una función o utilidad que desempeña un sistema.

Unidad de negocio: es un conjunto de actividades de una organización con el fin de tener una estrategia común y distinta a las del resto de actividades de la empresa.



RESUMEN

Esta monografía es importante porque permite profundizar las posibilidades de mejora para el proceso de gestión de accesos en el área de seguridad informática en la Pontificia Universidad Javeriana.

Además, es posible la inclusión de mejoras ante la prestación de servicios en la gestión de accesos ya que es función de un ingeniero dar soluciones a los problemas o inconvenientes que se presentan a la hora de dar el servicio de accesos a los diferentes módulos de campus que tiene la Universidad Javeriana.

Por último, la creación de este documento tiene como propósito integrar dichas mejoras al proceso que lleva acabo el área de seguridad informática en el proceso de gestión de accesos, esto con el fin de dar mejor rendimiento a las áreas interesadas que conforman la organización.



INTRODUCCIÓN

Todas las empresas de cualquier tipo de economía (almacenes de cadena, instituciones educativas, entre otras) cuenta con bases de datos y servicios tecnológicos y para evitar robo o mal uso de datos personales de la empresa está encargada el área de seguridad informática.

El área de seguridad informática está encargada de asesorar a sus empleados para el buen uso de dispositivos tecnológicos y datos de los empleados, docentes y estudiantes de la organización, además de proveedores de consultoría que los asesoran en el uso de herramientas y en consejos sobre seguridad informática, aquí es donde este proyecto tiene como función principal dar solución a los problemas encontrados en el área, formulando nuevas alternativas y planteando una mejor manera de realizar funciones con más agilidad, confiabilidad y seguridad en la Pontificia Universidad Javeriana.

Este documento tiene el propósito de dar una propuesta para mejorar el proceso de gestión de accesos mediante metodologías que complementen este proceso, esto implica que las funcionalidades del proceso sean más efectivas y ágiles, además, de reducir incidentes.

La gestión de acceso a los servicios TI (tecnologías de la información) es el proceso por el cual a un usuario se le brindan los permisos necesarios para hacer uso de los servicios documentados en el catálogo de servicios de la organización o empresa.

La gestión de acceso a los servicios TI está formado por los siguientes componentes o mini procesos:

- El catálogo del servicio: es la documentación sobre los servicios cuyo acceso solicitan los usuarios.
- La gestión de la seguridad: son las políticas de seguridad que la gestión de acceso debe tener en cuenta cuando dé los accesos a los servicios TI.
- Gestión de incidencias: son las peticiones de acceso o actividades relacionadas con los accesos que representen una excepción (por ejemplo: los proveedores de consultoría como es mi caso).
- Gestión técnica y gestión de aplicaciones: es un monitor que indica si los accesos están autorizados o no y para los que sí estén autorizados verificarlo con las políticas de acceso de la organización.



1. DESCRIPCIÓN DEL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

El problema que he visto en mi trabajo como consultor técnico y funcional en PeopleSoft lo he visto presente en el área de seguridad informática para el proceso de gestión de accesos que actualmente tiene en cuenta todos los módulos PeopleSoft de campus de la Pontificia Universidad Javeriana; este proceso no cuenta con alguna metodología de trabajo que complemente el trabajo del proceso.

Las actividades del proceso requieren de trabajo manual (trabajo humano) y los encargados de las funcionalidades del proceso no tienen todos los recursos y/o las herramientas que permitan un trabajo eficiente y yo como ingeniero y consultor debo buscar una solución para reducir los tiempos de trabajo y el área de seguridad informática dé mejor atención.

Además del problema principal explicado en los párrafos anteriores, también he visto que en este proceso se pierde la comunicación entre quienes participan en el flujo de trabajo, esto implica: demoras al atender los servicios e incidentes reportados porque el equipo no es notificado a tiempo sobre cambios o nuevas funcionalidades que entren en el proceso de gestión de accesos.



1.2. OBJETIVOS DEL PROBLEMA

1.2.1 Objetivo General

Formular una propuesta de mejoramiento en los servicios de la gestión de accesos, para que las respuestas de ingreso a los módulos del sistema PeopleSoft se otorguen de una forma rápida y efectiva, basados en la norma ISO/IEC 20000 y la metodología SCRUM en la Pontificia Universidad Javeriana de la ciudad de Bogotá.

