



NORMA ADMINISTRATIVA INTERNA NAI-028-OTI/UIST/004



GESTIÓN DE CAMBIOS DE LA INFRAESTRUCTURA TECNOLÓGICA DEL RENIEC



PRIMERA VERSIÓN

UNIDAD DE INFRAESTRUCTURA Y SOPORTE TECNOLÓGICO



OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN



INDICE

I. OBJETIVO	3
II. BASE LEGAL.....	3
III. DESCRIPCION.....	5
IV. VIGENCIA.....	9
V. APROBACIÓN.....	10
VI. ANEXOS.....	10
ANEXO N° 01_FORMATO DE SOLICITUD DE GESTIÓN DE CAMBIO DE EQUIPOS DE INFRAESTRUCTURA TECNOLÓGICA DEL RENIEC.....	11
ANEXO N° 02_FORMATO DE CATÁLOGO DE CAMBIO DE EQUIPOS DE INFRAESTRUCTURA TECNOLÓGICA DEL RENIEC.....	12
ANEXO N° 03_DEFINICIÓN DE TÉRMINOS	13

I. OBJETIVO

Garantizar la adecuada implementación de los cambios en la infraestructura tecnológica del RENIEC, asegurando la confidencialidad, integridad y disponibilidad de los servicios que presta el RENIEC a nivel nacional.

II. BASE LEGAL

- 2.1 **Ley N° 26497**, Ley Orgánica del Registro Nacional de Identificación y Estado Civil, del 12 de julio de 1995 y sus modificatorias.
- 2.2 **Ley N° 27269**, Ley de Firmas y Certificados Digitales, del 28 de mayo de 2000 y su modificatoria
- 2.3 **Ley N° 27309**, Ley que incorpora los delitos informáticos al Código Penal, del 17 de julio de 2000 y modificatorias.
- 2.4 **Ley N° 27658**, Ley Marco de Modernización de la Gestión del Estado, del 30 de enero de 2002 y sus modificatorias.
- 2.5 **Ley N° 27815**, Ley del Código de Ética de la Función Pública, del 13 de agosto de 2002 y sus modificatorias.
- 2.6 **Ley N° 28716**, Ley de Control Interno de las Entidades del Estado, del 18 de abril de 2006 y sus modificatorias.
- 2.7 **Ley N° 29733**, Ley de Protección de Datos Personales, del 3 de julio de 2011 y sus modificatorias.
- 2.8 **Decreto de Urgencia N° 006-2020**, que crea el Sistema Nacional de Transformación Digital, del 9 de enero de 2020.
- 2.9 **Decreto de Urgencia N° 007-2020**, que aprueba el Marco de Confianza Digital, del 9 de enero de 2020.
- 2.10 **Decreto Legislativo N° 1412**, que aprueba la Ley de Gobierno Digital, del 13 de setiembre de 2018 y su modificatoria.
- 2.11 **Decreto Supremo N° 030-2002-PCM**, que aprueba el Reglamento de la Ley Marco de Modernización de la Gestión del Estado, del 3 de mayo de 2002.
- 2.12 **Decreto Supremo N° 052-2008-PCM**, que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales, del 19 de julio de 2008 y sus modificatorias.
- 2.13 **Decreto Supremo N° 019-2017-JUS**, que aprueba el Reglamento del Decreto Legislativo N° 1353, Decreto Legislativo que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el régimen de protección de datos personales y la regulación de la gestión de intereses, del 15 setiembre de 2017, y sus modificatorias.
- 2.14 **Decreto Supremo N° 016-2024-JUS**, que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales, del 30 de noviembre de 2024.
- 2.15 **Decreto Supremo N° 092-2017-PCM**, que aprueba la Política Nacional de Integridad y Lucha Contra la Corrupción, del 14 de setiembre de 2017.
- 2.16 **Decreto Supremo N° 033-2018-PCM**, que crea de la Plataforma Digital Única del Estado Peruano y establecen disposiciones adicionales para el desarrollo del Gobierno Digital, del 23 de marzo de 2018 y sus modificatorias.

