UNIVERSIDAD DE TARAPACÁ
ARICA – CHILE

APRUEBA NORMATIVA PARA USO DE CLAVES (CONTRASEÑAS) DE INTERNET Y PLAN DE CONTINGENCIA INSTITUCIONAL, CONTINUIDAD DE SERVICIOS ANTE EVENTOS Y CATASTROFES, DE LA UNIVERSIDAD DE TARAPACÁ.

DECRETO EXENTO N° 00.267/2020

Arica, abril 30 de 2020.

Con esta fecha la Rectoría de la Universidad de Tarapacá, ha expedido el siguiente decreto:

VISTO:

Lo dispuesto en D.F.L. N° 150, de 11 de diciembre de 1981, del Ex Ministerio de Educación Pública; Resolución Exenta Universitaria CONTRAL. N°0.01/2002, de enero 14 de 2002, Resolución Exenta Universitaria CONTRAL N°0.01/2018, de abril 23 de 2018; Decreto N°104, del 18 de marzo de 2020, del Ministerio del Interior, Carta de la Dirección de Asuntos Legales N°260/2020, de abril 29 de 2020, Carta de Rectoría N°711/2020, de abril 29 de 2020; los antecedentes adjuntos, y las facultades que me confiere el Decreto N° 193, de 08 de junio de 2018, del Ministerio de Educación.

CONSIDERANDO:

Que, la Universidad de Tarapacá es una corporación de derecho público, autónoma y con patrimonio propio, que goza de una triple autonomía académica, económica, administrativa, en conformidad con lo preceptuado en la Ley N° 21.094, sobre Universidades Estatales, dedicada a la enseñanza y cultivo superior de las artes, las letras y las ciencias, creada por D.F.L N° 150, de 11 de diciembre de 1981, del Ex Ministerio de Educación Pública.

Que, de acuerdo a lo expresado por la Directora de Planificación y Proyectos, en su Carta de fecha 29 de abril de 2020, resulta necesario oficializar los presentes documentos, como requerimiento a lo indicado en el resumen ejecutivo del informe final N°814, de 2019, de la Contraloría Regional de Arica y Parinacota, Unidad de Control Externo.

Que, en este contexto se hace necesaria la aprobación de normativa que regule el uso de claves y el ingreso a la plataforma institucional de Intranet y los accesos a los diferentes ambientes que allí se encuentran y así como la aprobación del Plan de contingencia institucional, continuidad de servicios ante eventos y catástrofes, de la Universidad de Tarapacá

DECRETO EXENTO N°00.267/2020.
30.04.2020

DECRETO:

1.- Apruébase el **NORMATIVA DE USO DE CLAVES (CONTRASEÑAS) DE INTERNET**, contenido en documento adjunto compuesto de seis (06) hojas, rubricadas por la Secretaria de la Universidad de Tarapacá.

2.- Apruébase el **PLAN DE CONTINGENCIA INSTITUCIONAL, CONTINUIDAD DE SERVICIOS ANTE EVENTOS Y CATASTROFES**, contenido en documento adjunto compuesto de veinte (20) hojas, rubricadas por la Secretaria de la Universidad de Tarapacá.

3.- Notifíquese el presente acto administrativo conforme lo prescrito en el artículo 45 y siguiente de la Ley N°19.880, que establece Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado.

4.- Publíquese, en el sistema informático conforme lo señalado en el art. 7 de la Ley N°20.285 de 2008, del Ministerio Secretaria General de la Presidencia, sobre Acceso a la información pública.

Anótese, y remítase a la Contraloría de la Universidad, para su control y registro. Comuníquese una vez tramitado totalmente el acto.

SECRETARIA DE LA UNIVERSIDAD

PAULA LEPE CAICONTE
Secretaria de la Universidad

UNIVERSIDAD DE TARAPACA RECTOR ARICA

EMILIO RODRIGUEZ PONCE
Rector

UNIVERSIDAD DE TARAPACA CONTRALORIA ARICA

ERP.PLC.ycl.