1.2.2 Objetivos Específicos

- Diagnosticar el proceso de gestión de accesos con el apoyo de la norma ISO-IEC 20000 y la metodología SCRUM.
- Analizar los diferentes roles de usuario y la forma en cómo se comunica el equipo para organizar las funciones y responsabilidades con la metodología SCRUM y las actividades del proceso de gestión de accesos y determinar los requerimientos para el proceso bajo la norma ISO-IEC 20000.
- Diseñar el proceso de gestión de accesos para que puedan ser aplicadas en el área de seguridad informática.



2. MARCOS DE REFERENCIA

2.1. MARCO TEÓRICO

Según los lineamientos de la gestión de proyectos de tecnologías PGTI (Scrum, ISO 20000, Cobit, ITIL V4), estas metodologías como propósito en común buscan asegurar la formulación adecuada de proyectos de tecnología de la Información (TI) y realizar un seguimiento eficiente que garantice el desarrollo y conclusión satisfactoria de los proyectos relacionados al área informática.

La finalidad en común de las metodologías, normas, estándares y marcos de referencia es cubrir el ciclo completo de un proyecto informático, desde la documentación hasta su implementación y pruebas. Teniendo en cuenta lo anterior, primero se debe identificar correctamente el problema con un levantamiento de información para conocer el alcance real del problema y sus posibles soluciones, lo que implica conocer la relación de los conceptos. (PlatziConf, 2021)

En las metodologías, normas y marcos de referencia existen métodos de ingeniería estructurados que se basan en modelos de sistemas, notaciones, reglas y guías de procesos que sirven como orientación en su correcto desarrollo, lo cual conlleva a un concepto de ingeniería, conocimiento aplicado de la computación para resolver un problema. (Normalización Española, 2021)

ISO / IEC 20000-1 es el mejor estándar internacional para un sistema de gestión de servicios que brinda servicios consistentes y confiables. Este estándar ayuda a integrar una estrategia de ciclo de vida del servicio en la organización o empresa donde uno labora, da una guía de mejores prácticas sobre cómo se debe administrar el catálogo de servicios para que permanezcan actualizados y agreguen valor de servicio.

ISO / IEC 20000-1 es el estándar recomendado para cualquier proveedor de servicios que requiera seguridad de alta calidad en los servicios que presta. Se usa comúnmente para administración de instalaciones, servicios de TI y servicios de negocios para garantizar servicios efectivos y resistentes.



¿Cuáles son las ventajas de ISO/IEC 20000?

- Desarrollar servicios TI que estén apoyados por objetivos comerciales y/o empresariales.
- Integrar personas, procesos y tecnología para apoyar las metas comerciales de la organización o empresa.
- Poner en práctica controles para medir y mantener altos niveles de calidad de cada servicio.

(Grup, 2021)

Ítem 6 PROCESO DE PRESTACIÓN DEL SERVICIO

Apartado 6.6 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

- ✓ Política de seguridad de la información

La dirección con la autoridad adecuada debe aprobar una política de seguridad de la información que tenga en cuenta los requisitos de: servicio, estatutarios, reglamentarios y las obligaciones contractuales. La dirección debe:

- a) Comunicar la política de seguridad de la información y la importancia de su cumplimiento al personal apropiado del prestador del servicio, del cliente y de los proveedores externos.
- b) Garantizar que se establecen los objetivos para la gestión de la seguridad de la información.
- c) Definir el enfoque que se ha de tomar para la gestión de los riesgos para la seguridad de la información y los criterios para la aceptación de riesgos.
- d) Asegurar que las valoraciones de riesgo para la seguridad de la información se realicen a intervalos planificados.
- e) Garantizar que las auditorías internas para la seguridad de la información se realicen.
- f) Asegurar que los resultados de la auditoría se revisen para identificar las oportunidades para la mejora.



✓ Controles para la seguridad de la información

El prestador o proveedor del servicio debe implementar y poner en práctica controles físicos, administrativos y técnicos para la seguridad de la información con el propósito de:

- a) Mantener la confidencialidad, integridad y accesibilidad de los activos de información.
- b) Cumplir con los requisitos de la política de seguridad de la información.
- c) Lograr los objetivos de la gestión de la seguridad de la información.
- d) Gestionar los riesgos relacionados con la seguridad de la información.