- 2.17 Decreto Supremo N° 042-2018-PCM**, que establece medidas para Fortalecer la Integridad Pública y Lucha Contra la Corrupción del 22 de abril de 2018.
- 2.18 Decreto Supremo N° 044-2018-PCM**, que aprueba el Plan Nacional de Integridad y Lucha Contra la Corrupción 2018-2021, del 26 de abril de 2018; mantiene su vigencia según lo dispuesto en el Decreto Supremo N° 180-2021-PCM del 10 de diciembre de 2021.
- 2.19 Decreto Supremo N° 123-2018-PCM**, que aprueba el Reglamento del Sistema Administrativo de Modernización de la Gestión Pública, del 19 de diciembre de 2018.
- 2.20 Decreto Supremo N° 004-2019-JUS**, que aprueba el Texto Único Ordenado de la Ley N° 27444 Ley del Procedimiento Administrativo General, del 25 de enero de 2019 y sus modificatorias.
- 2.21 Decreto Supremo N° 021-2019-JUS**, que aprueba el Texto Único Ordenado de la Ley 27806, Ley de Transparencia y Acceso a la Información Pública, del 11 de diciembre de 2019, y su modificatoria.
- 2.22 Decreto Supremo N° 029-2021-PCM**, que aprueba el Reglamento del Decreto Legislativo N° 1412 que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, del 19 de febrero de 2021 y su modificatoria.
- 2.23 Decreto Supremo N° 103-2022-PCM**, que aprueba la “Política Nacional de Modernización de la Gestión Pública al 2030”, del 21 de agosto de 2022.
- 2.24 Resolución de Contraloría N° 320-2006-CG**, que aprueba Normas de Control Interno, del 3 de noviembre de 2006.
- 2.25 Resolución de Contraloría N° 146-2019-CG**, que aprueba la Directiva N° 006-2019-CG/INTEG “Implementación del Sistema de Control Interno en las entidades del Estado”, del 17 de mayo de 2019 y sus modificatorias.
- 2.26 Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD**, que aprueba la Directiva N° 001-2023-PCM/SGTD, Directiva que establece el perfil y responsabilidades del Oficial de seguridad y confianza digital, del 8 de setiembre de 2023.
- 2.27 Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD**, que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas, del 8 de setiembre de 2023.
- 2.28 Resolución Directoral N° 022-2022-INACAL/DN**, que aprueba la Norma Técnica Peruana NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición. Reemplaza a la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, del 12 de enero de 2023.
- 2.29 Resolución Jefatural N° 000176-2022/JNAC/RENIEC**, que aprueba la conformación del Equipo de respuestas ante incidentes en seguridad digital del Registro Nacional de Identificación y Estado Civil - RENIEC, del 12 de octubre de 2022.

- 2.30 Resolución Jefatural N° 000153-2023/JNAC/RENIEC**, que aprueba la Política y Objetivos de Seguridad de la Información del Registro Nacional de Identificación y Estado Civil - RENIEC, del 18 de setiembre 2023.
- 2.31 Resolución Jefatural N° 000185-2023/JNAC/RENIEC**, que resuelve reconformar el Comité de Gobierno Digital del Registro Nacional de Identificación y Estado Civil - RENIEC, constituido mediante Resolución Jefatural N° 000107-2019/JNAC/RENIEC (22JUL2019) y reconformado por las Resoluciones Jefaturales N° 000156-2019/JNAC/RENIEC (26SET2019), N° 000183-2020/JNAC/RENIEC (17NOV2020) y N° 000022-2022/JNAC/RENIEC (14FEB2022) y modificado mediante la Resolución Jefatural N° 000147-2023/JNAC/RENIEC (01SET2023); del 21 de noviembre de 2023.
- 2.32 Resolución Jefatural N° 000061-2024/JNAC/RENIEC**, que aprueba el Reglamento de Organización y Funciones y la Estructura Orgánica del Registro Nacional de Identificación y Estado Civil - RENIEC, del 11 de abril de 2024.
- 2.33 Resolución Jefatural N° 000067-2024/JNAC/RENIEC**, que aprueba el Cuadro de Equivalencias y Siglas de las unidades de organización del Registro Nacional de Identificación y Estado Civil - RENIEC, del 22 de abril de 2024.
- 2.34 Resolución Secretarial N° 000084-2024/SGEN/RENIEC**, que aprueba la Directiva DI-001-OPPM/001 “Documentos Normativos del RENIEC”, del 8 de julio 2024.
- 2.35 Resolución Secretarial N° 000121-2024/SGEN/RENIEC**, que aprueba la Directiva DI-038-OTI/003 “Controles Tecnológicos de Seguridad de la información del SGSI - RENIEC”, primera versión, del 10 de octubre de 2024.
- 2.36 Norma Internacional ISO 27001:2022** Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos; publicada el 25 octubre de 2022.

