PROCEDIMIENTO DE RECURSOS TECNOLÓGICOS

Contenido

1. OBJETIVOS

El Proceso Gestión de Sistemas e Infraestructura Tecnológica considera los procesos de Gestión de Sistemas Tecnológicos, Gestión de Infraestructura y del Equipamiento Tecnológico, Gestión de Soporte y de Ciberseguridad. Estos procesos están orientados a mejorar la eficiencia, la calidad, la productividad y la sostenibilidad de las operaciones de la Universidad y a apoyar la ejecución de procesos estratégicos, académicos, administrativos y de apoyo, definidos en el Sistema de Aseguramiento de la Calidad UNAB.

2. ALCANCE Y GRUPOS DE INTERÉS – PARTES INTERESADAS

El proceso tributa al Macro proceso de Gestión de Recursos de carácter de apoyo en el Sistema de Aseguramiento Interno de la Calidad definido por la Universidad Andrés Bello. Los grupos de interés involucrados en este proceso corresponden a Estudiantes, Académicos y Colaboradores.

El alcance de este documento es a nivel global de la UNIVERSIDAD, en particular para todas aquellas áreas que requieran de apoyo de procesos de Tecnología.

3. ROLES Y RESPONSABILIDADES

Rol	*Responsabilidad*
Dirección de Proyectos de TI	Recibir y revisar requerimientos de la necesidad solicitada por las unidades internas Corregir vulnerabilidades asociadas a sistemas.
Dirección de Operaciones e infraestructura TI	Realizar análisis de los requisitos del sistema Definir las infraestructuras para los sistemas Coordinar trabajos de corrección de vulnerabilidades Aprobar o rechazar las solicitudes de creación de cuentas genéricas, de sistemas, temporales, de altos privilegios y de accesos remotos VPN.
Dirección de Ciberseguridad	Identificar desviaciones de cobertura diariamente. Gestionar vulnerabilidades detectadas a partir de Reporte de Vulnerabilidades semanal. Realizar chequeo de seguridad a aplicaciones nuevas o modificaciones. Autorizar paso a producción de aplicaciones nuevas o modificaciones. Coordinar pruebas de explotación con proveedor.
Área de accesos TI Dirección de Tecnologías de la Información	Ejecutar la creación y revocación de las cuentas en los sistemas. Ejecutar la creación, modificación y revocación de los perfiles en los sistemas de UNAB. Registrar todas las creaciones y revocaciones en el sitio SharePoint del área de cumplimiento TI.
Mesa de Servicios Dirección de Tecnologías de la Información	Generar los tickets de los solicitantes y asignarlos al área de Accesos TI, con las solicitudes de creación y modificación de cuentas de usuarios, cuentas de sistemas, cuentas genéricas, cuentas con altos privilegios, y accesos remotos VPN. Realizar seguimiento de los casos generados a través de sus canales establecidos.
Oficial de Seguridad de la Información Dirección de Tecnologías de la Información	Aprobar o rechazar las solicitudes de creación de cuentas genéricas, de sistemas, temporales, de altos privilegios y de accesos remotos VPN.

4. ELEMENTOS DE ENTRADA

Nombre documento	*Origen*
Solicitud de creación cuentas AD y correo electrónico	Remuneraciones – RRHH
Necesidad tecnológica	Unidades Internas UNAB
Reporte Diario de Cobertura	Proveedor
Reporte de Vulnerabilidades	Herramienta de Seguridad

5. PROCESO RECURSOS TECNOLÓGICOS

5.1 Subproceso Gestión de Sistemas Tecnológicos

Descripción de Actividades de Subproceso Gestión de Sistemas Tecnológicos

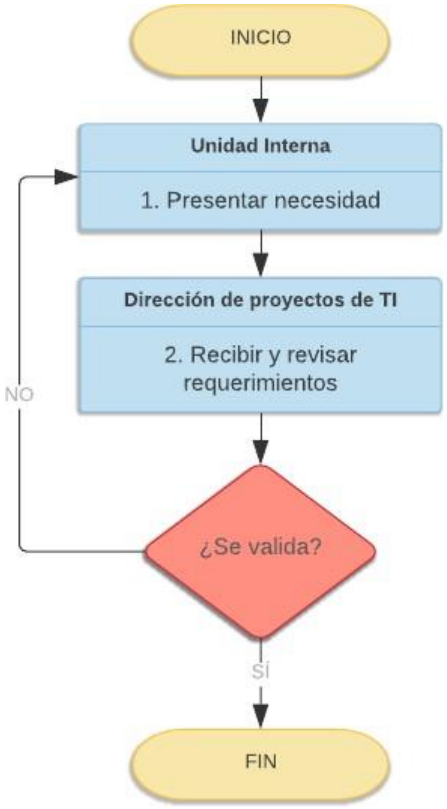
1. Presentar necesidad

Los sistemas tecnológicos parten su ciclo de vida a través de un proyecto derivado de una necesidad de alguna Unidad interna de la Universidad. Esta necesidad parte tu tratamiento en el ciclo de desarrollo en la Dirección de Proyectos de TI.

2. Recibir y revisar requerimientos

Una vez que la unidad interna requirente ha validado que el sistema tecnológico cumple con los requerimientos, se realiza el traspaso a producción a través del procedimiento de Gestión de Cambios de la DGTI. Este proceso está documentado. Toda actualización de un sistema ya sea por nuevas funcionalidades o por “bugs”, también pasa por el proceso de Gestión de Cambios.

Diagrama de Subproceso Gestión de Sistemas Tecnológicos



5.2 Subproceso de Gestión de Infraestructura Tecnológica

Descripción de actividades Subproceso Gestión de Infraestructura Tecnológica

1. Realizar análisis de los requisitos del sistema

Desde el punto de vista de la Infraestructura y Operación, este nuevo sistema podría requerir una nueva infraestructura o reutilización de alguna ya existente, así como también nuevos procesos operativos. De esta forma se enlazan la Gestión de Sistemas Tecnológicos con la Gestión de Infraestructura Tecnológica. La definición de Infraestructura y procedimientos operativos pasa por un análisis de la "Dirección de Operaciones e Infraestructura TI" en relación con los requisitos de los sistemas tecnológicos, sólo algunas premisas se deben cumplir:

- Si hay software involucrado, se da preferencia a que este esté dentro del contrato de licencias que la Universidad tiene con Microsoft.
- Se debe utilizar software licenciado o abierto, sin conflictos de licencia

- Si el producto es un desarrollo llave en mano, el proveedor debe realizar las capacitaciones de infraestructura y operación al área de sistemas y funcionales al área de proyecto.
- Debe existir una contraparte funcional identificada asociada al sistema.
- Si hay infraestructura involucrada, para las comunicaciones se deben utilizar productos CISCO.
- En lo posible se debe contar con ambiente de desarrollo, beta y producción.
- Si se utiliza algún producto licenciado, el costo debe estar incluido en el proyecto durante todo el ciclo de vida del servicio.
- El producto debe estar licenciado e instalado con todos sus parches de seguridad al día.
- Sólo los integrantes de sistemas de la Dirección de Operaciones tienen acceso a los ambientes productivos.
- Todo cambio debe realizarse siguiendo el procedimiento de Gestión de Cambios.