Estos controles de seguridad de la información deben estar documentados y describir los riesgos con los cuales se relacionan los controles, y la forma de operación y el mantenimiento de éstos.

El proveedor del servicio debe revisar la eficiencia de estos controles. También debe tomar las acciones necesarias.

✓ Cambios e incidentes en la seguridad de la información

Las solicitudes de cambio se deben evaluar para identificar:

- a) Riesgos para la seguridad de la información, nueva o modificada.
- b) Impacto potencial sobre los controles y la política de seguridad de la información.

Ítem 8 PROCESOS DE SOLUCIÓN

Apartado 8.1 GESTIÓN DE INCIDENTES Y SOLICITUDES DE SERVICIO

Debe existir un procedimiento documentado para todos los incidentes para definir:

- a) Registro.
- b) Asignación de prioridad.
- c) Clasificación.
- d) Actualización de registros.
- e) Escalamiento.
- f) Solución.
- g) Cierre.



Es importante establecer un procedimiento documentado para la gestión de la atención de las solicitudes de servicio, desde el registro hasta el cierre. Los incidentes y las solicitudes de servicio se deben gestionar de acuerdo con los procedimientos y/o procesos.

El proveedor del servicio debe garantizar que el personal involucrado en el proceso de gestión de incidentes y solicitudes de servicio puede tener acceso y utilizar la información pertinente. La información pertinente debe contar con los procedimientos de gestión de las solicitudes de servicio, los errores conocidos, la solución de problemas y la base de datos de gestión de la configuración. El proceso de gestión de incidentes y solicitudes de servicio debe utilizar la información sobre las versiones exitosas o fallidas y las fechas de las versiones futuras.

El proveedor siempre debe informar al cliente acerca del progreso de los incidentes que reportó o de las solicitudes de servicio. Si los objetivos del servicio no se pueden satisfacer, el proveedor debe informar al cliente y a las partes interesadas y realizar el escalamiento según el procedimiento.

El proveedor por buenas prácticas siempre debe documentar y acordar con el cliente la definición de incidente mayor. La alta dirección administrativa del cliente debe estar informada de los incidentes mayores.

Scrum es un proceso en el que se aplican de manera regular un conjunto de buenas prácticas para trabajar en equipo, y obtener el mejor resultado posible de un proyecto. Estas prácticas se apoyan unas a otras y su selección tiene origen en un estudio de la manera de trabajar de equipos altamente productivos. (ICONTEC, 2012)

En la metodología Scrum se realizan entregas parciales y regulares del producto final, priorizadas por el beneficio que aportan al encargado de evaluar el proyecto. Por esta razón, Scrum está especialmente planeado para ser aplicado a proyectos en entornos complejos donde por ejemplo se necesita:

- Obtener resultados pronto
- Los requisitos son cambiantes o poco detallados.

Scrum también se utiliza para resolver situaciones en que no se está entregando al cliente lo que necesita, cuando las entregas se tardan demasiado, los costos aumentan o la calidad del producto o servicio es regular.



2.2. MARCO JUDICIAL

Las mejoras que van a ser aplicadas al proceso explicado anteriormente deben tener en cuenta las siguientes leyes:

- Ley 1341 del 30 de Julio del 2009 "por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - tic-, se crea la agencia nacional de espectro y se dictan otras disposiciones". (Colombia, Secretaría Senado, 2021)
- Resolución 670 de 14 de diciembre de 2017, de la Procuraduría General de la Nación, por medio de la cual se adopta el manual de políticas y procedimientos para la protección de datos personales. (Colombia, 2021)
- Ley 1918 de 24 de julio de 2018, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest. (Colombia, 2021)



3. METODOLOGÍA

Norma ISO/IEC 20000: es el estándar sobre gestión de recursos que permite la certificación empresarial y profesional, con el fin de planificar e implementar un sistema de gestión de servicios IT.

El proveedor del servicio tiene la obligación de determinar y proporcionar los recursos humanos, técnicos, de información y financieros necesarios para establecer, implementar y mantener el SMS (System Management Services, en español: servicios de gestión de sistemas).

Teniendo en cuenta los párrafos anteriores, mi propuesta es definir los niveles de servicio que permitan garantizar la prestación del servicio.