III. DESCRIPCION

3.1 DE LAS CONSIDERACIONES GENERALES

3.1.1 La presente norma administrativa interna describe los lineamientos para efectuar la gestión de cambios de los equipos de la infraestructura tecnológica del RENIEC, así como evaluar y determinar el impacto, autorización, implantación e implementación del cambio.

3.1.2 Los coordinadores de los servicios de la infraestructura tecnológica de la UIST deben seguir los lineamientos de la presente norma administrativa interna cuando se realicen mantenimientos, actualizaciones o cambios de los equipos de la infraestructura tecnológica del RENIEC.

Las fuentes u orígenes para la gestión de cambios se generan por:

- Proyectos o ajustes requeridos en la infraestructura tecnológica
- Mantenimientos correctivos o preventivos en la infraestructura tecnológica.
- Retiro, ingreso o cambios de servicios de TI.

- Gestión de incidentes. (Alertas de seguridad)
- Actualizaciones de soluciones
- Por cambio de proveedor.
- Por actualización y configuración en el hardware de servidores, equipos informáticos, colaboración, redes e infraestructura física de comunicación.
- Mejora e innovaciones de los servicios de la Entidad.
- Por obsolescencia tecnológica de los equipos de la Infraestructura Tecnológica del RENIEC.
- Otros (cualquier servidor, ciudadano o proveedor puede sugerir mejoras en los servicios que pueden requerir cambios en la infraestructura tecnológica).
- Gestiones fuera del alcance de gestión de cambios:
- Recuperación de desastres.
- Los cambios realizados en el proceso de soporte diario como son:
 - ✓ Gestión de contraseñas.
 - ✓ Gestión de cuentas usuarios.
 - ✓ Reinicio de sistemas, aplicaciones o equipos.
 - ✓ Cambios de permisos de archivos.
 - ✓ Cambios en los perfiles y/o permisos de navegación de usuarios.
 - ✓ Publicación de información en la página web o intranet.

3.2 DE LA SOLICITUD DE CAMBIO

3.2.1 Los coordinadores de los servicios de la infraestructura tecnológica de la UIST realizan un control permanente y/o análisis técnico del estado de operatividad de la infraestructura tecnológica e identifican la necesidad del cambio generada por los motivos indicados en el numeral 3.1.2.

En el “Catálogo de Cambios de Equipos de la Infraestructura Tecnológica del RENIEC” – Anexo 02, se describen los cambios en la infraestructura tecnológica y sirve de orientación para los diferentes actores en las actividades de este documento normativo

3.2.2 Los coordinadores de los servicios de la infraestructura tecnológica de la UIST según sea el caso, convocan cuando se requiera, la participación de uno o más usuarios a fin de tener una mejor comprensión de la problemática e identificar la necesidad del cambio.

3.2.3 Los coordinadores de los servicios de la infraestructura tecnológica de la UIST según corresponda, registran la gestión de cambios de la infraestructura tecnológica del RENIEC en el “Formato de Solicitud de Gestión de Cambios de Equipos de la Infraestructura Tecnológica del RENIEC” - Anexo 01, cuando se realicen mantenimientos, actualizaciones o cambios de los equipos de la infraestructura tecnológica del RENIEC de acuerdo con el numeral 3.1.2.

El analista del servicio de la UIST que corresponde el cambio debe registrar la solicitud de gestión de cambio en la “Herramienta Tecnológica para Gestión de Servicios TI” de Mesa de Ayuda/Servicios para la atención de uno de los coordinadores de servicios de infraestructura de la UIST.

3.3 ANÁLISIS Y VALIDACIÓN DEL CAMBIO

3.3.1 Los coordinadores de los servicios de la infraestructura tecnológica de la UIST, según sea el caso, evalúan la solicitud de gestión de cambio considerando el impacto y la naturaleza del cambio.