NORMATIVA PARA USO DE CLAVES (CONTRASEÑA) DE INTERNET Y PLAN DE CONTINGENCIA INSTITUCIONAL, CONTINUIDAD DE SERVICIOS ANTE EVENTOS Y CATASTROFES, DE LA UNIVERSIDAD DE TARAPACÁ.

Uso de Contraseña – Intranet Universidad de Tarapacá

1. **Creación de nuevos usuarios**
   - Para poder ingresar a la intranet, el usuario debe estar enrollado en la Intranet de la Universidad, una vez que un nuevo usuario sea creado, recibirá vía correo su clave inicial y al acceder por primera vez a la intranet se le ofrecerá al usuario la aceptación de condiciones y términos de uso de la Intranet, posteriormente el usuario deberá cambiar en forma obligatoria su clave inicial.
   - Normas para la creación de una nueva claves de la Intranet
     - Debe contener al menos un carácter en minúscula
     - Debe contener al menos un carácter en mayúscula
     - Debe contener al menos un valor numérico
     - Debe contener al menos un carácter especial
     - Debe contener al menos 8 caracteres
     - No debe contener caracteres repetidos consecutivos
   - La imagen 1, muestra como se le entrega al usuario información visual referente al formato de la clave ingresada.

2. **Acceso a la intranet**
   - Para ingresar a la intranet el usuario debe presionar el botón Intranet, de la página oficial de la Universidad
   - El usuario debe ingresar su clave la que debe coincidir con la clave asignada al momento del enrolamiento (nuevo usuario), o a la clave modificada por el usuario.
   - El usuario tendrá 3 intentos para ingresar la clave, si el tercer intento es fallido, se reportará al Administrador del sistema y se bloqueara la cuenta.
   - Cada 6 meses el sistema debe cambio de clave en forma obligatoria a los usuarios.
   - Adicionalmente, el usuario podrá utilizar su cuenta de Google registrada para acceder a la intranet, para ello se utilizara las normas de clave y acceso definidas por Google (ver anexo 1).

3. **Cambio de Contraseña**
   - Una vez dentro de la Intranet, el usuario podrá realizar su cambio de contraseña cada vez que lo estime conveniente y se realizara siguiendo las normas establecidas en el apartado de creación de nuevos usuarios.
   - Aquí se incorporan nuevas consideraciones:
     - No puede utilizarse una contraseña ya utilizada con anterioridad
     - No podrá reutilizar la actual contraseña.

4. **Perdida de contraseña**
   - Si un usuario olvida su clave, podrá solicitar la generación de una nueva en la opción, recuperar contraseña de correspondiente al módulo de acceso a la intranet, luego, se le enviará un correo con un link a uno de los correos que el usuario haya definido como propio en la misma intranet,
   - Vía este link, el usuario accederá al módulo donde deberá crear su nueva contraseña según las normas definidas anteriormente.