- Gestión del nivel del servicio
- Gestión de la seguridad de la información
- Gestión de incidencias y peticiones de servicio
- Gestión de problemas

(GrupoACMS, 2021)

Scrum: esta metodología trata sobre el proceso de gestión que reduce la complejidad en el desarrollo de productos para satisfacer las necesidades de los clientes. Esta práctica entrega valor de un servicio o producto de forma simple que promueve la colaboración en los equipos para lograr desarrollar productos complejos.

De esta metodología voy a utilizar la planificación de las tareas a realizar (cierre de tickets de ABM de gestión de accesos), ésta está formado por:

- QUÉ: es la primera mitad de las tareas y se realiza en un timebox de alrededor de 2 horas (si la iteración es de 2 semanas): el cliente presenta a su equipo de trabajo y/o al proveedor (como es mi caso) la lista de requisitos del producto o servicio pone nombre a la meta de la iteración (de manera que ayude a tomar decisiones durante su ejecución) y propone los requisitos más prioritarios a desarrollar en ella. El equipo de trabajo del cliente o el proveedor examinan la lista, pregunta al cliente las dudas que encuentren adicionan más condiciones de satisfacción y escogen los objetivos/requisitos más prioritarios que prevé completar en la iteración.
- CÓMO: es la segunda mitad de las tareas y se realiza en un timebox de alrededor de 2 horas (si la iteración es de 2 semanas). El equipo de trabajo o el proveedor (como es mi caso) planifican la iteración, elaboran la táctica que consiga el mejor resultado posible con el mínimo esfuerzo.

El proceso de la Pontificia Universidad Javeriana también puede aplicar el documento Sprint Backlog ya que este último define las tareas necesarias para poder completar cada objetivo/requisito, creando la lista de tareas de la iteración.



El equipo de trabajo del cliente o el proveedor realizan una estimación conjunta de lo que se requiere para hacer cada tarea. Los miembros del equipo se reparten las tareas que pueden hacer, se agrupan para trabajar en parejas, tríos o como mejor les convenga, con el propósito de compartir conocimiento entre ellos (creando un equipo con más conocimiento) o para resolver juntos objetivos difíciles.

(Martínez, 2021)



4. DIAGNÓSTICO

✓ Diagnóstico

La baja eficiencia de la asignación de los accesos en peoplesoft actualmente genera insatisfacción y malestar a los usuarios, porque algunas veces estos no son entregados oportunamente o la asignación de dichos permisos se realiza mal. Estas falencias se presentan porque los accesos son dados por los analistas de seguridad informática de forma manual, recibiendo primero un correo de algún usuario solicitando permisos de accesos y después el analista asignándolos por medio del formulario de permisos en peoplesoft.

Los analistas interpretan cada solicitud enviada por los coordinadores, revisan las solicitudes detenidamente (implicando más tiempo invertido) para evitar errores y hacer una excelente gestión para los usuarios finales, aunque hay que tener en cuenta que el flujo de solicitudes para accesos puede incrementar ocasionando que los analistas tomen mucho tiempo de respuesta de otros módulos de la universidad, esto implica indirectamente que el proceso de asignación de accesos y permisos no sea el mejor y seguro, permitiendo que se filtren accesos restringidos y vulnerabilidades y todo esto causa más incidencias en el área de accesos y menor eficiencia en la atención de otros casos o requerimientos de los demás módulos.

✓ Obtención de datos mediante cuestionarios

El malestar por la demora de la gestión de accesos a los módulos de PeopleSoft lo podemos evidenciar mediante un cuestionario realizado a tres analistas funcionales que normalmente solicitan esos accesos para realizar su trabajo.

El cuestionario evalúa: la clasificación de módulos del sistema PeopleSoft, la plataforma por donde los usuarios crean las solicitudes y la agilidad del Departamento de Tecnología e Información (DTI) a la hora de realizar las asignaciones.



Nombre completo:
Correo:
Employee ID:
Documento de identidad:
Cargo:

CUESTIONARIO: EVALUACIÓN DE LA GESTIÓN DE ACCESOS A MÓDULOS DE PEOPLESOFT

1. ¿Cómo evalúa la clasificación de módulos del sistema PeopleSoft?
 - a. Malo
 - b. Regular
 - c. Excelente
2. ¿Cómo evalúa el sistema Aranda para las solicitudes de acceso?
 - a. Malo
 - b. Regular
 - c. Excelente
3. ¿Cómo evalúa la agilidad de asignación de accesos a los módulos de PeopleSoft?
 - a. Malo
 - b. Regular
 - c. Excelente

