



Pontificia Universidad Católica de Chile

Política y Normativa de Red UC

Código documento	:	Política y Normativa de Red UC
Versión	:	1.0
Preparado por	:	Dirección de Informática UC
Preparado para	:	UC
Autor	:	Marcelo Maraboli
Fecha creación	:	julio 2021
Última modificación	:	agosto 2023
Aprobado por	:	Diego Biscar
Fecha entrada en vigencia	:	3 agosto 2023

CONTENIDOS

1	Definiciones.....	1
2	Introducción	2
2.1	<i>Propósito.....</i>	2
2.2	<i>Aplicabilidad</i>	2
2.3	<i>Red UC</i>	2
3	Política	3
4	Normativa de RED	4
4.1	<i>Administración de la Red UC.....</i>	4
4.2	<i>Administración de Red en servicios Nube (Cloud).....</i>	5
4.3	<i>Instalaciones y Mantenimiento de Infraestructura</i>	5
4.4	<i>Unidades con gestión propia de red</i>	5
4.5	<i>Responsabilidades de la gestión de red</i>	6
4.6	<i>Conexiones autorizadas</i>	7
4.7	<i>Acceso para usuarios</i>	7
4.8	<i>Seguridad: Accesos desde y hacia Internet</i>	8
4.9	<i>Red Inalámbrica</i>	9
4.10	<i>Actualizaciones y obsolescencia de equipamiento de red</i>	10
4.11	<i>Excepciones a la Política</i>	10
5	Sanciones	11
6	anexo: Estándares asociados a la Normativa.....	12

1 DEFINICIONES

- **Comunidad UC:** Todo integrante de los diferentes estamentos de la Universidad: académicos, alumnos, directivos, personal administrativo y profesional.
- **Modelo OSI:** Modelo de red de datos según la ISO (*International Standards Organization*).
- **Punto de Acceso WIFI (Access Point o AP):** Un dispositivo de red cableado que sirve como equipo de conexión común para múltiples dispositivos inalámbricos. En consecuencia, todos los dispositivos inalámbricos comparten el ancho de banda (o “velocidad”) del punto de acceso.
- **Red inalámbrica (WIFI):** Tecnología de red que utiliza frecuencias de radio o enlaces ópticos para conectar, sin cable de red, un dispositivo a la red cableada.
- **Red UC:** Red de datos de la Pontificia Universidad Católica de Chile.
- **SSID (Service Set Identifier):** Nombre o identificador de una señal WIFI.
- **Usuario:** Cualquier persona de la comunidad UC que utilice recursos informáticos, computacionales y de comunicaciones. Se extiende también a personas invitadas por algún integrante de la comunidad UC o que, circunstancialmente, se les autorice utilizar los recursos tecnológicos de la UC.
- **VPN (Virtual Private Network):** Mecanismo que permite la conexión lógica de un dispositivo a una red remota cifrando todo los datos transmitidos y recibidos.
- **Web DI:** Sitio Web de la Dirección de Informática (informatica.uc.cl).

2 INTRODUCCIÓN

2.1 PROPÓSITO

Esta política tiene como propósito **regular el uso de la Red UC** en cuanto a proteger el acceso, la disponibilidad e integridad de la Red UC para que pueda ser utilizada para la misión, objetivos y operación de la Universidad, así como también **definir el uso aceptable, responsabilidades y la normativa** a cumplir para lograr este propósito.

La normativa definida en esta política está diseñada para minimizar el daño causado por la conexión de dispositivos no oficiales, mal administrados o instalados y otras causales que puedan afectar el rendimiento, la integridad, disponibilidad, estabilidad y el normal funcionamiento de la Red UC.

Esta política y normativa está alineada con el **uso aceptable** definido en la **Normativa de uso de Recursos Informáticos UC**, promulgada por Decreto Rectoría N° 32/2012.