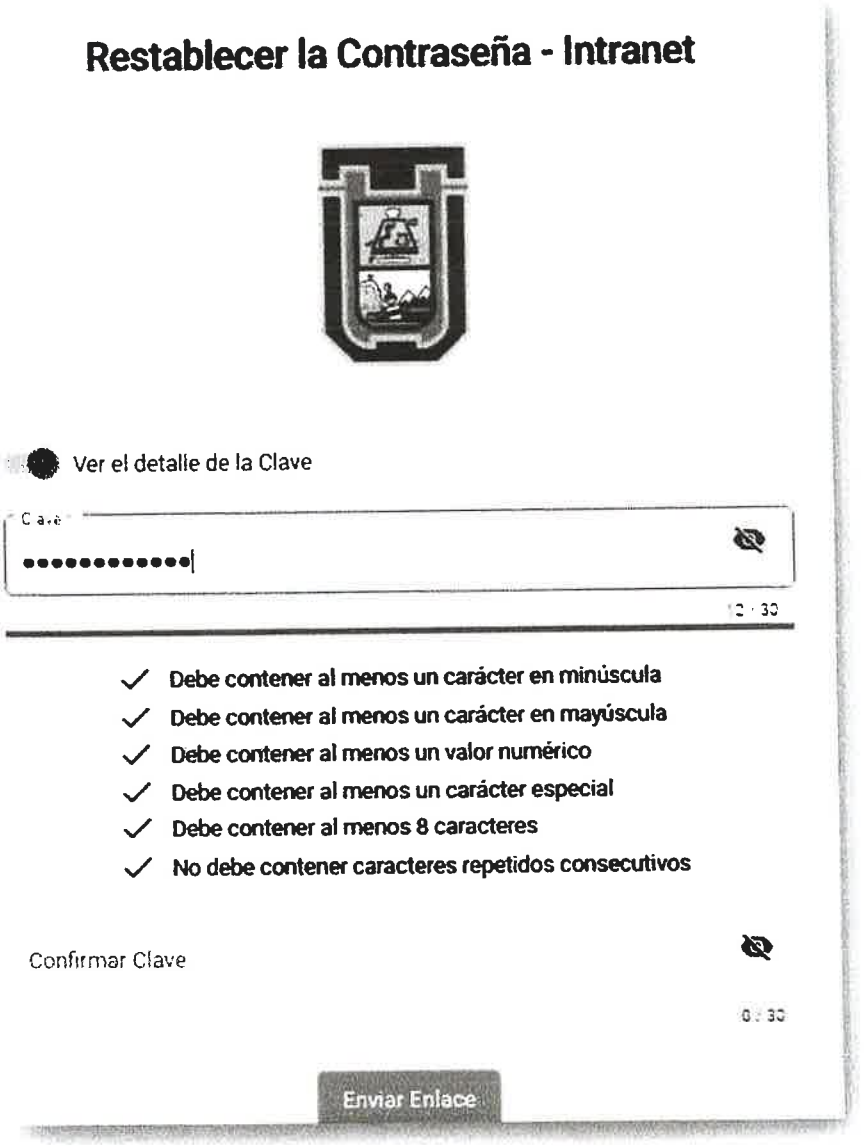

Imagen 1: Restablecer contraseña

Anexo 1

Uso alternativo de acceso a la intranet mediante el uso de la cuenta GOOGLE, de los usuarios registrada en la intranet institucional.

Utilizar cuentas de Google para iniciar sesión en otros sitios web o aplicaciones, referencia: (https://support.google.com/accounts/answer/112802?co=GENIE.Platform%3DDesktop&hl=es).

SECRETARIA DE LA UNIVERSIDAD

Se puede usar la cuenta de Google para iniciar sesión en sitios web y aplicaciones de terceros. De esta manera, no tendrás que memorizar los nombres de usuario ni las contraseñas de cada una de tus cuentas.

Nota: Google no mantiene ninguna relación con los sitios web externos que solicitan autenticación, simplemente les ofrece una tecnología de inicio de sesión.

Normativa de GOOGLE, respecto a sus claves de acceso, referencia (https://support.google.com/accounts/answer/32040?hl=es-419).

Contraseña segura

Una contraseña segura te permite:

- Proteger tu información personal
- Proteger tus correos electrónicos, archivos y demás contenido
- Evitar que otra persona acceda a tu cuenta

Requisitos para la contraseña

Crea tu contraseña con 8 caracteres o más. Puede ser cualquier combinación de letras, números y símbolos (solo caracteres ASCII estándar). No se admiten acentos ni caracteres acentuados.

No puedes usar una contraseña que:

- Sea poco segura, p. ej., "contrasena123"
- Hayas usado antes en tu cuenta
- Empiece o termine con un espacio en blanco

Sugerencias para crear una contraseña segura

Una contraseña segura debe ser fácil de recordar para ti, pero prácticamente imposible de adivinar para otra persona. Obtén información sobre qué características debe tener y sigue estas sugerencias para crear una propia.

- **La contraseña que sea única**
  Usa una contraseña diferente para cada una de las cuentas importantes, por ejemplo, la cuenta de correo electrónico y la banca en línea.
  Es riesgoso reutilizar contraseñas para cuentas importantes. Si alguien averigua tu contraseña de una de esas cuentas, podría conocer tu dirección o acceder a tu correo electrónico e, incluso, tu dinero.