2. Definir infraestructura de los sistemas

Para la definición de la infraestructura de los sistemas, como norma general todos los sistemas deben cumplir con lo siguiente:

- Los sistemas operativos asociados a las nuevas implementaciones deben considerar los elementos de seguridad a nivel de end-point que defina la Universidad, actualmente se usan: Cisco AMP, Cisco UMBRELLA, Agente de Nessus, Agente de BigFix.
- Toda nueva implementación de infraestructura, aunque no sea un proyecto liderado por la Dirección General de TI, debe estar validado por ésta.
- En cuanto a recursos de procesamiento, la Universidad ha definido como estándar AMAZON.
- Toda la infraestructura de REDES de la Universidad debe ser CISCO.
- Los servicios de Infraestructura se consumen de preferencia en la modalidad IaaS (Infraestructura como servicio), actualmente:
    - Provisión de Servidores Virtuales
    - Balanceadores de Carga
    - Firewall de sedes y Datacenter
    - Virtual Datacenter con Amazon

3. Analizar caso a caso

En caso de que no se haya incluido en el presupuesto, se analiza caso a caso.

4. Comprometer y asignar los recursos

En forma paralela se comprometen y asignan los recursos con los proveedores de Infraestructura.

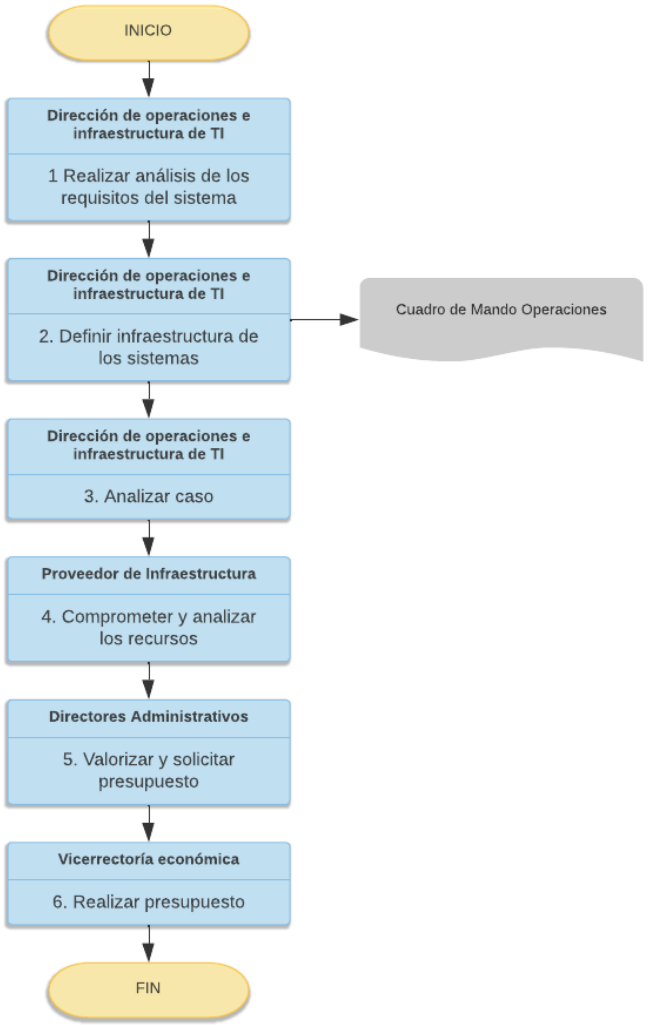
5. Valorizar y solicitar presupuesto

Los directores administrativos, una vez definida la infraestructura para los sistemas, valorizan y solicitan el presupuesto al área requirente para que esta infraestructura pueda ser levantada.

6. Realizar presupuesto

La Vicerrectoría económica realiza el presupuesto terminando con el ciclo de vida de la Infraestructura para luego pasar al procedimiento de Gestión de Cambios. Si bien no se ha definido una política de renovación de la infraestructura se trata de que esta tenga una vida de entre tres años, tanto en la compra directa como en el contrato.

Diagrama de Subproceso Gestión de Infraestructura Tecnológica



5.3 Subproceso de Equipamiento tecnológico

Descripción de Actividades de Subproceso Gestión de Equipamiento Tecnológico

1. Presentar necesidad de equipamiento

La gestión de equipamiento tecnológico se inicia con un requerimiento de alguna unidad de la Universidad para enviarlo a la DGTI.

2. Recibir y revisar necesidad

Este requerimiento llega a la DGTI para que revisen la necesidad y lo canalicen a través de los directores de operación e infraestructura TI.

3. Recibir y analizar necesidad

Los directores de operación e infraestructura TI reciben y analizan la necesidad. Luego del análisis de lo requerido, se itera con la parte interesada para que en la medida de lo posible el equipamiento esté dentro del catálogo de equipamiento que se maneja a través de Servicios Andinos.

4. Realizar adquisición como activo o servicio

Una vez que se logra el acuerdo se decide en conjunto con los Directores Administrativos si se hace la adquisición como activo o como servicio. Dentro de este proceso se incluye el soporte del equipamiento, lo que equivale a la adquisición de garantía sobre los equipos comprados o a lo que se defina como soporte dentro de los servicios de arriendo de equipamiento.

5. Solicitar presupuesto

Los directores administrativos, luego de lograr el acuerdo, solicitan el presupuesto a la Vicerrectoría Académica.

6. Realizar presupuesto

La Vicerrectoría Académica realiza el presupuesto solicitado por los directores administrativos.

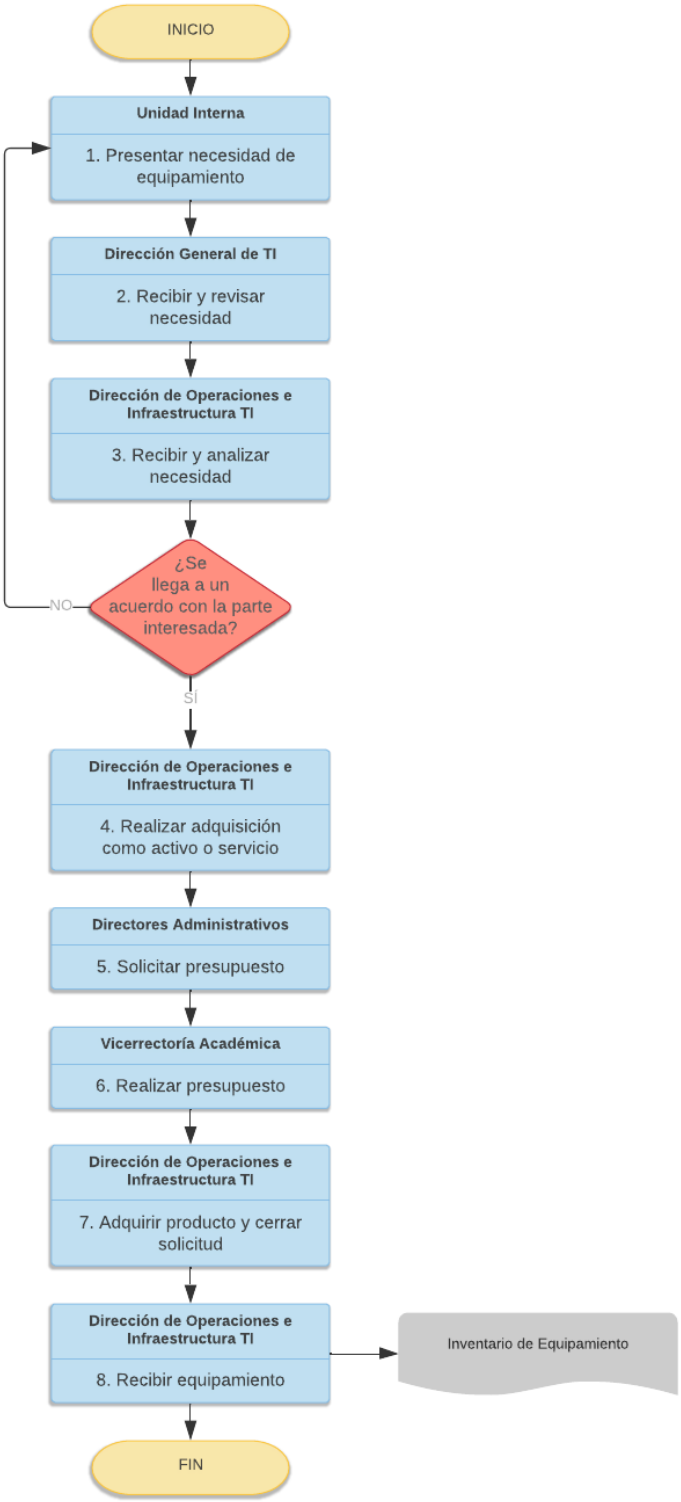
7. Adquirir producto y cerrar solicitud

La Dirección de Operaciones e Infraestructura TI adquiere el producto y cierra la solicitud.