2.2 APLICABILIDAD

Esta política aplica a todos los miembros **de la Comunidad UC** y visitantes que poseen algún dispositivo conectado (directamente o remotamente) a la Red UC, incluyendo pero no limitado a, computadores de escritorio, notebooks, servidores, dispositivos móviles, smartphones, cámaras de video, POS, telemetría y equipos especializados, es decir, **cualquier dispositivo que se conecte vía inalámbrica o cableada a la red IP administrada por la Universidad, sean dispositivos personales o dispositivos que la UC sea dueña o administre.**

Asimismo, también aplica a cualquier persona, dispositivo o sistema que acceda a los recursos de la Red UC en forma remota a través de Internet.

2.3 RED UC

La Red UC se define como la infraestructura de red compuesta por hardware (equipos switches, routers, firewall, entre otros), cableado, gabinetes de telecomunicaciones, servicios de red (software con servidores DHCP, DNS, Radius, entre otros) y el direccionamiento IP necesarios para su funcionamiento en dependencias de la Universidad.

La Red UC contempla los puntos de red cableado, los puntos de acceso WIFI, las redes de las unidades, todos los equipos y conectividad de los Datacenter UC y la conexión con el(los) proveedor(es) de comunicaciones (Internet y WAN).

3 POLÍTICA

- **Responsable de la Red UC.** La Dirección de Informática es la unidad responsable de proveer un servicio de red confiable para la Universidad. Esta responsabilidad consiste en administrar la Red UC y establecer una Normativa que incluya la definición del uso y acceso, la asignación y delegación de direcciones IP, la seguridad, el ancho de banda de acceso a Internet, el despliegue WIFI y todas las materias relacionadas necesarias para cumplir el objetivo.
- **Conexión a Internet o proveedores.** La conexión de la Red UC a Internet o a proveedores externos es gestionada exclusivamente por la Dirección de Informática.
- **Nube/Cloud.** La Dirección de Informática es la unidad responsable de la administración de red de los servicios centrales UC que estén desplegados en proveedores externos tipo nube (Cloud) donde se contraten servicios de Infraestructura como servicio (IaaS) o Plataforma como servicio (PaaS).
- **Diseño de Red.** La Dirección de Informática realiza los diseños y especificaciones de las redes de datos y de voz para asegurar el correcto funcionamiento e interoperabilidad de la Red UC. El estándar de la instalación, operación y mantención del cableado de red y de los gabinetes de telecomunicaciones son definidos por la Dirección de Informática. Esto se realiza a través de las Especificaciones Técnicas DI, que están sujetas al estándar técnico vigente de la TIA, IEEE e ISO o basado en las mejores prácticas del fabricante y es considerado parte del estándar UC para todos los edificios y dependencias.
- **Acceso físico.** La Dirección de Informática es el único responsable del **acceso físico** a los gabinetes de telecomunicaciones en todas las dependencias de la Universidad en las que sea responsable de la administración de red. Las unidades deben dar las facilidades de acceso necesarios.
- **WIFI y redes inalámbricas.** Se establece que la Dirección de Informática es el único responsable del despliegue y la gestión de las redes inalámbricas (cualquier norma) en las dependencias de la Universidad.
- **Red Central.** La gestión de red de las unidades centrales o dependientes de una Vicerrectoría o Prorectoría está a cargo de la Dirección de Informática para velar por su correcto funcionamiento.
- **Incidentes.** Toda persona perteneciente a la Comunidad UC debe reportar todas las fallas severas y los incidentes seguridad TI a la Dirección de Informática en un plazo no superior a 48 horas. De esta manera, se podrán tomar medidas de protección para toda la Red UC. Asimismo, deberá reportar dentro de 48 horas hábiles la existencia y ubicación de dispositivos de red no autorizados como switches o router wifi.
- **Usuarios.** Los usuarios de la Red UC deben cumplir con el uso aceptable definido en la Normativa de Uso de los Recursos Informáticos UC.