Impacto

Para la evaluación de la solicitud debe tomar en cuenta las siguientes consideraciones:

El impacto determina la importancia de los equipos de la infraestructura tecnológica del RENIEC dependiendo de cómo éste afecta a los procesos del negocio y/o del número de usuarios afectados. El impacto puede ser: crítico, alto, medio y bajo.

- Crítico:** Cuando la falla de los equipos de la infraestructura tecnológica del RENIEC afecta a toda la organización. Por ejemplo, falla de los servidores de base de datos, servidores de aplicaciones, equipo de comunicaciones instalado en el Centro de Datos de la Sede Operativa.
- Alto:** Cuando la falla de los equipos de la infraestructura tecnológica del RENIEC afecta gravemente algunos usuarios o a un gran número de usuarios o a una de las sedes del RENIEC. Por ejemplo, falla de servidores de bases de datos y servidores de aplicaciones afectan en la atención al público, falla del equipo de comunicaciones afecta la conectividad y el uso de los servicios y aplicaciones en una de las sedes.
- Medio:** Cuando la falla de los equipos de la infraestructura tecnológica del RENIEC afecta a los locales RENIEC. Por ejemplo, si la falla de los servidores de la base de datos y servidores de aplicaciones falla del equipo de comunicaciones afecta a la Oficina Registral de Jesús María.
- Bajo:** Cuando la falla de los equipos de la infraestructura tecnológica del RENIEC afecta a una de las áreas internas. Por ejemplo, si la falla de equipos de colaboración de equipos informáticos afecta al usuario.

El resultado de la evaluación se registra en el “Solicitud de Gestión de Cambios de Equipos de la Infraestructura Tecnológica del RENIEC” - Anexo N° 01.

Naturaleza del cambio

3.3.2 Los coordinadores de los servicios de la infraestructura tecnológica de la UIST según sea el caso, en base a la evaluación del impacto realizado, definen la naturaleza del cambio a realizar de acuerdo con las siguientes consideraciones:

Cambios estándar: Son cambios de bajo riesgo y su manejo es de amplio conocimiento por parte del equipo que los desarrolla y caracterizadas por:

- Las actividades para realizar son las mismas.
- Los riesgos son similares y se mitigan de igual o similar forma.
- Las acciones de verificación son las mismas.
- Los recursos y el tiempo de implementación no impactan la operación habitual de servicios de T.I.
- Se puede implementar en horas de la noche o en el día sin mayor impacto para la entidad.

Cambios normales: Son cambios que se deben programar con periodicidad recurrente (Semestral o anual), y cumplen las siguientes características:

- Tiene un impacto en la plataforma tecnológica y en los servicios TI que modifican la configuración de los componentes de TI.
- Involucran interrupción de servicios de TI y son visibles para los usuarios finales.
- Se requiere realizar actividades para asegurar la integridad, disponibilidad y confidencialidad de la información, como por ejemplo copias de respaldo en procesos de migración.
- Existe el riesgo de que los resultados esperados no se obtengan.
- Implican acciones complejas y/o amplios espacios de tiempo en su implementación.

Cambios de emergencia: Son cambios que deben implementarse lo antes posible; por ejemplo, para resolver un incidente o implementar un parche de seguridad. Los cambios de emergencia no se suelen incluirse en un cronograma, dado que se presentan sin previo aviso y requieren ejecutarse de manera inmediata en pro de la seguridad de la información.

El resultado de la definición de la naturaleza del cambio se registra en el formato “Solicitud de Gestión de Cambios de equipos de la infraestructura tecnológica del RENIEC” - Anexo N° 01.

3.3.3 En caso de que se dispongan de los recursos necesarios para la realización del cambio, los coordinadores de los servicios de la infraestructura tecnológica de la UIST aprueban la realización del cambio, y se coordina con el usuario o usuarios involucrados.

3.3.4 Si los recursos asociados a la naturaleza del cambio son complejos o implican un presupuesto mayor, los coordinadores de los servicios de la infraestructura tecnológica de la UIST envían a través del correo electrónico el “Formato de Solicitud de Gestión de Cambios Equipos de la Infraestructura Tecnológica del RENIEC” – Anexo N° 01, con los resultados de la evaluación al jefe de la UIST.