8. Recibir equipamiento

La Unidad UNAB recibe el equipamiento solicitado.

Diagrama de Subproceso Gestión de Equipamiento Tecnológico



5.4 Subproceso Gestión de Soporte

Descripción de actividades Subproceso Gestión de Soporte

1. Requerir soporte

Los usuarios administrativos que requieran cualquier tipo de soporte lo solicitan a través de la mesa de servicios a través de correo electrónico o a través del número de soporte de la mesa de servicio.

2. Recibir y registrar solicitud

En la mesa de servicios un agente es el encargado de registrar la solicitud en la herramienta de tickets.

3. Revisar categoría y dar solución

Si el problema del usuario está dentro del catálogo de servicios de la mesa de servicios, el agente revisa a que categoría corresponde e intenta la solución que podría entregar él directamente, a esto corresponde la solución de nivel 1.

4. Asignar a área resolutoria

Si no existe la solución y de acuerdo con el flujo de la mesa de servicios, el ticket se asigna a un área resolutoria, correspondientes al nivel 2 de solución.

5. Recibir notificación por correo electrónico

Al área resolutoria le llega una notificación por correo electrónico.

6. Analizar Ticket

Algún especialista de esa área tomará el ticket desde la herramienta de gestión de tickets y le dará solución.

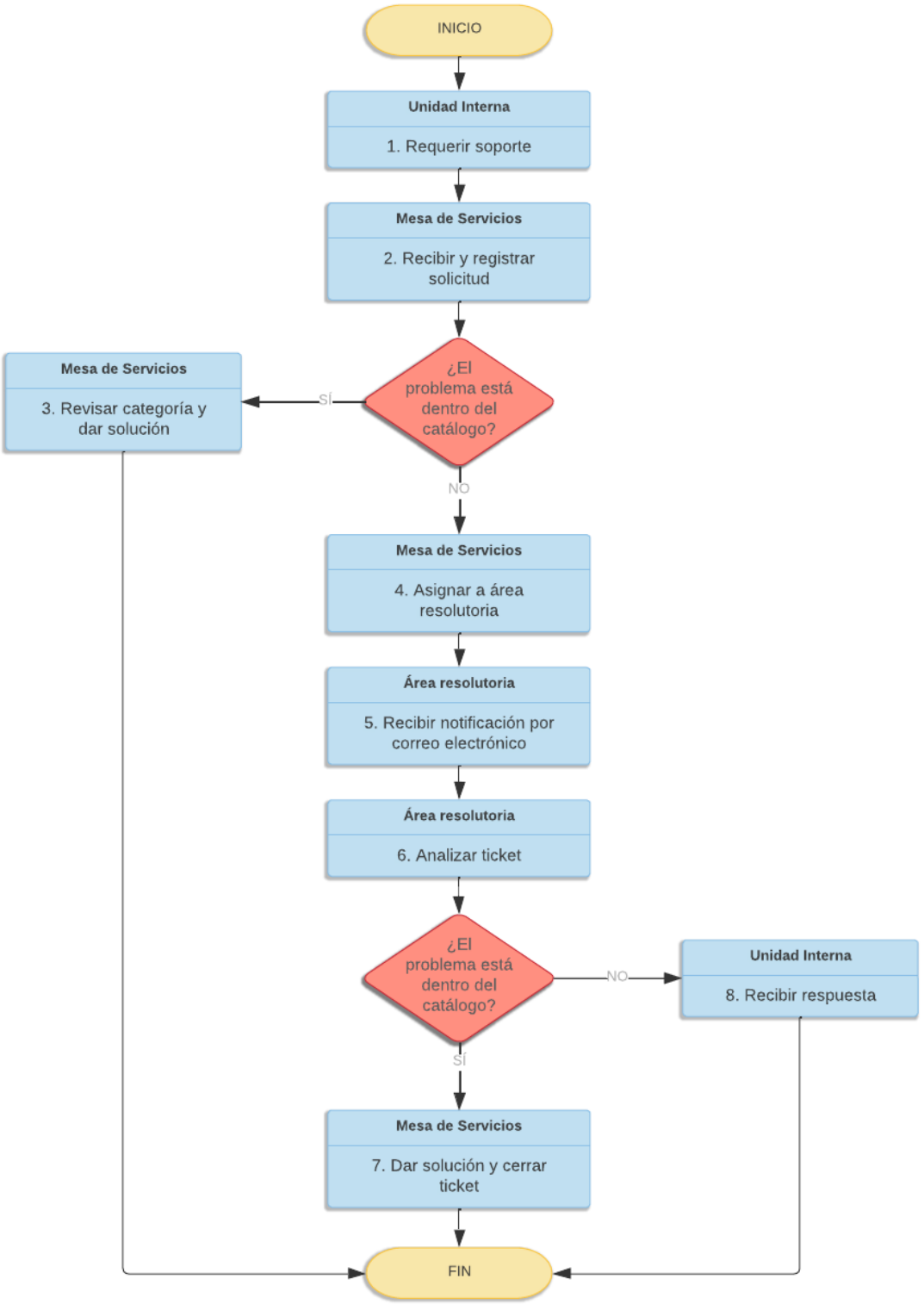
7. Dar solución y cerrar Ticket

En caso de resolución exitosa se cierra el ticket de atención ingresando toda la información de cierre; con el cierre del caso le llegará al usuario requirente un correo informándole de la solución.

8. Recibir respuesta

En caso de no encontrar solución y en caso de que exista un nivel superior de atención, el ticket con el requerimiento de soporte seguirá tratándose de esta forma hasta encontrar solución o hasta determinar que no es factible la solución por el catálogo de servicios. En este caso se comunica al usuario y este verá directamente con la DGTI si se está en presencia de algún problema mayor que deba tratarse con un nuevo proyecto o con mejora de infraestructura.

Diagrama de Subproceso Gestión de Soporte



5.5 Subproceso Sistemas de Gestión

Subproceso Creación de Cuentas de usuario UNAB y Correo Electrónico

El proceso de creación de cuentas de usuario UNAB debe ser gestionado de la siguiente manera:

1. Solicitar creación de cuentas en AD y correo electrónico

El Analista de Remuneraciones de RR.HH. debe realizar la solicitud de creación de cuentas enviando un correo electrónico al área de accesos TI, indicando la siguiente información del usuario:

- Nombre completo
- RUT
- cargo fantasía
- área
- departamento
- ubicación
- jefatura

Adicionalmente, debe generar en sistema DocuShare, en la carpeta de Recursos Humanos, la nómina de nuevas contrataciones.

2. Crear cuenta en AD y correo electrónico

El área de Accesos TI crea la cuenta de usuario solicitada en AD y correo electrónico.