4 NORMATIVA DE RED

4.1 ADMINISTRACIÓN DE LA RED UC

- **Responsable de la Red UC.** La Dirección de Informática es responsable de proveer un servicio de red confiable para la Universidad. Esta responsabilidad consiste en administrar la Red UC y establecer una Normativa que incluya la definición del uso y acceso, la asignación y delegación de direcciones IP, la seguridad, el ancho de banda de acceso a Internet, el despliegue WIFI y todas las materias relacionadas necesarias para cumplir el objetivo.

La administración se realiza con miras a proveer un acceso que permita el intercambio de información de la manera más eficiente posible para apoyar la misión de la Universidad, manteniendo la integridad y disponibilidad de la Red UC.

- **Ancho de banda.** La Dirección de Informática realiza gestiones de asignación de ancho de banda y prioridad de las aplicaciones críticas de la Universidad como también cambiar el ancho de banda a los segmentos de la red basados en el uso o también para reducir/negar el servicio a usuarios/servidores que violen esta política.
- **Restricción de aplicaciones/sitios.** La Dirección de Informática tiene la facultad de restringir acceso a ciertos sitios, aplicaciones, ancho de banda, contenidos o protocolos de internet según las necesidades de la Universidad e informará a las unidades de las medidas aplicadas.
- **Monitoreo de actividad.** La Dirección de Informática realiza el monitoreo de la Red UC para detectar actividad maliciosa, inapropiada o causantes de niveles inaceptables de interferencia con la operación de la Red UC.
- **Desconexión por uso inapropiado.** En el evento que un dispositivo (cualquiera) esté realizando dichas actividades, el dispositivo podrá ser desconectado de la red hasta que haya sido remediado.
- **Disrupciones.** Las unidades y las personas no podrán ejecutar acciones o servicios que provoque disrupción o interrupción de los servicios centrales de red. Estos servicios incluyen, pero no limitado a, correo electrónico, DNS, DHCP y enrutamiento IP.
- **Conexión de equipos.** No está permitido instalar equipos de red en las redes de la Universidad que son directamente administradas por la Dirección de Informática, debido a la posible interferencia o una degradación en el rendimiento en la red del edificio. En esta categoría están considerados los switches, access point wifi, router o conversores de medio.
- **Equipos no oficiales.** Los equipos considerados irregulares ("Pirata") podrán ser desactivados o removidos por completo por parte de la Dirección de Informática.

4.2 ADMINISTRACIÓN DE RED EN SERVICIOS NUBE (CLOUD)

- **Nube/Cloud.** La Dirección de Informática es la unidad responsable de la administración de red de los servicios centrales UC que estén desplegados en proveedores externos tipo nube (Cloud) donde se contraten servicios de Infraestructura como servicio (IaaS) o Plataforma como servicio (PaaS).
- **Interconexión con Nube.** Los usuarios y unidades no podrán interconectar una red de un proveedor de nube con la Red UC sin la aprobación de la Dirección de Informática.

4.3 INSTALACIONES Y MANTENCIÓN DE INFRAESTRUCTURA

- **Infraestructura de cableado.** El cableado y componentes electrónicos de la red (gabinetes de telecomunicaciones, switches, AP WIFI, convertidores ópticos, etc.) son considerados como parte de la infraestructura básica de red de cualquier edificio o dependencia de la Universidad. La instalación y mantención de la red son parte de los costos básicos de la construcción, mantenimiento y renovaciones de un edificio y, por ende, no deben ser considerados opcionales, sino costos permanentes.
- **Estándar de cableado.** El estándar de la instalación, operación y mantención del cableado de red, de los componentes eléctricos (UPS, exigencias eléctricas, etc.) y de los gabinetes de telecomunicaciones son definidos por la Dirección de Informática (DI) UC, a través de las Especificaciones Técnicas DI (ver Anexo), que están sujetas al estándar técnico vigente de la TIA, IEEE e ISO o basado en las mejores prácticas del fabricante y es considerado parte del estándar UC para todos los edificios y dependencias.
- **Instalaciones y diseño de red.** Las unidades que deseen instalar, renovar o ampliar la conectividad cableada o inalámbrica en sus dependencias, deben solicitar la instalación de cableado de red a la Dirección de Informática para así cumplir los estándares definidos por la Universidad. Asimismo, la Dirección de Informática realiza los diseños y especificaciones de red adecuadas a cada caso para asegurar el correcto funcionamiento e interoperabilidad de la Red UC.
- **Acceso físico.** La Dirección de Informática es el único responsable del acceso físico a los gabinetes de telecomunicaciones en todas las dependencias de la Universidad en las que sea responsable de la administración de red. Las unidades deben dar las facilidades de acceso necesarios.