Ilustración: Cuestionario sobre la gestión de accesos

A continuación presento los datos de las analistas funcionales que respondieron mi cuestionario:

Nombre Completo	Correo	Employee ID	Cédula	Cargo
Leidy Rocío Calderón Vera	lrocio.calderon@javeriana.edu.co	00020311150	1018417715	Analista Funcional
Karen Alexandra Galaviz Rubiano	galavis-k@javeriana.edu.co	00020247471	52265162	Analista Funcional
Adriana Patricia Casas Valencia	acasas@javeriana.edu.co	00010155405	1030522587	Analista Funcional

Ilustración: Datos de las analistas funcionales que respondieron el cuestionario



A continuación presento los resultados en un diagrama de barras, los criterios de excelente, regular y malo valen 3, 2 y 1 respectivamente:

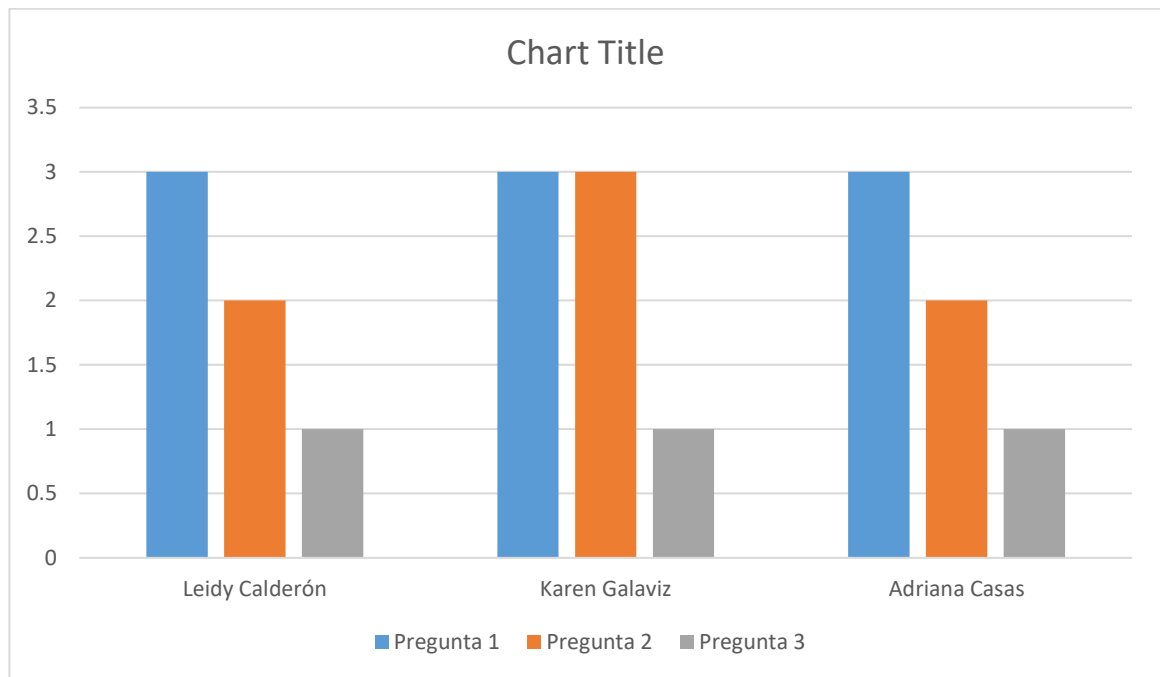


Ilustración: resultados de las respuestas de las analistas funcionales.

Analizando los resultados del cuestionario realizado a las tres analistas funcionales, evidenciamos que tanto el sistema PeopleSoft y Aranda (la aplicación para los casos) son eficientes y tienen buenas calificaciones a diferencia de la gestión de accesos que administra el DTI, estos resultados me indican que el personal del DTI que gestiona los accesos a los módulos de DTI tienen falencias con respecto a eficiencia y agilidad, esto puede solucionarse aplicando metodologías ágiles como SCRUM e ISO 20000.