3. Adjuntar listado de cuentas creadas en DocuShare

El área de Accesos TI adjunta el listado de las cuentas creadas en la carpeta de DocuShare de RR.HH., y en el sitio SharePoint del área de cumplimiento de la DGTI.

4. Informar creaciones de cuentas a RRHH y a Jefatura directa

El área de Accesos TI informa la creación de las cuentas a través de correo electrónico al Analista de Remuneraciones de RR.HH. Adicionalmente, se envía ID y contraseña a la jefatura directa del usuario para configuración de la estación de trabajo.

5. Recibir informe de creación de cuentas

El Analista de Remuneraciones de RR.HH. recibe respuesta con el listado de cuentas creadas en AD y correo electrónico, según solicitud.

Subproceso Creación/Modificación de cuentas de usuario en Sistemas

1. Solicitud de creación o modificación de cuenta en Sistemas UNAB

El solicitante debe realizar la solicitud de creación de cuenta o modificación del perfil alSistema, enviando un correo electrónico a la Mesa de servicios TI (mesadeservicios@unab.cl), completando el formulario definido para cada sistema, e indicando la siguiente información del usuario:

- Nombre completo
- RUT
- cargo fantasía
- ubicación
- correo electrónico
- tipo de perfil

Para solicitar el acceso al sistema Banner de un usuario temporal, este usuario debe tener asignado un correo genérico UNAB, ya que sus credenciales de acceso a Banner serán enviadas a este correo.

2. Recibir solicitud y generar Ticket

La Mesa de Servicios TI recibe la solicitud, genera el ticket de servicio y lo asigna al área de Accesos TI.

Para el sistema Banner, la mesa de servicios TI envía el formulario al dueño del sistema para que indique y valide el Rol a asignar al usuario. En el caso de que sea rechazada la solicitud, se indica el motivo y se termina el proceso.

3. Validar información de solicitud

El área de Accesos TI valida que la información contenida en la solicitud se encuentre completa. En el caso que la información este completa se sigue a la tarea 2.8.

4. Indicar datos faltantes

El área de Accesos TI devuelve el ticket a la Mesa de Servicios TI, indicando los datos faltantes requeridos.

5. Solicitar datos faltantes

La Mesa de Servicios TI se contacta con el solicitante vía mail, para que envíe la información indicada como faltante por área de accesos TI.

6. Añadir datos faltantes

El Solicitante debe entregar toda la información faltante para procesar su solicitud.

7. Adjuntar información al ticket

Una vez recibidos los datos faltantes, la Mesa de Servicios TI incorpora dicha información al ticket previamente levantado.

8. Solicitar aprobación de perfil

El área de accesos TI envía la solicitud de aprobación del perfil a través de correo electrónico al dueño del Sistema.

9. Validar solicitud de aprobación del perfil

El dueño del Sistema recibe la solicitud, validando la información del usuario, para lo cual debe determinar si aprueba o rechaza el acceso o modificación del perfil al sistema requerido.

10. Indicar motivo de rechazo

Si el dueño del sistema rechaza la solicitud, el área de accesos TI procede a ingresar el motivo del rechazo y a cerrar el ticket, por lo cual se termina el proceso.

11. Enviar aprobación

Si el dueño del sistema aprueba la solicitud, envía la aprobación a través de correo electrónico al área de accesos TI.

12. Ejecutar la solicitud

El área de accesos TI ejecuta la solicitud, creando el acceso o modificando el perfil del usuario en el sistema requerido.

Para el sistema Banner, en el caso de que se genere un conflicto en la segregación de funciones al momento de otorgar el perfil solicitado, el área de accesos TI informa al responsable del Rol.

13. Informar conflicto de segregación de funciones

El área de accesos TI informa a través de correo electrónico al responsable del Rol, el conflicto generado en la segregación de funciones, para que vuelva a analizar la solicitud y determine si aprueba o rechaza dicha solicitud.

14. Informa solicitud resuelta

El área de accesos TI envía a través de correo electrónico el ID y contraseña de acceso al sistema, directamente al usuario responsable, por temas de confidencialidad y seguridad.

El área de accesos TI ingresa la información de la creación del acceso o modificación del perfil al ticket, y el solicitante recibe una notificación automática a través de la herramienta de solicitud resuelta.

En forma paralela, el área de Accesos TI registra los datos de las cuentas de accesos y/o modificaciones de perfil realizadas en los sistemas, en el sitio SharePoint del área de cumplimiento de la DGTI.

15. Confirmar creación/modificación de cuenta

El solicitante procede a validar o rechazar la creación del acceso o modificación del perfil en el sistema requerido, dentro de los 3 días siguientes, luego de recibir la notificación por correo electrónico desde la herramienta.

16. Cerrar Ticket

El ticket se cierra una vez que el solicitante valide el acceso o modificación del perfil en el sistema, o de lo contrario se procede a cerrar automáticamente.

Subproceso Creación de Cuentas Genéricas de Sistemas o Temporales

1. Solicitar creación de cuenta genérica/sistema/temporal

El Solicitante debe completar el formulario de solicitud, según el sistema requerido, para las cuentas genéricas, de sistemas o temporales, el cual debe contener los datos del responsable UNAB, los datos del beneficiario y los datos del servicio (descripción). En el caso de que se requieran varias cuentas con un único responsable, el solicitante podrá completar el formulario de solicitud masiva de cuentas.

Luego, el solicitante debe enviar adjunto el formulario a la Mesa de Servicios TI al correo electrónico (mesadeservicios@unab.cl).

2. Recibir solicitud y generar ticket

La Mesa de Servicios TI recibe la solicitud, genera el ticket de servicio y lo asigna al área de Accesos TI.

3. Validar información de solicitud

El área de Accesos TI recibe el ticket asignado, validando que la información contenida en la solicitud se encuentre completa. En el caso que exista información incompleta o errónea, se devuelve el ticket a la Mesa de Servicios TI, para que se contacte al solicitante y envíe nuevamente toda la información requerida.

4. Indicar datos faltantes

El área de Accesos TI devuelve el ticket a la Mesa de Servicios TI, indicando los datos faltantes requeridos.

5. Solicitar datos faltantes

La Mesa de Servicios TI se contacta con el solicitante vía mail, para que envíe la información indicada como faltante por área de accesos TI.

6. Añadir datos faltantes

El Solicitante debe entregar toda la información faltante para procesar su solicitud.

7. Adjuntar información al ticket

Una vez recibidos los datos faltantes, la Mesa de Servicios TI incorpora dicha información al ticket previamente levantado.

8. Solicitar aprobación

El área de accesos TI envía la solicitud de aprobación, al dueño del Sistema, Director de Infraestructura TI y al Oficial de Seguridad de la Información, a través del formulario digital, para los sistemas que así lo requieren.

El área de accesos TI envía la solicitud de aprobación al dueño del sistema a través de correo electrónico, para los sistemas que no requieren de formulario.

9. Recibir solicitud de aprobación

El dueño del Sistema, el Director de Infraestructura TI y el Oficial de Seguridad de la Información reciben la solicitud, validando la información del usuario, para lo cual deben determinar si aprueban o rechazan la solicitud de creación de cuenta genérica, de sistema o temporal al sistema requerido.

10. Indicar motivo de rechazo

Si el dueño del Sistema, Director de Infraestructura TI o el Oficial de Seguridad de la Información rechazan la solicitud, el área de accesos TI procede a ingresar el motivo delrechazo y a cerrar el ticket, por lo cual se termina el proceso.

11. Firmar o enviar aprobación

Si el dueño del sistema, Director de Infraestructura TI y el Oficial de Seguridad de la Información aprueban la solicitud, deben firmar el formulario digital para los sistemas que así lo requieren.

