NORMA ADMINISTRATIVA INTERNA
NAI-023/OTI/UIST/001

ADMINISTRACIÓN DEL CENTRO DE DATOS Y CUARTOS DE TELECOMUNICACIONES

PRIMERA VERSIÓN

UNIDAD DE INFRAESTRUCTURA Y SOPORTE TECNOLÓGICO

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

ÍNDICE

I. OBJETIVO

Establecer los lineamientos para la administración de los Centros de Datos (sala de servidores y sala de telecomunicaciones) y cuartos de telecomunicaciones a nivel nacional, asegurando la disponibilidad, integridad y confidencialidad de la información.

II. BASE LEGAL

2.1 **Ley Nº 26497**, Ley Orgánica del Registro Nacional de Identificación y Estado Civil - RENIEC, del 12 de julio de 1995 y sus modificatorias.

2.2 **Ley Nº 27269**, Ley de Firmas y Certificados Digitales, del 28 de mayo de 2000 y sus modificatorias.

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 Nº 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 Nº 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 Nº 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 Nº 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 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 19 de agosto 2022.

2.24 Resolución de Contraloría Nº 320-2006-CG, que aprueba Normas de Control Interno, del 3 de noviembre de 2006.

2.25 Resolución de Contraloría Nº 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 Nº 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 Nº 000056-2024/JNAC/RENIEC**, que aprueba el Plan Estratégico Institucional (PEI) correspondiente al período 2021 - 2027 Ampliado del Registro Nacional de Identificación y Estado Civil - RENIEC, del 29 de marzo de 2024.

2.33 **Resolución Jefatural Nº 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.

2.34 **Resolución Jefatural Nº 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.

2.35 **Resolución Secretarial Nº 000084-2024/SGEN/RENIEC**, que aprueba la Directiva DI-001-OPPM/001 “Documentos Normativos del RENIEC” Primea versión, del 8 de julio 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

La Unidad de Infraestructura y Soporte Tecnológico – UIST de la Oficina de Tecnología de la Información- OTI es la encargada de la administración del Centro de Datos (sala de servidores y sala de telecomunicaciones) y cuartos de telecomunicación a nivel nacional y de velar por la operatividad de los servidores y de los equipos del comunicación y seguridad digital para asegurar la disponibilidad, integridad y confidencialidad de la información.

3.1 DEL ACCESO FÍSICO AL CENTRO DE DATOS

3.1.1 El acceso al Centro de Datos es restringido y está clasificado en tres tipos de acceso

- **Acceso directo,** se otorga a los servidores civiles que por la naturaleza de sus funciones tienen acceso permanente a las instalaciones del Centro de Datos y no requiere autorización expresa y figuran en el formato “Relación de Personal con Acceso Directo al Centro de Datos”, que se indica en el Anexo 01.

- **Acceso Autorizado,** se otorga a los servidores civiles que requieren ingresar al Centro de Datos eventualmente y deben figurar en la lista de servidores civiles autorizados que figuran en el, formato “Relación de Personal con Acceso Autorizado al Centro de Datos”, que se indica en el Anexo 02 y registrar su ingreso.

- **Accesos Especiales,** se otorga excepcionalmente a personal diverso (servidores civiles de RENIEC de otras UUOO, consultores, visitas externas, proveedores entre otros) y requiere autorización expresa del Supervisor del Centro de Datos, Jefe de la UIST o el Jefe de la OTI. Deben registrar su ingreso en el formato "Bitácora de Control de Acceso del Centro de Datos" - Anexo 3.

3.1.2 El servidor civil con acceso directo al Centro de Datos debe realizar su ingreso haciendo uso de los siguientes medios que se encuentra en la puerta de ingreso: tarjeta o control biométrico (registrando su huella dactilar) u otro mecanismo que disponga el órgano competente en esta materia.