- **Una contraseña más extensa y que puedas recordar mejor**
  Las contraseñas largas son más seguras: verifica que la tuya tenga ocho caracteres como mínimo. Estas sugerencias pueden ayudarte a crear contraseñas más largas y que sean más fáciles de recordar. Intenta usar:
  - La letra de una canción o un poema

- Una cita significativa de una película o un discurso
- El pasaje de un libro
- Una secuencia de palabras que te resulten significativas
- Una abreviatura (crea una contraseña con la primera letra de cada palabra de una oración)
- No elijas contraseñas que sean fáciles de adivinar por:
  - Personas que conoces
  - Personas que busquen información de fácil acceso (como tu perfil en redes sociales)

- **No incluyas información personal ni palabras comunes**
  - No uses información personal

    No crees contraseñas que incluyan información que otras personas puedan saber o descubrir fácilmente. Ejemplos:

    - Tu apodo o iniciales
    - El nombre de tu hijo o mascota
    - Años o fechas de nacimiento importantes
    - El nombre de tu calle
    - Los números de tu dirección
  - No uses palabras o patrones comunes

    Evita palabras, frases y patrones simples que sean fáciles de adivinar. Ejemplos:

    - Palabras y frases evidentes, como "contrasena" o "acceder"
    - Secuencias, como "abcd" o "1234"
    - Patrones del teclado, como "qwerty" o "qazwsx"
    - Ejemplos de este artículo, como "F3l1zN@v1d@D" o "EtPsCt2CdC@!""

Proceso de Verificación de Permisos de Accesos de Usuario

La universidad de Tarapacá, cuenta con una Intranet en la que se implementan diferentes modalidades de acceso a sus opciones.

En primera Instancia se encuentran las opciones principales de la Intranet, las cuales son accedidas una vez que el usuario se autentifica en ella, y las opciones a las que puede acceder el usuario está directamente relacionada con los perfiles a los cuales se haya autorizado el usuario, esta asociación en la mayoría de las veces se realiza de forma automática de acuerdo a sus funciones dentro de la universidad, estos perfiles son:

- **Alumno**: perfil que se obtiene automáticamente una vez que la persona es matriculada a la universidad.
- **Académico**: perfil asignado en forma automática a los nuevos profesores una vez que se le asigna una carga académica.
- **Funcionario**: perfil que se le asigna a las personas que son contratadas en la universidad.
- **Honorario**: perfil que se asigna automáticamente cuando se le realiza el primer convenio a la persona dentro de la universidad.

Para la verificación de accesos existe una opción dentro de los sistemas administrativos, que permite verificar los accesos de los usuarios enrolados, verificar los periodos donde se le ha permitido acceder y los diferentes perfiles dentro de esta, ver imagen 2

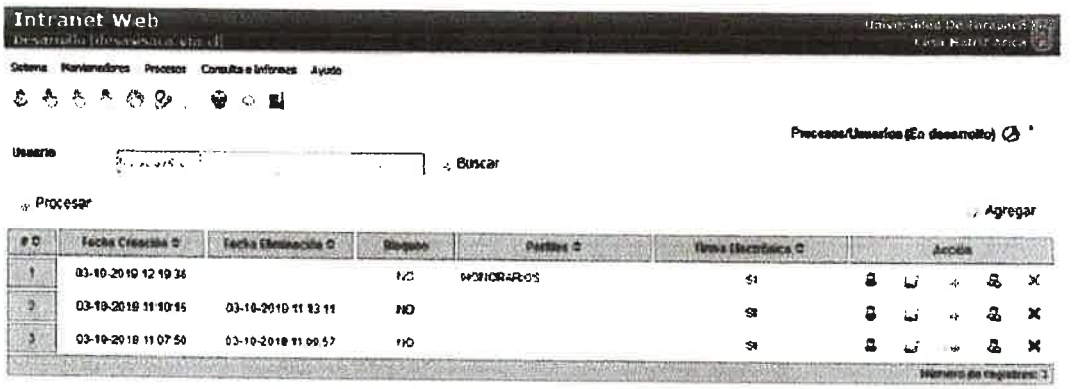

Imagen 2: verificación de permisos Usuarios Intranet

La segunda modalidad es a través de los sistemas administrativos a los cuales sólo tienen acceso los funcionario y que dependen de las unidades académica administrativas de la universidad.