Si el dueño del sistema aprueba la solicitud, para los sistemas que no requieren de formulario, envía la aprobación a través de correo electrónico al área de accesos TI.

12. Ejecutar solicitud

El área de Accesos TI recibe el formulario digital firmado y aprobado, o recibe el correo electrónico con la aprobación del dueño del sistema, procede a ejecutar la creación de la cuenta en el sistema requerido.

13. Informar resolución de solicitud

El área de accesos TI envía a través de correo electrónico el ID y contraseña de acceso al sistema, directamente al usuario responsable, por temas de confidencialidad y seguridad.

El área de accesos TI ingresa la información de la creación de la cuenta al ticket, por lo que el solicitante recibe una notificación automática a través de la herramienta de solicitud resuelta.

En forma paralela, el área de Accesos TI registra los datos de las cuentas creadas en los sistemas, en el sitio SharePoint del área de cumplimiento de la DGTI.

14. Confirmar creación de cuenta

El solicitante procede a validar o rechazar la creación de la cuenta en el sistema requerido, dentro de los 3 días siguientes, luego de recibir la notificación por correo electrónico desde la herramienta.

15. Cerrar Ticket

El ticket se cierra una vez que el solicitante valide el acceso en el sistema, o de lo contrario se procede a cerrar automáticamente.

Subproceso Creación de cuentas de altos privilegios

Las cuentas de altos privilegios corresponden a cuentas de usuario que poseen un perfil de administrador con acceso total al sistema solicitado.

1. Solicitar creación de cuenta de altos privilegios

El proceso comienza cuando el solicitante completa el formulario de solicitud de cuentas de Altos Privilegios, el cual debe contener los datos del solicitante de UNAB (responsable), los datos del beneficiario (interno o externo) y los datos del servicio requerido (descripción).

Luego el solicitante debe enviar adjunto el formulario a la Mesa de Servicios TI a través del correo electrónico (mesadeservicios@unab.cl).

2. Recibir solicitud y generar ticket

La Mesa de Servicios TI recibe la solicitud, genera el ticket de servicio y lo asigna al área de Accesos TI.

3. Validar información de solicitud

El área de Accesos TI recibe el ticket asignado, validando que la información contenida en la solicitud se encuentre completa. En el caso que exista información incompleta o errónea, se devuelve el ticket a la Mesa de Servicios TI, para que se contacte al solicitante y envíe nuevamente toda la información requerida.

4. Indicar datos faltantes

El área de Accesos TI devuelve el ticket a la Mesa de Servicios TI, indicando los datos faltantes requeridos.

5. Solicitar datos faltantes

La Mesa de Servicios TI se contacta con el solicitante vía mail, para que envíe la información indicada como faltante por área de accesos TI.

6. Añadir datos faltantes

El Solicitante debe entregar toda la información faltante para procesar su solicitud.

7. Adjuntar información al ticket

Una vez recibidos los datos faltantes, la Mesa de Servicios TI incorpora dicha información al ticket previamente levantado.

8. Solicitar aprobación

El área de accesos TI envía la solicitud de aprobación al Director General de TI, Director de Infraestructura TI y al Oficial de Seguridad de la Información, a través del formulario digital.

9. Recibir solicitud de aprobación

El Director General TI, el Director de Infraestructura TI y el Oficial de Seguridad de la Información reciben la solicitud, validando la información del usuario, para lo cual deben determinar si aprueban o rechazan la solicitud de creación de cuenta con altos privilegios.

10. Indicar motivo de rechazo

Si el Director General de TI, Director de Infraestructura TI o el Oficial de Seguridad de la Información rechazan la solicitud, el área de accesos TI procede a ingresar el motivo delrechazo y a cerrar el ticket, por lo cual se termina el proceso.

11. Firmar aprobación

Si el Director General de TI, Director de Infraestructura TI y el Oficial de Seguridad de la Información aprueban la solicitud, deben firmar el formulario digital.

12. Ejecutar solicitud

El área de Accesos TI recibe el formulario firmado y aprobado, y procede a asignar el permiso de altos privilegios.

13. Informar resolución de solicitud

El área de accesos TI ingresa la información de la asignación del permiso de altos privilegios al ticket, por lo que el solicitante recibe una notificación automática a través de la herramienta de solicitud resuelta.

En forma paralela, el área de Accesos TI registra los datos de la asignación del permiso de altos privilegios, en el sitio SharePoint del área de cumplimiento de la DGTI.

14. Confirmar permiso de altos privilegios

El solicitante procede a validar o rechazar la asignación de permiso de altos privilegios en el sistema requerido, dentro de los 3 días siguientes, luego de recibir la notificación por correo electrónico desde la herramienta.

15. Cerrar Ticket

El ticket se cierra una vez que el solicitante valide el permiso de altos privilegios en el sistema, o de lo contrario se procede a cerrar automáticamente.

Subproceso Solicitud de cuenta para acceso remoto VPN

Las cuentas VPN corresponden a cuentas asignadas a personal externo, la cual permite realizar una conexión en forma remota (fuera de la red UNAB) a los sistemas de la Universidad. La duración máxima de la cuenta será de 3 meses, pudiendo ser extendido dicho plazo, previa autorización formal por parte del Director de Infraestructura TI. En caso excepcional y debidamente justificado, se podrá otorgar accesos remotos con duración indefinida, previa autorización formal por parte de la Dirección General de TI.

1. Completar y enviar formulario de solicitud de acceso remoto

El proceso comienza cuando el solicitante completa el formulario de solicitud de Acceso Remoto, el cual debe contener los datos del solicitante de UNAB (responsable), los datos del beneficiario (externo) y los datos del servicio requerido (descripción). Luego el solicitante debe enviar adjunto el formulario a la Mesa de Servicios TI a través del correo electrónico (mesadeservicios@unab.cl).

2. Recibir solicitud y generar ticket

La Mesa de Servicios TI recibe la solicitud, genera el ticket de servicio y asigna la solicitud al área de Accesos TI para que realice la gestión del requerimiento.

3. Validar información de la solicitud

El área de Accesos TI recibe el ticket asignado, validando que la información contenida en la solicitud se encuentre completa. En el caso que exista información incompleta o errónea, se devuelve el ticket a la Mesa de Servicios TI, para que se contacte al solicitante y envíe nuevamente toda la información requerida.

4. Indicar datos faltantes

El área de Accesos TI devuelve el ticket a la Mesa de Servicios TI, indicando los datos faltantes requeridos.

5. Solicitar datos faltantes

La Mesa de Servicios TI se contacta con el solicitante vía mail, para que envíe la información indicada como faltante por área de accesos TI.

6. Añadir datos faltantes

El Solicitante debe entregar toda la información faltante para procesar su solicitud.

7. Adjuntar información al ticket

Una vez recibidos los datos faltantes, la Mesa de Servicios TI incorpora dicha información al ticket previamente levantado.

8. Solicitar aprobación

El área de accesos TI envía la solicitud de aprobación al Director de Infraestructura TI y al Oficial de Seguridad de la Información, a través del formulario digital.

9. Validar solicitud de cuenta de acceso remoto

El Director de Infraestructura TI y el Oficial de Seguridad de la Información reciben la solicitud, validando la información del usuario, para lo cual deben determinar si aprueban o rechazan la solicitud de creación de cuenta de acceso remoto.

10. Indicar motivo de rechazo

Si el Director de Infraestructura TI o el Oficial de Seguridad de la Información rechazan la solicitud, el área de accesos TI procede a ingresar el motivo del rechazo y a cerrar el ticket, por lo cual se termina el proceso.