3.1.3 El personal de los proveedores que prestan servicios de mantenimiento y soporte deben ingresar al Centro de Datos con las herramientas y materiales indispensables para su trabajo; si se presentan con mochilas y/o bolsos, éstos son revisados por el personal de vigilancia (en busca de equipos tecnológicos, memorias o documentos en físico) y registrados para su posterior verificación a la hora de su retiro u otras disposiciones dadas por el Órgano competente.

3.1.4 El servidor civil del RENIEC o personal de los proveedores, al momento de ingresar al Centro de Datos, acepta y reconoce la existencia de una cláusula de confidencialidad (para los proveedores o locadores cláusula especificada generalmente en el TDR, orden de compra o servicio o documento similar), en la cual se especifica la no divulgación de información de la infraestructura, equipos y documentación del RENIEC.

3.1.5 El servidor civil y los proveedores del RENIEC están prohibidos de tomar fotos al Centro de Datos.

3.1.6 El servidor civil del RENIEC o los proveedores que incumplan con lo dispuesto en el numeral que antecede será retirado del Centro de Datos.

3.1.7 Para el ingreso o salida de materiales y/o equipos a ser instalados o retirados al Centro de Datos, el servidor civil debe verificar la guía de ingreso/salida del proveedor e informar al supervisor del Centro de Cómputo y/o Jefe de la UIST.

3.2 DEL ACCESO FÍSICO A LOS CUARTOS DE TELECOMUNICACIÓN

3.2.1 El acceso a los cuartos de comunicaciones es restringido. Solo pueden acceder los analistas de infraestructura física de comunicaciones y/o los asistentes informáticos.

3.2.2 El acceso del personal de los proveedores o terceras personas a los cuartos de comunicaciones es autorizado por la UIST a través de correos electrónicos o de documentos emitidos por el SITD.

3.2.3 El personal de los proveedores que prestan servicios de mantenimiento y soporte deben ingresar al cuarto de comunicaciones con las herramientas y materiales indispensables para su trabajo; si se presentan con mochilas y/o bolsos, éstos son

revisados por el personal de vigilancia (en busca de equipos tecnológicos, memorias o documentos en físico) y registrados para su posterior verificación a la hora de su retiro, de acuerdo con las disposiciones dadas por el Órgano competente.

3.2.4 El personal del RENIEC o de los proveedores, al momento de ingresar a los cuartos de comunicaciones, acepta y reconoce la existencia de una cláusula de confidencialidad (para los proveedores cláusula especificada generalmente en el TDR, orden de compra o servicio o documento similar), en la cual se especifica la no divulgación de información de la infraestructura, equipos y documentación del RENIEC.

3.2.5 El servidor civil y los proveedores del RENIEC están prohibidos de tomar fotos al cuarto de comunicaciones.

3.2.6 Los analistas de infraestructura física de comunicaciones y/o los asistentes informáticos, para el ingreso o salida de un equipo de comunicación, deben verificar la guía de salida/ingreso del proveedor e informar a la UIST.

3.3 DE LA PROTECCIÓN FÍSICA DEL CENTRO DE DATOS

3.3.1 El Supervisor del Centro de Datos controla el cumplimiento de los lineamientos establecidos para la protección física del Centro de Datos; así como las condiciones ambientales (temperatura, humedad, y carga eléctrica) con la finalidad de mantener operativos los servidores.

3.3.2 Se debe contar con un servicio de mantenimiento preventivo y correctivo que asegure la continuidad de las operaciones de la Sala de Servidores y Telecomunicaciones del Centro de Datos con el fin de salvaguardar la integridad y disponibilidad de los activos de información que el RENIEC ofrece a entidades públicas, privadas y ciudadanía.

3.3.3 El Supervisor del Centro de Datos es el responsable de la elaboración del Plan de Mantenimiento Preventivo del Centro de Datos.

3.3.4 El servicio de mantenimiento preventivo y correctivo considera todos los bienes, componentes, accesorios y/o dispositivos, que conforman y permiten el óptimo funcionamiento de la Sala de Servidores y Sala de Telecomunicaciones, los cuales hacen posible la operatividad y disponibilidad de los servicios informáticos.