3.3.5 El jefe de la UIST coordina con el jefe de la OTI de ser necesario, a fin de definir la aprobación del cambio, gestionando con el usuario o usuarios los recursos necesarios para realizar del cambio o si se requiere desarrollar un proyecto de Tecnología de información. A que te refieres proyecto de tecnología.

3.1.6 El jefe de la UIST es el responsable de aprobar o rechazar la solicitud de cambio y registrar la aprobación o rechazo de la evaluación en el “Formato de “Solicitud de Control de Cambios de

Equipos de la Infraestructura Tecnológica del RENIEC” - Anexo N° 01.

3.4 IMPLEMENTACIÓN DEL CAMBIO

3.4.1 En el caso de cambios que puedan realizarse con los recursos existentes, el coordinador del servicio de infraestructura tecnológica de la UIST correspondiente designa al especialista o equipo de especialistas para la implementación del cambio.

3.4.2 Cuando los cambios requieran recursos adicionales de los existentes y se necesite la coordinación y aprobación de un ente superior, el jefe de la UIST, en coordinación con el coordinador del servicio de infraestructura tecnológica correspondiente, designa al especialista o equipo de especialistas para la implementación del cambio.

3.4.2 El especialista o el líder del equipo de implementación del cambio de la UIST registra las actividades a realizar para la implementación del cambio en el “Formato de Solicitud de Gestión de Cambios de Equipos de la Infraestructura Tecnológica del RENIEC” - Anexo N° 01.

3.5 VALIDACIÓN DE LA DE LA IMPLEMENTACIÓN DEL CAMBIO

3.5.1 El coordinador del servicio de infraestructura tecnológica correspondiente realiza el monitoreo y seguimiento de la solicitud de gestión de cambio hasta la implementación, asimismo supervisa el cierre de la solicitud en la Herramienta Tecnológica para Gestión de Servicios TI de Mesa de Ayuda/Servicios de la UIST.

3.6 CIERRE DE LA SOLICITUD DE CAMBIO

3.6.1 El especialista y/o el líder del equipo de implementación del cambio de la UIST una vez concluida con la implementación registra los resultados en el “Formato de Solicitud de Gestión de Cambios de Equipos de la Infraestructura Tecnológica del RENIEC” - Anexo N° 01.

3.6.2 El especialista y/o el líder del equipo de implementación del cambio de la UIST y el coordinador o los coordinadores de servicios de infraestructura tecnológica de la UIST según sea el caso, una vez atendida la solicitud de cambio, firman digitalmente en el “Formato de Solicitud de Gestión de Cambios de Equipos de la Infraestructura Tecnológica del RENIEC” - Anexo N° 01.

3.6.3 El especialista y/o líder del equipo de implementación del cambio de la UIST registra la solución, adjunta el “Formato de Solicitud de Gestión de Cambios de Equipos de la Infraestructura Tecnológica del RENIEC” firmado digitalmente y realiza el cierre del ticket en la Herramienta Tecnológica para Gestión de Servicios TI de Mesa de Ayuda/Servicios de la UIST.

IV. VIGENCIA

La presente Norma Administrativa Interna entra en vigencia a partir de su aprobación.

V. APROBACIÓN

Se aprueba mediante Resolución de Oficina.