11. Firmar aprobación

Si el Director de Infraestructura TI y el Oficial de Seguridad de la Información aprueban la solicitud, deben firmar el formulario digital.

12. Asignar solicitud de acceso remoto

El área de Accesos TI recibe el formulario firmado y aprobado, procede a asignar el ticket de solicitud al área de Redes TI para su ejecución.

En forma paralela, el área de Accesos TI registra los datos de las solicitudes de acceso remoto, en el sitio SharePoint del área de cumplimiento de la DGTI.

13. Crear el acceso remoto

El área de Redes TI crea el acceso remoto de acuerdo con la solicitud recibida.

14. Actualizar y resolver el ticket

El área de Redes TI procede a ingresar la información del acceso remoto otorgado al ticket, por lo que el solicitante recibe una notificación automática a través de la herramienta de solicitud resuelta.

15. Confirmar acceso remoto

El solicitante procede a validar o rechazar el acceso remoto, dentro de los 3 días siguientes, luego de recibir la notificación por correo electrónico desde la herramienta.

16. Cerrar Ticket

El ticket se cierra una vez que el solicitante valide el acceso remoto, o de lo contrario se procede a cerrar automáticamente.

Subproceso Revocación de Accesos

1. Solicitar revocación de accesos en sistemas

El proceso de revocación de acceso se realiza de la siguiente manera:
Cuando se realiza la desvinculación de un colaborador, RR.HH. en forma paralela a esta actividad, debe informar al área de accesos TI a través de correo electrónico, para que realicen la revocación de los accesos en los sistemas, de forma de evitar cualquier conducta inapropiada por parte del colaborador desvinculado.

Adicionalmente, el analista de remuneraciones de RR.HH. sube al sistema DocuShare la lista de colaboradores desvinculados de la Universidad de forma periódica.

2. Revocar accesos en sistemas

El área de accesos TI revoca los accesos del usuario desvinculado en todos los sistemas que son administrados por la Dirección General de TI.

3. Registrar revocaciones de accesos

El área de Accesos TI registra los datos de todas las revocaciones de accesos de usuarios desvinculados informados por Recursos Humanos, en el sitio SharePoint del área de cumplimiento de la DGTI.

Los plazos establecidos para realizar la revocación de accesos son de 3 días hábiles para eliminar las cuentas en los sistemas, a partir de la fecha en la cual Recursos Humanos informa las desvinculaciones al área de accesos TI.

En casos excepcionales y con autorización por correo electrónico de RR.HH., una cuenta de usuario podrá mantenerse activa por un período de tiempo más prolongado.

4. Informar revocaciones de accesos

El área de accesos TI notifica y envía al analista de remuneraciones de RR.HH. la lista de los usuarios desvinculados a los cuales se les dio de baja sus cuentas de accesos.

5. Recibir listado con revocación de cuentas

El Analista de Remuneraciones de RR.HH. recibe respuesta con el listado de cuentas revocadas en los sistemas, según solicitud.

Subproceso Revisión periódica de cuentas

El área de cumplimiento de la DGTI, en conjunto con el área de Accesos TI, los distintos dueños de sistemas y los responsables de los roles de accesos en los sistemas, revisan de forma semestral el listado de cuentas de accesos a los sistemas definidos como críticos para la institución.

1. Solicitar listado de cuentas en sistemas

El área de cumplimiento TI solicita al área de Accesos TI a través de correo electrónico el listado de las cuentas de accesos en los sistemas que son administrados por la DGTI.

2. Enviar listado de cuentas

El área de accesos TI recibe la solicitud, extrae los listados de las cuentas de accesos desde los distintos sistemas, y procede a enviarlos.

3. Enviar listado de cuentas en sistemas propios

El dueño del sistema recibe la solicitud, extrae los listados de las cuentas de accesos desde los distintos sistemas, y procede a enviarlos.

4. Elaborar informes

El área de cumplimiento TI recibe los listados de las cuentas de accesos en los distintossistemas, y procede a elaborar los informes.

5. Enviar informes para revisión

El área de cumplimiento TI envía los informes a los dueños de sistemas o responsables de roles en los sistemas, para su revisión y validación.

6. Revisión y validación de informes

Cada dueño de sistema o responsable de Rol, debe enviar al área de cumplimiento TI el informe de usuarios vigentes revisado, validado y adjuntando observaciones en caso de requerir modificaciones a las cuentas.

7. Solicitar la realización de modificaciones de cuentas

El área de cumplimiento TI recibe los informes, revisa la información y en caso de existir modificaciones a las cuentas, solicita al área de acceso TI realizar las modificaciones a las cuentas de usuarios solicitadas en los aplicativos.

8. Ejecutar la solicitud de modificación de cuentas

El área de accesos TI recibe la solicitud de modificación de cuentas de usuarios en los distintos aplicativos, procede a generar un ticket y a ejecutar la actividad. Luego, procede a documentar en el sitio SharePoint del área de cumplimiento de la DGTI.

9. Generar informe de revisión final

El área de cumplimiento TI procede a elaborar el informe de revisión final con el detalle y evidencias de las cuentas de usuarios revisadas y modificadas.

Subproceso Creación, modificación y eliminación de cuentas Payroll

1. Completar formulario

Subdirector(a) de Remuneraciones debe solicitar la creación de usuarios en sistema Payroll, completando el formulario de solicitud e indicando el tipo de perfil y enviándolo al Jefe de Remuneraciones mediante correo electrónico.

2. Revisar solicitud

El Jefe de Remuneraciones recibe la solicitud de creación de usuario en sistema Payroll, revisando la información adjunta en ella. Si se identifica que falta algún dato la solicitud será enviada de vuelta a Subdirector(a) de Remuneraciones, para que adjunte lo indicado.

3. Solicitar creación de usuario en Citrix

El Jefe de Remuneraciones solicita la creación de usuario en sistema Citrix a través del portal ADP eService.

4. Crear usuario

El proveedor de servicio procede a crear el usuario en sistema Citrix.

5. Indicar solicitud ejecutada

El proveedor de servicio informa la creación del usuario al Jefe de Remuneraciones, resolviendo el ticket en portal ADP eService.

6. Crear usuario

Una vez recibida la notificación de usuario creado en Citrix, el Jefe de Remuneraciones procede a crear el usuario en sistema Payroll.

7. Informar datos de cuentas

El Jefe de Remuneraciones le comunica al usuario sus credenciales de acceso a los sistemas Payroll y Citrix, mediante correo electrónico.

8. Recepcionar claves de acceso Payroll y Citrix

El usuario toma conocimiento de sus credenciales a los sistemas Payroll y Citrix y procede a validar sus accesos.

9. Informar usuario creado

El Jefe de Remuneraciones informa a Subdirector(a) de Remuneraciones la creación del usuario solicitado en sistema Payroll, mediante correo electrónico.

10. Solicitar eliminación cuenta de usuario

Subdirector(a) de Remuneraciones solicita la eliminación de usuario en sistema Payroll, indicando los datos de la persona a eliminar y enviándolo al Jefe de Remuneraciones mediante correo electrónico.

11. Eliminar o bloquear al usuario final

El Jefe de Remuneraciones procede a bloquear o eliminar el usuario en el sistema Payroll.

12. Solicitar eliminación de usuario en Citrix

El Jefe de Remuneraciones procede a solicitar al Proveedor la eliminación del usuario en sistema Citrix, mediante ticket en el portal ADP eService.

13. Eliminar usuario

El Proveedor de servicio procede a eliminar el usuario indicado en el sistema Citrix.