4.4 UNIDADES CON GESTIÓN PROPIA DE RED

- **Red Central.** La gestión de red de las unidades centrales o dependientes de una Vicerrectoría o Prorectoría está a cargo de la Dirección de Informática para velar por el correcto funcionamiento de las redes de la administración central de la Universidad.
- **Unidades autogestionadas.** Las Facultades, Institutos o Centros que estén autorizadas para realizar su propia gestión de red podrán realizar las tareas de: Asignación de IP a los dispositivos de las redes delegadas por la DI, configuraciones de red de computadores y dispositivos, administración de equipos de red (L2, L3), control físico de los gabinetes de telecomunicaciones, gestión de servicios de DHCP y DNS locales, y la instalación de medidas adicionales de seguridad agregando equipamientos locales como firewall y/o VPN.

- **Cumplimiento de estándar.** Las unidades con gestión propia de red deben cumplir las normas y estándares UC para asegurar una interoperabilidad de la Red UC.
- **Facilidad de acceso a red autogestionada.** Las unidades con gestión propia de red deben permitir el acceso a toda su red interna a la Dirección de Informática con el propósito de monitoreo, cumplimiento de normativas internas y diagnóstico de problemas potenciales que afecten a la Red UC.
- **Calidad de servicio de red autogestionada.** La unidad será entonces responsable de la disponibilidad, integridad y rendimiento de todos los segmentos de su red local.
- **Diseño de Red.** Las Facultades, Institutos o Centros que estén autorizadas para instalar y mantener su propia infraestructura de cableado de red deben solicitar el diseño físico y lógico de red a la Dirección de Informática, donde se definirán aspectos de las capas 1, 2 y 3 del modelo OSI. Las instalaciones deben cumplir el “Estándar de la instalación y mantención del cableado de red UC” (ver Anexo). Los equipos de red a instalar deben cumplir el “Estándar de equipos de Red UC” (ver Anexo) para asegurar la interoperabilidad de las telecomunicaciones (WIFI, telefonía IP, etc.) y aplicaciones UC.
- **Direcciones IP.** Toda asignación o delegación del espacio de direccionamiento IP, tanto privada como pública, en versión 4 como 6, es de responsabilidad y administración de la Dirección de Informática. Las Unidades con gestión propia, sólo podrán hacer uso de direccionamiento IP delegado por la DI. En el caso de hacer uso de direccionamiento IP auto asignado, estas redes no serán visibles desde la Red UC y será responsabilidad de la Unidad la interoperación con la Red UC.

4.5 RESPONSABILIDADES DE LA GESTIÓN DE RED

- **Responsabilidad de gestión de red.** Todo el personal de la Dirección de Informática o de Facultades, Institutos o Centros que tengan a cargo la gestión de un segmento de la Red UC son responsables por el funcionamiento correcto de sus recursos, incluyendo infraestructura, equipos, software y datos que estén en su control o protección.
- **Cumplimiento.** Todas las unidades deben adherir a las políticas, normativas, protocolos y estándares de red fijados por la Dirección de Informática. Cuando se implementen políticas, procedimientos o soluciones técnicas que respondan a necesidades propias de la unidad, se debe asegurar que estén en cumplimiento con todas las disposiciones de la Red UC mencionadas anteriormente.
- **Incidentes.** Asimismo, la persona a cargo de la gestión de un segmento de red debe reportar (vía teléfono al 95504-5555) todas las fallas severas y los incidentes seguridad a la Dirección de Informática en un plazo no superior a 48 horas. De esta manera, se podrán tomar medidas de protección para toda la Red UC. Asimismo, deberá reportar dentro de 48 horas hábiles la existencia y ubicación de dispositivos de red no autorizados como switches, router wifi u otro dispositivo de red.
- **Corresponsabilidad en servicio WIFI y Telefonía IP.** Respecto de los servicios centrales UC como la telefonía IP y red inalámbrica WIFI, el correcto funcionamiento de éstos depende del funcionamiento de la red local de la unidad y, por ende, la unidad es considerada corresponsable.