En este caso cada unidad cuenta con un responsable o dueño del sistema el cual puede otorgar o revocarlos accesos a los sistemas que tiene a cargo, además tiene la facultas de dar acceso hasta el nivel de opción dentro del sistema, ver imagen 3 y 4.

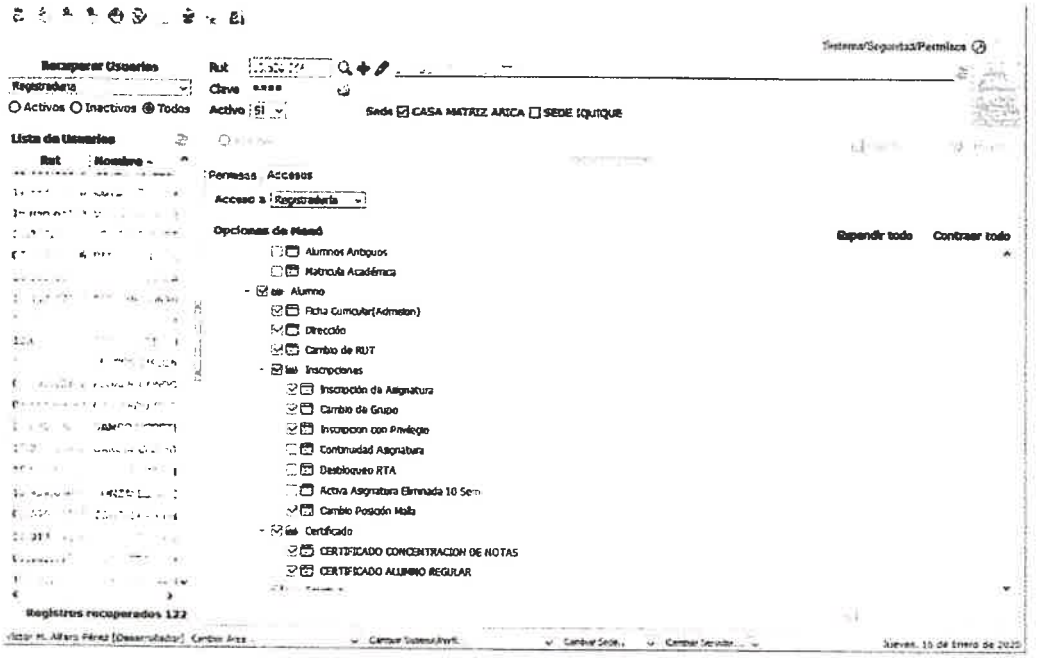

Imagen 3: verificación de permisos de acceso Sistemas Administrativos

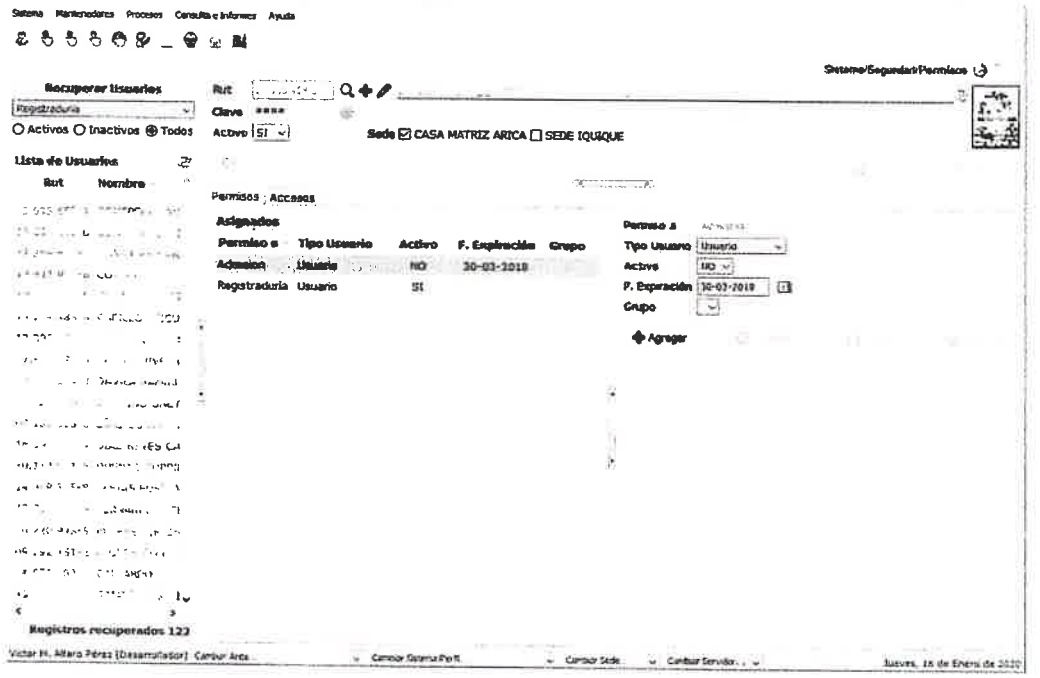

Imagen 4: Visualización de permisos a sistemas administrativos

UNIVERSIDAD DE TARAPACÁ

Plan de Contingencia Institucional

Continuidad de Servicios ante eventos y catástrofes

Unidad de Desarrollo Tecnológico
18 de Septiembre # 2222 Arica - Chile
Teléfono: 56-582205175
E-mail: udt@uta.cl

SECRETARIA DE LA UNIVERSIDAD

1. OBJETIVO

El presente Documento de Procedimiento, es establecer la forma de manejar los eventos relacionados con la Continuidad Operativa de la Conectividad de las Redes (Servicios de Transporte de Datos) y de los Servidores Centrales (Servicios Internet, Servicios Intranet, Bases de Datos, Correo Institucional, entre otros Servicios) alojados en el Datacenter o bajo la administración de la Unidad de la institución.

2. ALCANCE

El presente Documento de Procedimiento será de aplicación de los funcionarios del Área Ingeniería de Sistemas, quienes tendrán la función y responsabilidad de registrar los errores, fallas o eventos relevantes que se detecten en el funcionamiento de la Continuidad Operativa de la Conectividad de las Redes a nivel Local, Intercampus, Redes Externas, acceso a Internet y Servidores Centrales.

Se define las responsabilidades de Funcionarios de Área Soporte TICs ULOO, en cuanto a la notificación de Eventos no Programados y Situaciones de Contingencia en Dependencias donde Área Ingeniería de Sistemas no tiene personal disponible.