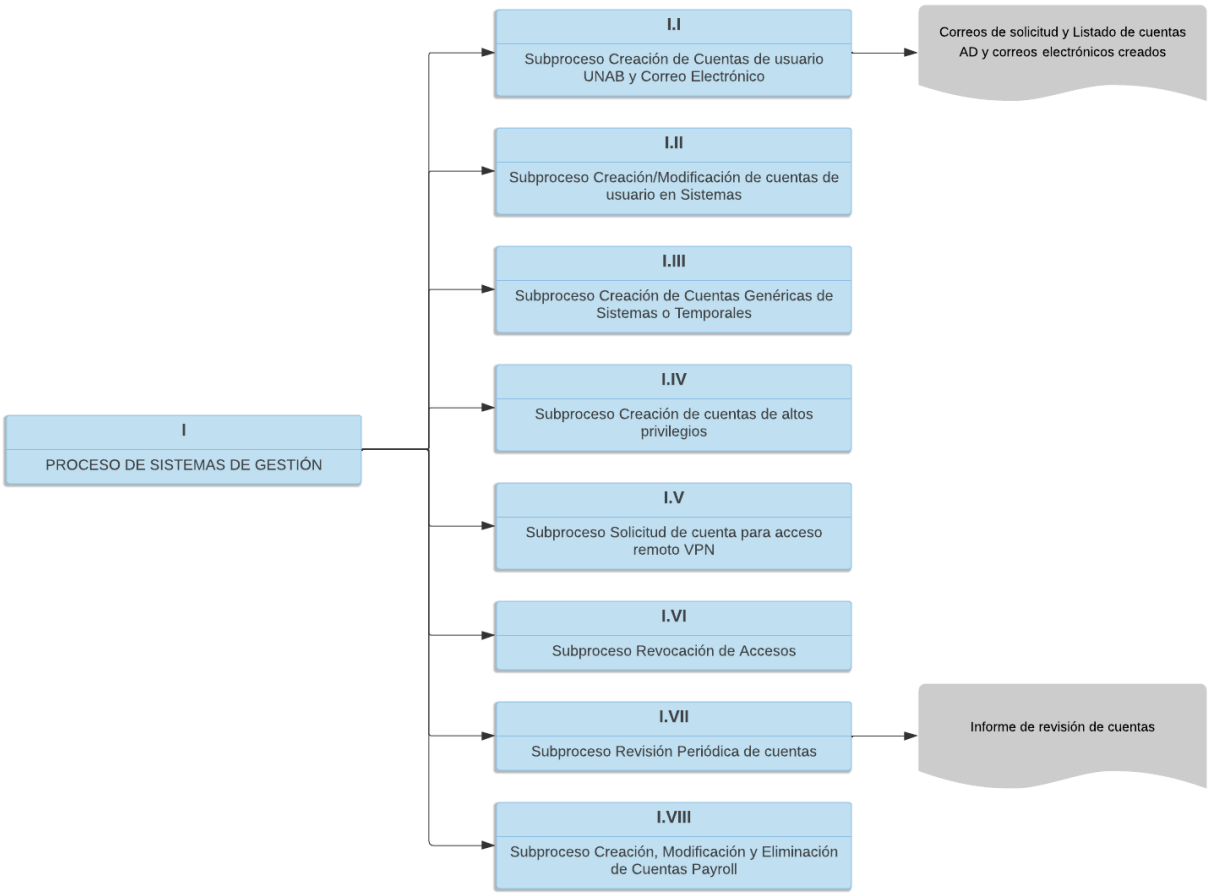
14. Indicar solicitud resuelta

El proveedor de servicio informa la eliminación del usuario al Jefe de Remuneraciones, resolviendo el ticket en portal ADP eService.

15. Informar usuario eliminado

El Jefe de Remuneraciones informa a Subdirector(a) de Remuneraciones la eliminación del usuario solicitado en sistema Payroll, mediante correo electrónico.

Diagrama Subprocesos de Sistemas de Gestión



5.6 Subproceso Revisión de Vulnerabilidades Aplicaciones Nuevas o Modificaciones

Descripción de actividades Subproceso Revisión de Vulnerabilidades Aplicaciones Nuevas o Modificaciones

1. Informar aplicaciones web nuevas o modificaciones a revisar

De acuerdo a definición entregada por la Dirección de Ciberseguridad, cualquier aplicación web nueva o modificación que se realice debe estar alineada al menos con los TOP 10 de OWASP (prácticas de programación segura a nivel mundial). Para evitar múltiples iteraciones con el proveedor o desarrollador UNAB, la Dirección de Ciberseguridad genera un documento en donde se especifica que se debe desarrollar basado en Owasp e informa la herramienta a utilizar para chequear vulnerabilidades.

De acuerdo a lo anterior, cada vez que se desarrolle una aplicación nueva o se realice una modificación a una existente, será responsabilidad del desarrollador de la aplicación (proveedor o desarrollador UNAB) identificar las vulnerabilidades de la aplicación y resolvérselas, o bien, justificar la razón por la cual la vulnerabilidad no puede ser mitigada.

Previo al paso a producción de la modificación o creación de aplicación web, la Dirección de Desarrollo Web o Dirección de Sistemas (según corresponda) deberá informar las vulnerabilidades detectadas en la aplicación con su respectiva justificación a la Dirección de Ciberseguridad, continuando el proceso en la actividad N°3

2. Coordinar análisis de vulnerabilidad detallado para aplicaciones web

Por otro lado, la Dirección de Ciberseguridad podrá coordinar la revisión de vulnerabilidades a través de un Proveedor de Ciberseguridad, quien realizará una revisión detallada de vulnerabilidades para que las aplicaciones pasen con la menor cantidad de vulnerabilidades posibles

El Director de Sistemas o Director de Desarrollo Web deberá informar las aplicaciones web que deberán pasar por este servicio a la Dirección de Ciberseguridad

El Director de Ciberseguridad definirá según disponibilidad del servicio las aplicaciones que podrán pasar por el servicio e informará a la Dirección de Sistemas o la Dirección de Desarrollo Web, según corresponda.

La Dirección de Sistemas/Dirección de Desarrollo Web deberá coordinar la actividad con el proveedor directamente. Una vez realizado el análisis, el proveedor entregará el Informe de Hallazgos, el cual deberá ser enviado a la Dirección de Ciberseguridad, continuando el proceso en la actividad N°3.

3. Autorizar paso a producción

La Dirección de Ciberseguridad analizará cada una de las vulnerabilidades informadas previo a la instalación en producción de la aplicación con el fin de determinar si dichas vulnerabilidades son aceptables o deben ser corregidas.

Las vulnerabilidades a corregir deberán ser informadas a la Dirección de Desarrollo Web/Dirección de Sistemas (según corresponda). Una vez corregidas o justificadas, deberán ser informadas nuevamente a la Dirección de Ciberseguridad para su análisis.

Una vez corregidas o justificadas todas las vulnerabilidades detectadas, la Dirección de Ciberseguridad autorizará el paso a producción de la aplicación.

En caso de corresponder a un proceso crítico y las vulnerabilidades detectadas requieren de un plazo mayor para ser corregidas, la Dirección de Ciberseguridad podrá autorizar el paso a producción de la aplicación con un plan de trabajo comprometido por parte de la Dirección de Desarrollo Web/Dirección de Sistemas (según corresponda).

Diagrama Subproceso Revisión Vulnerabilidades Aplicaciones Nuevas o Modificaciones

5.7 Subproceso Revisión de Cobertura de Herramientas de Seguridad

Descripción Actividades Revisión de Cobertura de Herramientas de Seguridad

1. Enviar reporte diario de cobertura del día anterior

Diariamente, el proveedor que administra las herramientas de seguridad (antivirus, antispam, filtro de navegación), envía un reporte de cobertura del día anterior el cual contiene un compilado de la información de las herramientas de seguridad al día anterior.