4.6 CONEXIONES AUTORIZADAS

- **Conexión de Red.** Se permite la conexión de dispositivos autorizados de los usuarios (notebook, computadores, smartphones, tablets, etc.) a la Red UC en los puntos de red y antenas inalámbricas oficiales de la UC.
- **VPN y SSH.** Solo se permiten las conexiones remotas vía VPN y túnel SSH en servidores autorizados por la Dirección de Informática.
- **Modificaciones de red.** Las modificaciones a la red o a los equipos de red administradas por la Dirección de Informática no están permitidas porque generalmente causan efectos no deseados incluyendo la pérdida de conectividad de la red. Por ello, dichas intervenciones deben ser realizadas por la Dirección de Informática o por personal competente inscrito en los registros de la Dirección de Informática.
- **Dispositivos IOT.** La conexión de dispositivos de propósito específico (i.e.: impresoras, TV, equipos de videoconferencia, sensores de temperatura, controles de acceso, cámaras, medidores eléctricos, etc.) deben conectarse a la red cableada. La conexión de este tipo de dispositivos a la red inalámbrica UC no está permitida ya que impacta en el desempeño y calidad de servicio a los usuarios con WIFI.
- **Impresoras.** Toda impresora que se desee conectar a la Red UC debe conectarse a la red cableada siguiendo el “Norma para la configuración de impresoras en la Red UC” (Ver Anexo).
- **Impresión vía WIFI.** Si la unidad requiere que los usuarios WIFI puedan imprimir a la impresora conectada vía cable, pueden solicitar la habilitación de la impresora siguiendo el procedimiento “Norma para la configuración de impresoras en la Red UC” (Ver Anexo).

4.7 ACCESO PARA USUARIOS

- **Uso Aceptable.** El acceso a la Red UC se otorga a las personas para permitir el desarrollo de las funciones propias de la Comunidad UC, siempre y cuando no causen perjuicios al normal funcionamiento de ésta y se enmarquen en los usos aceptables indicados por la Universidad.
- **Conexión de personas externas.** No se permite ofrecer acceso o conectividad a la Red UC o a alguno de sus recursos a personas ajenas a la UC, es decir, sin un fin autorizado previamente por la Dirección de Informática. La red WIFI UCinvitados es una red diseñada para estos fines y, por ende, es el medio oficial para dar conectividad a las personas invitadas.
- **Privacidad.** La Red UC es una red de transmisión de datos que por sí sola no implementa medidas de cifrado o privacidad de los datos que circulan por ella. En consecuencia, el usuario no debe tener expectativas respecto de la privacidad de sus datos en la Red UC. La privacidad se logra a través de los sistemas y sitios web que implementan tales medidas como https, entre otros. Es de responsabilidad del administrador de dichos sistemas y sitios web implementar medidas de privacidad.
- **Seguridad y autenticación.** La conexión de un dispositivo a la Red UC podrá requerir de autenticación del usuario en algunos segmentos de red. Los dispositivos podrán requerir

tener instalado un cliente de seguridad, definido por la Dirección de Informática, para permitir la conexión a la Red UC. El rol de dicho cliente de seguridad será revisar el cumplimiento, por parte del dispositivo, de ciertos requisitos y estándares de seguridad.