✓ Incidencias

ID INCIDENCIA	FECHA INCIDENCIA	RESPONSABLE	ATENDIDO POR	SOLICITADO POR	DESCRIPCIÓN
19784736	26/04/2021	DTI (Departamento de Tecnología e Información)	ACRUZ	LUISA MOLINA	Permisos para el módulo de RH
19784786	6/05/2021	DTI (Departamento de Tecnología e Información)	AFERNADEZR	ANDRÉS GARCÍA	Permisos para el módulo de finanzas
19784812	15/05/2021	DTI (Departamento de Tecnología e Información)	AFERNADEZR	KAREN GALAVIS	Permisos para generar certificados
19784838	27/05/2021	DTI (Departamento de Tecnología e Información)	ACRUZ	MAGDA BELTRÁN	Permisos para el módulo de finanzas
19784870	2/06/2021	DTI (Departamento de Tecnología e Información)	AFERNADEZR	OSCAR GUERRERO	Permisos para el módulo de RH
19785001	14/06/2021	DTI (Departamento de Tecnología e Información)	ACRUZ	MARTHA PÉREZ	Permisos para generar certificados
19785026	29/06/2021	DTI (Departamento de Tecnología e Información)	ACRUZ	ADRIANA CASAS	Permisos para el módulo de finanzas
19785054	11/07/2021	DTI (Departamento de Tecnología e Información)	AFERNADEZR	FABÍAN RUIZ	Permisos para generar certificados
19785100	24/07/2021	DTI (Departamento de Tecnología e Información)	ACRUZ	LEIDY CALDERÓN	Permisos para el módulo de RH
19785127	5/08/2021	DTI (Departamento de Tecnología e Información)	AFERNADEZR	JULY JARA	Permisos para el módulo de finanzas

Ilustración: Incidencias

En la imagen anterior se puede observar un pequeño reporte con 10 ejemplos de incidencias sobre accesos a módulos donde la asignación de permisos quedó mal hecha; el reporte muestra la información correspondiente al id del incidente



reportado, la fecha que se creó la incidencia, el área responsable de la revisión, el analista del área que atendió la incidencia, el usuario que creó la incidencia y la descripción de esta última.

✓ Formulario de Log In en PeopleSoft de la Universidad Javeriana

Select a Language: [English](#) [Español](#)

User ID:

Password:

[Set Trace Flags](#)

Ilustración: Formulario de Log In en PeopleSoft de la Universidad Javeriana

En la imagen anterior se observa el formulario de Log In de la Universidad Javeriana.

✓ Formulario para asignar roles y accesos a usuarios

General | ID | **Roles** | Workflow | Audit | Links | User ID Queries

User ID: PK_DSAENZ
Description: Peak-Diego Saenz

Role Name	Description	Dynamic	View Definition
AM Administrator	Absence Mngmnt Administrator	<input type="checkbox"/>	Route Control View Definition + -
AWE Administrator	AWE Administrator	<input type="checkbox"/>	Route Control View Definition + -
AppServer Administratc	AppServer Administrator	<input type="checkbox"/>	Route Control View Definition + -
Applicant	Internal Applicant	<input type="checkbox"/>	Route Control View Definition + -
Benefits Administrator	[WV] Benefits Administrator	<input type="checkbox"/>	Route Control View Definition + -
CS - Administrator	CS - Administrator	<input type="checkbox"/>	Route Control View Definition + -
CS Administrator NLD	CS - Administrator Netherlands	<input type="checkbox"/>	Route Control View Definition + -
Compensation Adminis	Compensation Administrator	<input type="checkbox"/>	Route Control View Definition + -
Directory Administrator	Directory Administrator	<input type="checkbox"/>	Route Control View Definition + -
E&G Administrator	Educ&Govt Administrator	<input type="checkbox"/>	Route Control View Definition + -



Ilustración: Formulario para asignar roles y accesos a usuarios

En la imagen anterior se observa el formulario donde asignan roles a usuarios para que estos últimos puedan acceder a componentes y módulos de campus.