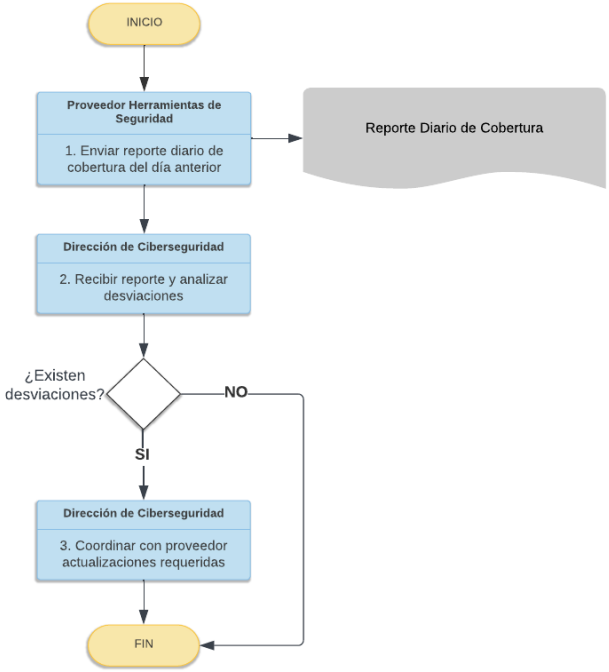
2. Analizar reporte de cobertura

La Dirección de Ciberseguridad analiza diariamente la información recibida de parte del proveedor, la cual corresponde a: estaciones de trabajo con antivirus agrupados por versión, servidores con antivirus agrupados por versión, eventos reportados por estaciones de trabajo, eventos reportados por servidores, cantidad de estaciones y servidores que tienen las firmas actualizadas y eventos de categorías específicas que fueron bloqueados por la plataforma de protección de navegación.

3. Corregir desviaciones

De acuerdo a las desviaciones detectadas, la Dirección de Ciberseguridad coordina con el proveedor la actualización de las nuevas versiones del agente y actualizaciones de firmas, la no actualización oportuna es una de las principales causas por la cual los antivirus son evadidos por software malicioso.

Diagrama Subproceso Revisión de Cobertura de Herramientas de Seguridad



5.8 Subproceso Gestión Semanal de Vulnerabilidades

Descripción Actividades Subproceso Gestión Semanal de Vulnerabilidades

1. Ejecutar escaneo de vulnerabilidades

Semanalmente, se ejecutan Jobs programados de búsqueda de vulnerabilidades en una herramienta de escaneo de vulnerabilidades. El resultado de esta ejecución queda registrado en la consola de la herramienta.

2. Generar reporte personalizado de vulnerabilidades

A partir del resultado anterior, la Dirección de Ciberseguridad genera un reporte personalizado sobre el cual se realiza un análisis de cada una de las vulnerabilidades detectadas.

Las vulnerabilidades detectadas que deben ser corregidas serán informadas a través de correo electrónico al Director de Infraestructura, Director de Sistemas, Oficial de Seguridad y Director de TI, con copia al proveedor del servicio.

3. Coordinar corrección de vulnerabilidades con Proveedor

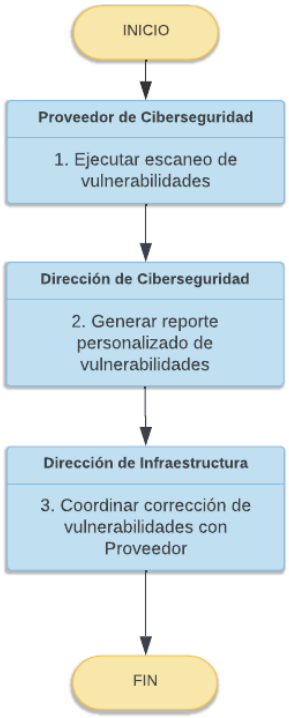
Recibida la información, la Dirección de Infraestructura coordina con el proveedor del servicio la corrección de las vulnerabilidades detectadas.

El Proveedor indicará aquellas vulnerabilidades que pueden ser resueltas a través de parches de seguridad, y para los servidores que están bajo su administración. La Dirección de Infraestructura se definirá que parches aplicar, en qué servidores y coordinará con el Proveedor la fecha para ejecutar los trabajos.

Por otro lado, el proveedor del servicio reportará aquellas vulnerabilidades que requieren actualización de versiones de software para que sean analizadas por la Dirección de Infraestructura, quien determinará si dichas vulnerabilidades podrán ser resueltas internamente, o serán derivadas a la Dirección de Sistemas.

También, podrán existir otras vulnerabilidades que deben ser resueltas realizando acciones sobre los servidores. En este caso, la Dirección de Infraestructura deberá analizar y determinar si las pueden resolver internamente, o deben ser derivadas a la Dirección de Sistemas.

Diagrama Subproceso Gestión Semanal de Vulnerabilidades



5.9 Subproceso Ethical Hacking Externo

Descripción Actividades Subproceso Ethical Hacking Externo

1. Realizar pruebas de explotación

Anualmente, se coordina con un proveedor la realización de pruebas de penetración con la finalidad de identificar vulnerabilidades.

A partir de las vulnerabilidades detectadas, la Dirección de Ciberseguridad coordina con el proveedor pruebas de explotación con la finalidad de evaluar brechas de seguridad.

El proveedor informará los resultados de las pruebas realizadas a la Dirección de Ciberseguridad.

2. Analizar resultados

La Dirección de Ciberseguridad realizará un análisis de los resultados informados y notificará a la Dirección de Sistemas y/o Dirección de Infraestructura, según corresponda, para que corrijan las vulnerabilidades detectadas.

Diagrama Subproceso Ethical Hacking Externo

6. ELEMENTOS DE SALIDA

Nombre documento	Volumen
Listado de accesos creados, revocados, modificados.	1/solicitud
Informe de revisión periódica de cuentas	1/ mes
Notificación de vulnerabilidades a corregir	1 registro por control ejecutado
Informe Final de Equipamiento Tecnológico	1/solicitud

7. INDICADORES DEL PROCESO

- ✓ Presupuesto DGTI.
- ✓ # Sistemas Operativos por tipo.
- ✓ # Servidores por Data center.
- ✓ Capacidad Disponible
- ✓ Cantidad de cuentas creadas/ revocadas / modificadas / Tickets de solicitudes recibidos.

8. REGISTROS

Subproceso	Nombre
Gestión de Infraestructura Tecnológica	Cuadro de Mando de Operaciones
Gestión de Equipamiento	Inventario de Equipamiento
Creación de Cuentas	Correos de solicitud y Listado de cuentas AD y correos electrónicos creados
Revisión Periódica de Cuentas	Informe de revisión de cuentas
Ciberseguridad	Reporte Diario de Cobertura
Ciberseguridad	Reporte de Vulnerabilidades

9. PROTOCOLIZACIÓN

Elaborado por:	Revisado por:	Autorizado por:
		
Diego Baeza de la Hera *Director de Procesos* *Vicerrectoría Económica*	***Luis Aguilar Gallardo*** *Director del SAIC* *Vicerrectoría de Aseguramiento de la Calidad*	***Carmen Gloria Jiménez Bucarey*** *Vicerrectora de Aseguramiento de la Calidad*

10. CONTROL DE CAMBIOS

Versión	Fecha	Elaborado	Descripción del Cambio
1	20-08-2020	Carlos Rojas Rodrigo Ortega Francisco Pérez	Documento Inicial
2	15-10-2021	Matías González	Actualización de Registros
3	20-09-2023	Diego Baeza	Actualización de Procedimiento y Registros