VI. ANEXOS



ANEXO N° 01
FORMATO DE SOLICITUD DE GESTIÓN DE CAMBIO DE EQUIPOS DE
INFRAESTRUCTURA TECNOLÓGICA DEL RENIEC

		SOLICITUD DE GESTIÓN DE CAMBIO DE EQUIPOS DE LA INFRAESTRUCTURA TECNOLÓGICA DEL RENIEC	
DATOS DEL FORMATO: CÓDIGO PIET-P-SCEIT-36/UIST/OTI/REN Versión: 01 Fecha Emisión: 26/02/2025 Fecha Actualización: 26/02/2025			
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL		N° SOLICITUD: 0001/UIST FECHA DE EMISIÓN: 7/02/2025	
DATOS DEL FUNCIONARIO SOLICITANTE			
OFICINA:			
UNIDAD:			
NOMBRES Y APELLIDOS:			
DATOS DEL SERVIDOR SOLICITANTE			
Nombres y Apellidos:		Teléfono de contacto:	
Ubicación:		Sede Nicolas de Piérola Piso: 5 Dirección: Jr. Nicolas de Piérola	
DATOS DEL REQUERIMIENTO			
Tipo de Cambio:			
Mantenimientos correctivos o preventivos		☒ Proyectos o ajustes en la infraestructura tecnológica	
Retiro, ingreso o cambios de servicios de TI		☐ Actualización y configuración en el hardware de la Infraestructura Tecnológica	
Gestión de incidentes		☐ Mejora e innovaciones de los servicios	
Actualizaciones de soluciones		☐ Por obsolescencia tecnológica.	
Por cambio del proveedor		☐ Otros	
DESCRIPCIÓN DEL CAMBIO			
EVALUACIÓN DEL IMPACTO DEL CAMBIO			
Responsable de la Evaluación:			
Impacto:		Recursos necesarios:	
Crítico ☒			
Alto ☐			
Medio ☐			
Bajo ☐			
Tipo de cambio			
Estandar ☒			
Normal ☐			
Emergencia ☐			
APRUBACION DEL CAMBIO POR EL COORDINADOR DEL SERVICIO			
Estado de la Solicitud:		Aprobado ☐ Rechazado ☐ Fecha:	
Nombres y apellidos: Coordinador(e)s del(os) servicio(s) responsable			
Comentarios:			
APROBACION DEL CAMBIO POR EL JEFE DE LA UNIDAD			
Estado de la Solicitud:		Aprobado ☐ Rechazado ☐ Fecha:	
Nombres y apellidos:			
IMPLANTACIÓN DEL CAMBIO			
Líder de Implementación: (Especialista de la UIST)		Nombres y Apellidos	
		1	
Responsables de la Implementación: (Analista de la UIST)		2	
		3	
IMPLEMENTACIÓN DEL CAMBIO			
Descripción de las actividades implementadas		Resultados de la implementación	
Estado inicial		Estado final	

CATALOGO DE CAMBIOS DE EQUIPOS DE LA INFRAESTRUCTURA TECNOLÓGICA DEL RENIEC

DATOS DEL FORMULARIO:

CÓDIGO: PBT-F-CCST-2400570101RENIEC
Versión: 01
Fecha Emisión: 26/03/2025
Fecha Actualización: 26/03/2025

SERVICIO / PROCESO

ACTIVO

TIPO DE ACTIVO

DIRECCIÓN / OFICINA

DESCRIPCIÓN DEL CAMBIO

Impacto

Bajo Estándar (Pre-aprobado)

Medio

Alto (A aprobar por Jefe Unidad)

Crítico (A aprobar por Jefe Unidad)

Grupo de personas

Sede/Oficina

Toda la organización

Tipos de cambio

Emergencia

Normal

Estándar

Se Libera con Ventana de mantenimiento

SERVICIO / PROCESO

ACTIVO

TIPO DE ACTIVO

DIRECCIÓN / OFICINA

DESCRIPCIÓN DEL CAMBIO

Impacto

Bajo Estándar (Pre-aprobado)

Medio

Alto (A aprobar por Jefe Unidad)

Crítico (A aprobar por Jefe Unidad)

Grupo de personas

Sede/Oficina

Toda la organización

Urgencia

Emergencia

Normal

Estándar

Se Libera con Ventana de mantenimiento

SERVICIO / PROCESO

ACTIVO

TIPO DE ACTIVO

DIRECCIÓN / OFICINA

DESCRIPCIÓN DEL CAMBIO

Impacto

Bajo Estándar (Pre-aprobado)

Medio

Alto (A aprobar por Jefe Unidad)

Crítico (A aprobar por Jefe Unidad)

Grupo de personas

Sede/Oficina

Toda la organización

Urgencia

Emergencia

Normal

Estándar

Se Libera con Ventana de mantenimiento

SERVICIO / PROCESO

ACTIVO

TIPO DE ACTIVO

DIRECCIÓN / OFICINA

DESCRIPCIÓN DEL CAMBIO

Impacto

Bajo Estándar (Pre-aprobado)

Medio

Alto (A aprobar por Jefe Unidad)

Crítico (A aprobar por Jefe Unidad)