- ✓ Base de datos de los roles y accesos por usuario

Hoja de Trabajo | Generador de Consultas

```
SELECT * FROM SYSADM.PSROLEUSER WHERE ROLEUSER = 'AFERNADEZR'
```

Resultado de la Consulta | Todas las Filas Recuperadas: 29 en 0,016 segundos

	ROLEUSER	ROLENAME	DYNAMIC_SW
1	AFERNADEZR	Aprobador_Seleccion	N
2	AFERNADEZR	CSUJ_ADMN_GESTOR_CONSULTAS	N
3	AFERNADEZR	Creador_Vacantes	N
4	AFERNADEZR	Empleados_Autoservicio_Gerente	N
5	AFERNADEZR	Gerente_Contratante	N
6	AFERNADEZR	PUJB_APE_EMPLEADO	Y
7	AFERNADEZR	PUJB_APE_JEFE	Y
8	AFERNADEZR	PUJB_ARBOL_COORD_DES_Y_MANT	N
9	AFERNADEZR	PUJB_ARBOL_DTI_REG_CONS_TURNOS	Y
10	AFERNADEZR	PUJB_CDB_CONFIG_IMPRESORAS	N

Ilustración: Base de datos de los roles y accesos por usuario

En la imagen anterior podemos observar la tabla que guarda los registro sobre los roles que tiene cada usuario, esos roles son los que dan accesos a todos los módulos de campus de la Universidad Javeriana.



5. DISEÑO DE INGENIERÍA

Teniendo en cuenta las necesidades y el desempeño actual de la gestión de accesos de la Pontificia Universidad Javeriana, propongo las siguientes alternativas de mejoramiento:

Es necesario establecer como una estrategia corporativa el valor de la gestión de (roles y perfiles) con el propósito de establecer un valor individual y mejorar los niveles de servicio. Cada año todos los líderes de área deben presentar con base en los planes para el año siguiente, el presupuesto proyectado presentando una justificación o sustentación de este. Es tarea del área realizar el presupuesto anual de gestión de accesos, teniendo en cuenta los costos y los recursos necesarios.

La seguridad de la información también debe formalizar las prioridades de asignación de recursos y el orden de inversión, maximizando la contribución a las necesidades de la empresa y la oportunidad de la inversión para obtener adecuados resultados.

- ✓ Procesos de organización seguridad de la información:

Gestión de roles y responsabilidades: todos los responsables de áreas deben determinar las funciones y responsabilidades de cada cargo y puesto, asegurándose que los miembros del equipo de trabajo tengan los privilegios necesarios en los módulos de campus.

Capacitación para el recurso humano: es importante identificar las necesidades, oportunidades de formación y promover el entrenamiento continuo.

Recomiendo establecer las siguientes metodologías ágiles de trabajo:

Norma ISO 20000

- ✓ Proceso 6 / Prestación de Servicios
- ✓ Apartado 6.6 / Gestión de la Seguridad de la Información
- ✓ Proceso 8 / Proceso de Solución
- ✓ Apartado 8.1 / Gestión de incidentes y solicitudes de servicio

SCRUM

- ✓ Daily Meeting
- ✓ Spring
- ✓ Spring Backlog
- ✓ Product Backlog

Matriz de las cuatro acciones: esta herramienta es útil para identificar los elementos de valor de la gestión de accesos en la organización respondiendo cuatro preguntas claves que buscan cuestionar el modelo actual:

- ✓ ¿Qué errores en el proceso se deben reducir?
- ✓ ¿Qué factores o procesos deben ser eliminados?
- ✓ ¿Cuáles aspectos o procesos se deben incrementar?



✓ ¿Cuáles aspectos o procesos se deben crear o implementar?

Para desarrollar esta matriz se utilizaron dos mecanismos de recolección de información:

- 1) A través de la encuesta de estado de la gestión de accesos realizada a los coordinadores y/o líderes de área y al personal dónde mediante preguntas abiertas se solicitaba contestar las cuatro preguntas mencionadas anteriormente.
- 2) Mediante una reunión donde hubo una lluvia de ideas, en ésta participó el equipo de trabajo del área de seguridad de la información aportando su percepción sobre estos aspectos basados en la propia experiencia.

Teniendo en cuenta la información anterior y los comentarios recibidos de los usuarios, una lista de las fortalezas y debilidades del área y de las tecnologías de información utilizadas en la gestión de accesos. Además de lo anterior, hay que tener presente el entorno, las nuevas tecnologías, los conocimientos y experiencia de cada uno para elaborar un listado de las oportunidades y amenazas que podría tener el área en un futuro cercano.

Una vez recopilada toda la información, se hace una reunión donde se expresen y sustenten las ideas de cada miembro del área y por consenso sigue definir las estrategias a utilizar en el proceso para mejorar el desempeño del área y por ende, ofrecer un mejor servicio a los usuarios: lluvia de ideas (teniendo en cuenta las opiniones de todos los miembros del equipo) y los resultados de la matriz de las cuatro acciones realizada previamente, entre otras.