3.3.5 Para la instalación de un nuevo equipo de comunicación y/o seguridad digital en la sala de comunicaciones se debe estimar la cantidad de carga eléctrica (voltaje) que consumirá y validar que se cuenta con capacidad para soportar esa carga adicional.

3.3.6 Para la conexión de un nuevo servidor se debe solicitar la autorización del supervisor del Centro de Datos para la evaluación y comprobar la disponibilidad del espacio (Unidad de medida=RU) que ocupará dentro del gabinete de telecomunicaciones que corresponda.

3.3.7 El supervisor del Centro de Datos cuenta con el inventario actualizado de los equipos de comunicación (appliances, switches, routers, etc.),

equipos de seguridad digital y gabinetes de telecomunicaciones. El inventario se realiza anualmente.

3.3.8 El Supervisor del Centro de Datos debe revisar el cumplimiento del Plan de Mantenimiento del Centro de Datos.

3.4 DE LA PROTECCIÓN FÍSICA DE LOS CUARTOS DE TELECOMUNICACIONES

3.4.1 El coordinador de infraestructura física de comunicaciones y el coordinador de redes son los responsables de la elaboración del Plan de Mantenimiento preventivo de los gabinetes de comunicaciones y equipos de comunicaciones a nivel nacional. Los proveedores cuentan con un cronograma respectivo.

3.4.2 Los coordinadores de seguridad digital, infraestructura física de comunicaciones y de redes cuentan con el inventario de bienes y el inventario actualizado de los gabinetes de comunicaciones y equipos de comunicación respectivamente. El inventario se debe realizar semestralmente. Así mismo, cuentan con las características de los equipos que administran.

3.4.3 Para la conexión de un nuevo equipo de comunicación, seguridad digital en la regleta eléctrica (PDU) dentro del gabinete de comunicaciones, se debe solicitar la autorización del coordinador de redes para la evaluación y comprobar la disponibilidad del espacio (Unidad de medida=RU) que ocupará dentro del gabinete de telecomunicaciones.

3.5 DEL REGISTRO DE PARÁMETROS DE TEMPERATURA DEL CENTRO DE DATOS

3.5.1 Cada Centro de Datos del RENIEC cuenta con equipos de climatización: Equipos de Aire Acondicionado de operatividad permanente, las 24 horas por 7 días de la semana durante los 365 días del año, a través de los cuales se controla los parámetros de temperatura y humedad relativa del centro de datos.

3.5.2 El “Registro de Control Diario de Temperatura y Humedad Relativa” se realiza los 365 días del año a cargo del operador de Centro de Datos. Se cuenta con tres turnos rotativos, como se visualiza en el cuadro N° 01.

CUADRO N° 01

TURNOS DEL OPERADOR DEL CENTRO DE DATOS	
TURNO	**HORARIO**
TURNO 01 *	23:00 a 07:00 hrs.
TURNO 02	07:00 a 15:00 hrs.
TURNO 03	15:00 a 23:00 hrs.

(*) Turno 01, *no registra en el formato de Control Diario de Temperatura y Humedad Relativa del Centro de Datos, sin embargo, el operador del turno 01 es responsable de monitorear y velar por la operatividad del funcionamiento de los equipos de aire acondicionado ante cualquier eventualidad, que pueda presentarse.*

3.5.3 El operador del centro de datos del site producción y del site contingencia, registra las lecturas de Temperatura y Humedad Relativa de acuerdo con el formato “Registro de Control Diario de Temperatura y Humedad Relativa del Centro de Datos”, ver Anexo N°04.