Grupo de personas

Sede/Oficina

Toda la organización

Urgencia

Emergencia

Normal

Estándar

Se Libera con Ventana de mantenimiento

SERVICIO / PROCESO

ACTIVO

TIPO DE ACTIVO

DIRECCIÓN / OFICINA

DESCRIPCIÓN DEL CAMBIO

Impacto

Bajo Estándar (Pre-aprobado)

Medio

Alto (A aprobar por Jefe Unidad)

Crítico (A aprobar por Jefe Unidad)

Grupo de personas

Sede/Oficina

Toda la organización

Urgencia

Emergencia

Normal

Estándar

Se Libera con Ventana de mantenimiento

SERVICIO / PROCESO

ACTIVO

TIPO DE ACTIVO

DIRECCIÓN / OFICINA

DESCRIPCIÓN DEL CAMBIO

Impacto

Bajo Estándar (Pre-aprobado)

Medio

Alto (A aprobar por Jefe Unidad)

Crítico (A aprobar por Jefe Unidad)

Grupo de personas

Sede/Oficina

Toda la organización

Urgencia

Emergencia

Normal

Estándar

Se Libera con Ventana de mantenimiento

SERVICIO / PROCESO

ACTIVO

TIPO DE ACTIVO

DIRECCIÓN / OFICINA

DESCRIPCIÓN DEL CAMBIO

Impacto

Bajo Estándar (Pre-aprobado)

Medio

Alto (A aprobar por Jefe Unidad)

Crítico (A aprobar por Jefe Unidad)

Grupo de personas

Sede/Oficina

Toda la organización

Urgencia

Emergencia

Normal

Estándar

Se Libera con Ventana de mantenimiento

SERVICIO / PROCESO

ACTIVO

TIPO DE ACTIVO

DIRECCIÓN / OFICINA

DESCRIPCIÓN DEL CAMBIO

Impacto

Bajo Estándar (Pre-aprobado)

Medio

Alto (A aprobar por Jefe Unidad)

Crítico (A aprobar por Jefe Unidad)

Grupo de personas

Sede/Oficina

Toda la organización

Urgencia

Emergencia

Normal

Estándar

Se Libera con Ventana de mantenimiento

SERVICIO / PROCESO

ACTIVO

TIPO DE ACTIVO

DIRECCIÓN / OFICINA

DESCRIPCIÓN DEL CAMBIO

Impacto

Bajo Estándar (Pre-aprobado)

Medio

Alto (A aprobar por Jefe Unidad)

Crítico (A aprobar por Jefe Unidad)

Grupo de personas

Sede/Oficina

Toda la organización

Urgencia

Emergencia

Normal

Estándar

Se Libera con Ventana de mantenimiento

SERVICIO / PROCESO

ACTIVO

TIPO DE ACTIVO

DIRECCIÓN / OFICINA

DESCRIPCIÓN DEL CAMBIO

Impacto

Bajo Estándar (Pre-aprobado)

Medio

Alto (A aprobar por Jefe Unidad)

Crítico (A aprobar por Jefe Unidad)

Grupo de personas

Sede/Oficina

Toda la organización

Urgencia

Emergencia

Normal

Estándar

Se Libera con Ventana de mantenimiento

SERVICIO / PROCESO

ACTIVO

TIPO DE ACTIVO

DIRECCIÓN / OFICINA

DESCRIPCIÓN DEL CAMBIO

Impacto

Bajo Estándar (Pre-aprobado)

Medio

Alto (A aprobar por Jefe Unidad)

Crítico (A aprobar por Jefe Unidad)

Grupo de personas

Sede/Oficina

Toda la organización

Urgencia

Emergencia

Normal

Estándar

Se Libera con Ventana de mantenimiento

SERVICIO / PROCESO

ACTIVO

TIPO DE ACTIVO

DIRECCIÓN / OFICINA

DESCRIPCIÓN DEL CAMBIO

Impacto

Bajo Estándar (Pre-aprobado)

Medio

Alto (A aprobar por Jefe Unidad)

Crítico (A aprobar por Jefe Unidad)

Grupo de personas

Sede/Oficina

Toda la organización

Urgencia

Emergencia

Normal

Estándar

Se Libera con Ventana de mantenimiento

ANEXO N° 03 DEFINICIÓN DE TÉRMINOS

1. Analista de la Unidad de Infraestructura y Soporte Tecnológico

Se considera a los analistas de las áreas de infraestructura física de comunicaciones, redes y seguridad.