CONCLUSIONES

La gestión de accesos en los productos informáticos de una empresa u organización es la primera clave importante de la productividad empresarial, esto implica mayor eficiencia operativa, de gestión y estratégica; de cada miembro que forma parte de la empresa, además asegura los tres pilares de la seguridad de la información (integridad, confidencialidad y disponibilidad).

En este documento, identifico oportunidades de mejora, que al implementarlas permiten un correcto desempeño en la entrega del producto final que son las cuentas de acceso ágilmente cumpliendo tiempos óptimos.



RECOMENDACIONES

Uno de los temas en que más se fijan las organizaciones son los controles de acceso. El control y monitoreo de acceso es recomendable e importante porque permite saber quién accede y a qué accede al sistema, el usuario autorizado o el infiltrado sin autorización pueden entrar a un módulo en concreto, por ejemplo: finanzas, donde puede tener acceso a datos personales muy delicados y hacer mal uso de ellos. El ejemplo anterior es un caso de miles que ocurren en empresas a nivel mundial y la idea es garantizar la seguridad de datos manteniendo un control sobre los activos de la organización.

Con respecto a la seguridad tangible, las tarjetas electrónicas acumulan datos de los usuarios (ejemplo como el ID y nombre completo), estas tarjetas sirven para acceder y salir de la empresa o utilizar activos de la organización (ejemplo: hardware de impresión). Esta herramienta es muy útil, pero la desventaja es que se pueden "prestar" entre los empleados de la organización, esto implica falta de veracidad en las identificaciones personales.

Los controles biométricos en la actualidad son unas de las herramientas más modernas en la seguridad informática, son populares y no tan costosas. Los lectores de huellas digitales son los más comunes. Lo recomendable es comprar dispositivos que como mínimo nos permitan dos huellas por usuario y tomarlas una de cada mano, en caso de que algún lector falle no produzca mayores problemas de acceso a todo el personal de la organización.

Toda la inversión que deba realizar una organización para garantizar seguridad a los accesos es necesaria y útil.



BIBLIOGRAFÍA

- Colombia, C. d. (10 de 07 de 2021). Obtenido de <http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf>
- Colombia, C. d. (10 de 07 de 2021). *Secretaría Senado*. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html
- Grup, B. (10 de 7 de 2021). *BSI*. Obtenido de Gestión de Servicios: <https://www.bsigroup.com/es-CO/gestion-de-servicios-de-ti-isoiec-20000-/>
- GrupoACMS. (10 de 07 de 2021). *NORMA ISO/IEC 20000-1:2018*. Obtenido de <https://www.grupoacms.com/iso-iec-20000-1-2018>
- ICONTEC. (2012). NORMA TÉCNICA NTC-ISO/IEC 20000-1. En I. C. (ICONTEC), *NORMA TÉCNICA NTC-ISO/IEC 20000-1* (págs. 17-25). Bogotá D.C: ICONTEC.
- Martínez, E. (10 de 07 de 2021). *Agile y Scrum*. Obtenido de <https://www.iebschool.com/blog/metodologia-scrum-agile-scrum/>
- Normalización Española. (10 de 07 de 2021). <https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0061236>. Obtenido de <https://www.normas-iso.com/nueva-norma-iso-iec-20000-1-2018/>
- PlatziConf. (10 de 07 de 2021). https://platzi.com/blog/metodologia-scrum-fases/?utm_source=google&utm_medium=paid&utm_campaign=intention&utm_content=&adgroup=65889444645&gclid=EA1aIQobChMI3piwplLeJ4wIV5f7jBx1fnALxEAAAYASAAEgJD_vD_BwE. Obtenido de https://platzi.com/blog/metodologia-scrum-fases/?utm_source=google&utm_medium=paid&utm_campaign=intention&utm_content=&adgroup=65889444645&gclid=EA1aIQobChMI3piwplLeJ4wIV5f7jBx1fnALxEAAAYASAAEgJD_vD_BwE: https://platzi.com/blog/metodologia-scrum-fases/?utm_source=google&utm_medium=paid&utm_campaign=intention&utm_content=&adgroup=65889444645&gclid=EA1aIQobChMI3piwplLeJ4wIV5f7jBx1fnALxEAAAYASAAEgJD_vD_BwE