3.5.4 El rango de horas establecidas para “Registro de Control Diario de Temperatura y Humedad Relativa” se muestra en el siguiente cuadro:

CUADRO N° 02

TURNO DEL OPERADOR	REGISTRO DE CONTROL DIARIO DE TEMPERATURA Y HUMEDAD RELATIVA	
	HORARIO	CONTROL
TURNO 02	08:00hrs a 14:00hrs.	Primer Control
TURNO 03	17:00hrs a 22:00hrs.	Segundo Control

3.5.5 En cuanto a la humedad, se debe encontrar un equilibrio justo, en un rango óptimo donde se eviten las descargas eléctricas y de condensación. El rango adecuado de humedad relativa es entre el 40% y el 55%. Ver Cuadro N° 03.

3.5.6 El formato de “Registro de Control Diario de Temperatura y Humedad Relativa del Centro de Datos” varía según la cantidad de equipos de aire acondicionado que posee cada Centro de Datos. Ver Anexo N° 04

3.5.7 El RENIEC cuenta con Centros de Datos, ubicados en sedes diferentes, donde funcionan los sistemas informáticos, cada uno de cuenta equipos de aire acondicionado

Los Centros de Datos se comunican entre sí mediante enlaces de fibra óptica multiplexada conectada y funcionan como una topología anillo que permite, en caso exista alguna interrupción de servicio en uno de los Centros de Datos, entre en funcionamiento el otro con la finalidad que el servicio continue.

3.5.8 Cada equipo de aire acondicionado cuenta con un panel de control, en la parte frontal, donde se visualiza los valores de temperatura y humedad relativa, estos valores están expresados en números enteros y/o decimales, en grados centígrados (° C) y porcentaje (%), tal como se muestra en la Figura N° 01

- Temperatura °C.
- Humedad %.

Figura N° 01 Valores de Temperatura y Humedad Relativa

3.5.9 Los valores que se visualicen y registren en el formato de "Registro de Control Diario Temperatura y Humedad Relativa del centro de Datos– Anexo 04", deben oscilar dentro los rangos recomendados por los fabricantes de los equipos de aire acondicionado, sin generar alarma y/o reporte alguno según el siguiente cuadro:

CUADRO N° 03

RANGO DE NIVELES DE TEMPERATURA Y HUMEDAD RELATIVA		
RANGO	**TEMPERATURA**	**HUMEDAD**
RANGO RECOMENDADO	18°C a 23°C	40% a 55%
RANGO DE OPERACIÓN	15°C a 25°C	30% a 65%
VARIACIÓN MÁXIMA	10°C/hora	----------
UMBRAL HUMEDAD ALTA	----------	75%
UMBRAL HUMEDAD BAJA	----------	10%

AIRE ACONDICIONADO DE CONFORT (No cuentan con equipos electrónicos)	
RANGO	**TEMPERATURA**
RANGO RECOMENDADO	18°C a 23°C
RANGO DE OPERACIÓN	21.5
VARIACIÓN MÁXIMA	+-5
UMBRAL HUMEDAD ALTA	----------
UMBRAL HUMEDAD BAJA	----------

3.5.10 Si los valores de la temperatura y humedad no oscilan dentro de los rangos configurados por el fabricante, el analista de monitoreo de redes debe comunicar al supervisor del Centro de Datos y este a su

vez al contratista para que se brinde la asistencia técnica según sea el caso.

3.5.11 El operador del centro de datos debe realizar el monitoreo de los paneles de control de aire acondicionado de precisión y confort, en las horas indicadas en el cuadro N°02 del presente documento.

3.6 DE LOS PROBLEMAS EN LOS EQUIPOS DE AIRE ACONDICIONADO

3.6.1 En caso de presentar desperfectos los equipos de aire acondicionado, el operador del centro de datos reporta al supervisor del centro de datos y al personal técnico de la de Unidad de Servicios Generales y Control Patrimonial del RENIEC, a fin de que el proveedor de servicio realice el mantenimiento necesario, según sea el caso.

3.6.2 Finalizado el mantenimiento y solución del incidente, el operador de Centro de Datos informa al supervisor del Centro de Datos y al Jefe de la UIST según corresponda.