- **Usuario.** Cada dispositivo tiene un dueño o es propiedad de la UC. En el último caso, el dispositivo tiene una persona responsable al cual se le ha asignado el uso. En ambos casos, se referirá como “usuario” a la persona que utilice el dispositivo.
- **Dirección IP.** Cada dispositivo que se conecte a la Red UC le será asignado una identificación de red (dirección IP) asociado a su segmento de red. Podrá utilizarse dicho identificador para contactar al usuario del dispositivo en caso de un incidente de seguridad que le afecte, alguna violación a la Normativa de Uso de Recursos Informáticos UC o algún requerimiento legal. Todo registro de asignación de IP (manual o automática) debe guardarse por al menos 2 años.

4.8 SEGURIDAD: ACCESOS DESDE Y HACIA INTERNET

- **Conexiones a equipos internos.** Solo se podrán realizar conexiones desde el exterior (Internet) hacia estaciones de trabajo de usuarios ubicadas dentro de la Red UC mediante el servicio VPN ofrecido por la Dirección de Informática o de las unidades autorizadas. Hacerlo de manera directa implica un riesgo de seguridad muy alto que podría afectar a un gran número de computadores de la red UC.
- **Correo Electrónico.** Los dispositivos conectados a la Red UC pueden enviar correo electrónico usando servidores externos solo a través del protocolo estándar Submission (tcp/587). El acceso a servidores SMTP (25/tcp) y SMTP+SSL (465/tcp) externos solo se permite a los servidores institucionales debidamente autorizados. La UC cuenta con una plataforma de servidores que ofrece el servicio de correo electrónico a toda la Comunidad UC, por lo que el envío de correos @uc.cl debe realizarse a través de este servicio.
- **Servidores.** Si un servidor en la Red UC ofrece algún servicio a público ubicado al exterior de la Universidad y requiere ser visible en todo Internet, la unidad responsable debe solicitar la creación de reglas de acceso para su funcionamiento al Área de Seguridad de la Dirección de Informática. El funcionamiento correcto y seguro del servidor mismos es de responsabilidad de la unidad solicitante.
- **Responsable de Servidor.** Todo servidor debe tener un administrador computacional designado para la gestión y mantención de éste, incluyendo las labores de seguridad, respaldo, control de acceso, actualizaciones y monitoreo.
- **Accesos especiales.** En casos en que se requiera de accesos especiales, éstos deben ser acreditados con la Dirección de Informática y siempre que se cumpla con los fines declarados anteriormente en la presente norma.
- **Solicitud de acceso.** Los accesos deben ser solicitados a través del Coordinador Computacional de la unidad a través de una solicitud generada en la Mesa de Servicios DI (Ver Anexo).

4.9 RED INALÁMBRICA

Las redes inalámbricas presentan varias ventajas de utilización al permitir gran movilidad y comodidad de conexión a las redes. Las redes inalámbricas WIFI están basadas en el estándar IEEE 802.11, que es por naturaleza fácil de implementar, pero muy sensible a la superposición de frecuencias causando degradación de las señales WIFI. Una mala instalación puede provocar fallas de seguridad para todos los usuarios cercanos y de los servicios UC.

Debido a estas características, todo uso inalámbrico debe ser planificado, implementado y gestionado de una manera muy cuidadosa y con una coordinación central para garantizar la funcionalidad básica, máximo ancho de banda y un uso seguro.