2. Cambio

Consiste en añadir, modificar o eliminar cualquier funcionalidad a un equipo que pudiera tener un efecto en los servicios de TI.

3. Confidencialidad

Propiedad de preservar restricciones autorizadas sobre el acceso y la divulgación, incluidos los medios para la protección de la privacidad y la propiedad de la información. La información no puede ser transmitida ni eliminada por cambios no autorizados o accidentales.

4. Coordinadores de servicios de la infraestructura de la Unidad de Infraestructura y Soporte Tecnológico UIST

Se considera a los coordinadores de las áreas de centro de datos y servidores, base de datos, redes y telecomunicaciones, seguridad informática y soporte técnico responsables de administrar, dirigir, coordinar las actividades del área a su cargo.

5. Disponibilidad

Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. Esta disponibilidad podrá estar sujeta en acuerdos de nivel de servicio o SLA.

6. Equipos de comunicación

Están considerados como equipos de comunicación: Switches, router, gabinete comunicaciones, Access Point, equipos de radioenlaces, equipos de videoconferencia y telefonía IP.

7. Equipos de seguridad digital

Están considerados como equipos de seguridad los servidores dedicados: Antivirus, WAF, filtro de contenidos, firewall perimetral, balanceador de carga, etc.

8. Especialista de la Unidad de Infraestructura y Soporte Tecnológico

Se considera a los especialistas de las áreas del centro de datos, infraestructura física, comunicaciones, redes, seguridad.

9. Gestión de cambios

Es la práctica formal que atiende, gestiona y asegura los cambios en un producto, proceso o sistema en el ámbito de los servicios de TI, que se introduce e implementa de forma controlada y coordinada, con el fin de minimizar la probabilidad de interrupción, alteraciones no autorizadas y errores mediante el análisis, la implementación y el seguimiento de todos los cambios solicitados y hechos.

10. Herramienta Tecnológica para Gestión de Servicios TI

Herramienta informática de la Unidad de Infraestructura y Soporte Tecnológico (UIST) que permite gestionar las solicitudes e incidencias de manera oportuna, con el apoyo de las áreas especializadas de TI.

11. Infraestructura Tecnológica del RENIEC

Comprende el Centro de Datos, servidores, equipos informáticos, seguridad digital, colaboración, redes e infraestructura física de comunicaciones.

12. Integridad

Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos. El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

La protección contra la modificación o destrucción de información inapropiada, e incluye el no repudio y la autenticidad de la información

13. Líder de implementación del cambio de la Unidad de Infraestructura y Soporte Tecnológico

Se considera a los líderes de las áreas de áreas de centro de datos y servidores, base de datos, redes y telecomunicaciones, seguridad informática y soporte técnico que dirigen la implementación de cambios.

14. Mesa de Ayuda/Servicios

Conjunto de recursos tecnológicos y humanos, para gestionar incidencias y requerimientos, relacionados a las tecnologías de la información y la comunicación (TIC) de manera integral, con escalamiento a las áreas especializadas de TI, siendo el objetivo principal la resolución de incidentes.

15. No repudio (Evitar el rechazo)

El aseguramiento de que un ente no puede negar en forma posterior el haber originado datos, provisión de pruebas de integridad y origen de los datos que pueden ser verificado por terceros. Una firma digital puede proveer no repudio.

16. Seguridad

Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.

17. Seguridad Digital

La seguridad digital es la protección del contenido de los dispositivos conectados a Internet de intrusos, que podrían caer en piratería, phishing y más, por lo que es una práctica fundamental de protección de información personal, como los datos privados y datos sensibles.

18. Seguridad de la Información

Es el conjunto de medidas que permiten resguardar y proteger la información buscando mantener la confidencialidad, disponibilidad e integridad de los activos de información. Es la base que promueve la implantación del Sistema de Gestión de Seguridad de la Información, teniendo además como otras medidas técnicas que colaboran para este marco: la ciberseguridad, seguridad informática y protección de datos personales.

19. Seguridad Informática y/o Ciberseguridad

La seguridad informática o ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en la red interna LAN y del ciberespacio