3.7 DE LOS REGISTROS DE EVENTOS DE LOG's

3.7.1 El log de los equipos de aire acondicionado de precisión y los gabinetes de telecomunicaciones deben configurarse para el envío por correo electrónico a la cuenta de correo del operador del Centro de Datos. Estos correos deben ser almacenados como mínimos seis (06) meses.

IV. VIGENCIA

La presente entra en vigencia a partir de su aprobación.

V. APROBACIÓN

Se aprueba mediante Resolución de Oficina.

VI. ANEXOS

ANEXO Nº01_FORMATO: RELACIÓN DEL PERSONAL CON ACCESO DIRECTO AL CENTRO DE DATOS

RELACIÓN DEL PERSONAL CON ACCESO DIRECTO AL CENTRO DE DATOS

DATOS DEL FORMATO:
CÓDIGO: PIST-F-RPCC-18/UIST/OTI/RENIEC Versión: 01 Fecha Emisión: 16/08/2024 Fecha Actualización: 16/08/2024

Sede Año:

N°	Nombres	Apellido Paterno	Apellido Materno	Cargo	Órgano	Unidad Orgánica	Observaciones
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

ANEXO Nº02_FORMATO: RELACIÓN DEL PERSONAL CON ACCESO AUTORIZADO AL CENTRO DE DATOS

RELACIÓN DEL PERSONAL CON ACCESO AUTORIZADO AL CENTRO DE DATOS

DATOS DEL FORMATO:
CÓDIGO: PIST-F-RPAC-20/UIST/OTI/RENIEC Versión: 01 Fecha Emisión: 16/08/2024 Fecha Actualización: 16/08/2024

Sede Año:

N°	Nombres	Apellido Paterno	Apellido Materno	Cargo	Organo/ Unidad Orgánica	Autorizado por	Fecha Ingreso	Firma
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								

ANEXO Nº03_FORMATO: BITÁCORA DE CONTROL DE ACCESO DEL CENTRO DE DATOS

BITÁCORA DE CONTROL DE ACCESO DEL CENTRO DE DATOS

DATOS DEL FORMATO:
CÓDIGO: PIST-F-BCACD-21/UIST/OTI/RENIEC Versión: 01 Fecha Emisión: 16/08/2024 Fecha Actualización: 16/08/2024

Sede: **Año:**

Item	Nombres y Apellidos	Órgano/ Empresa	Unidad Orgánica	Motivo	Fecha de Ingreso	Hora de Ingreso	Firma
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							

ANEXO Nº04_FORMATO: REGISTRO DE CONTROL DE TEMPERATURA Y HUMEDAD RELATIVA DEL CENTRO DE DATOS

REGISTRO DE CONTROL DE TEMPERATURA Y HUMEDAD RELATIVA DEL CENTRO DE DATOS

DATOS DEL FORMATO:
CÓDIGO: PIST-F-RCTH-22/UIST/OTI/RENIEC Versión: 01 Fecha Emisión: 16/08/2024 Fecha Actualización: 16/08/2024

Sede: Mes: Año:

Equipo	Control 1				Control 2				Control 3				Observaciones
	Temperatura °C	Humedad Relativa%	Fecha de Registro	Hora de Registro	Temperatura °C	Humedad Relativa%	Fecha de Registro	Hora de Registro	Temperatura °C	Humedad Relativa%	Fecha de Registro	Hora de Registro	
Equipo 1													
Equipo 2													
Equipo 3													
Equipo 4													
Equipo 5													
Equipo 6													
Equipo 1													
Equipo 2													
Equipo 3													
Equipo 4													
Equipo 5													
Equipo 6													
Equipo 1													
Equipo 2													
Equipo 3													
Equipo 4													
Equipo 5													
Equipo 6													
Equipo 1													
Equipo 2													
Equipo 3													
Equipo 4													
Equipo 5													
Equipo 6													