- **Responsable de la red inalámbrica.** Se establece que la Dirección de Informática es el único responsable del despliegue y la gestión de las redes inalámbricas (cualquier norma) en las dependencias de la Universidad.
- **Propósito.** Las instalaciones de red inalámbricas son consideradas parte suplementaria de la Red UC y no un reemplazo a la conectividad cableada. El servicio WIFI está destinada al uso de navegación y actividad regular por parte de dispositivos de usuarios de la Comunidad UC.
- **Señales SSID WIFI.** La Universidad pone a disposición varias señales (SSID) WIFI con distintos propósitos, coberturas y mecanismos de seguridad. Las características de las señales y condiciones de uso están publicadas en el sitio web de la Dirección de Informática.
- **Aplicaciones críticas.** Debido a que la red WIFI es un canal compartido entre todos los dispositivos conectados al mismo Access Point, la WIFI es considerada de “mejor esfuerzo” y no debe ser utilizado para actividades que requieran un nivel alto de estabilidad, velocidad o criticidad, ni para servicios productivos.
- **Antenas/equipos no oficiales.** No se permite a las unidades o personas instalar sus propios puntos de acceso inalámbrico en dependencias de la Universidad, debido a la interferencia de la señal resultante y su degradación en el rendimiento a la red inalámbrica UC. En esta categoría están considerados las impresoras, router wifi, datashow, televisores y otros equipos que emiten su propia señal de WIFI.
- **Equipos no oficiales.** Los equipos considerados irregulares (“Pirata”) podrán ser desactivados o removidos por completo por parte de la Dirección de Informática.
- **Protocolos y autorizaciones.** Las unidades deberán solicitar una aprobación a la Dirección de informática antes de utilizar un protocolo inalámbrico distinto a los estándares instalados en la UC.

4.10 ACTUALIZACIONES Y OBSOLESCENCIA DE EQUIPAMIENTO DE RED

- **Licencia y actualizaciones del fabricante.** Todo equipamiento y software debe contar con la licencia, el soporte y actualizaciones del fabricante. Es mandatorio instalar las actualizaciones de seguridad de los equipos y software dentro de los 6 meses de haberse liberado la actualización por parte del fabricante.
- **Obsolescencia.** En caso de que el fabricante declare el “fin de soporte” (*“End of Support”*) de un equipo o software, se considera en estado “obsoleto” posterior a la fecha declarada.
- **Reemplazo de equipos obsoletos.** La unidad responsable de un equipo o software obsoleto debe reemplazar dicha componente lo más pronto posible y a más tardar, en el siguiente año (período presupuestario siguiente).
- **Riesgo de obsolescencia.** Después de pasado el plazo para reemplazar el dispositivo, este podrá quedar inhabilitado en el caso de que represente un riesgo o presente problemas para la estabilidad de la Red UC.

4.11 EXCEPCIONES A LA POLÍTICA

Las excepciones a esta política son revisadas caso a caso y sujetos a aprobación o rechazo por parte de la Dirección de Informática.

5 SANCIONES

El incumplimiento de esta Política será sancionado de acuerdo con los reglamentos UC y legislación chilena vigente.

6 ANEXO: ESTÁNDARES ASOCIADOS A LA NORMATIVA

1) Especificaciones Técnicas DI

- Solicitar a la Dirección de Informática (Subdirección de Redes, Seguridad y Telecomunicaciones)

2) Estándar de la instalación y mantención del cableado de red UC

“Bases Técnicas Generales - Especificaciones Técnicas de Corrientes Débiles”, Versión 11.6

Dirección de Informática

3) “Norma para la configuración de impresoras en la Red UC”, publicado en la Web DI

<https://informatica.uc.cl/red-inalambrica/imprimir-via-wifi>

4) Mesa de Servicios DI.

- Teléfono: 95504-5555
- mesadeservicios.uc.cl

5) Estándar de equipos de Red UC

- Switch de Acceso usuarios L2

Features	Requerimiento
dhcp snooping	Obligatorio
dot1x	Obligatorio
L3 (ruta estatica)	Obligatorio
LACP	Obligatorio
LLDP	Obligatorio
Monitoreo SNMP	Obligatorio
PoE	Obligatorio
port security	Obligatorio
Radius / TACACS+	Obligatorio
Voice Vlan	Obligatorio
ZTP (Zero Touch Provisioning)	Obligatorio

SFP Generico	Obligatorio
Doble Power supply	Deseable
L3 (ospf, is-is basico)	Deseable
NETCONF / RESTCONF / API	Deseable
Netflow / sFlow	Deseable
stack - mclag	Deseable
VRF	Deseable
VXLAN	Deseable

HISTORIA DE REVISIONES

REVISIÓN	VERSIÓN	FECHA	FICHA DE CONTROL DE CAMBIOS
1	1.0	3 agosto 2023	Documento inicial