3. RESPONSABILIDADES

"El Encargado de la Unidad de Desarrollo Tecnológico", es el responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad y alta disponibilidad de la Continuidad Operativa de la Conectividad de las Redes Internas y Externas. Del mismo modo, debe realizar las gestiones para cumplimiento de la Continuidad Operativa de los Servidores Centrales de toda la organización, todo esto en coordinación con la Dirección de Planificación, Rectoría y Junta directiva. También es responsable de evaluar, adquirir e implantar productos de seguridad informática, equipamiento de conectividad y servidores, además de realizar las actividades necesarias para garantizar un ambiente informático seguro, de alta prestación y disponibilidad.

"El Ingeniero de Redes del Área Ingeniería de Sistemas", es el responsable de velar la Continuidad Operativa de la Conectividad de Redes Internas, Externas y la de los Servidores Centrales (Monitoreo del Performance de los distintos Servicios). En caso de un Evento no Programado, Fallas o Incidentes, se deben ejecutar las medidas de solución para los problemas pertinentes.

"El Ingeniero de Sistemas del Área Ingeniería de Sistemas", es el responsable de establecer los controles de monitoreo y supervisión del uso de los recursos Informáticos, además de llevar a cabo las tareas de seguridad relativas a los sistemas que administra.

"El personal de Área Soporte TICs ULOO", son los responsables de notificar los Eventos relacionados con la disponibilidad en la Continuidad Operativa de la Conectividad de Redes, falla de un servicio de Red, Servidores o Aplicación Cliente-Servidor en producción, Corte en el Suministro Eléctrico que afecte la disponibilidad del Servicio.

"Los Funcionarios de la Comunidad Universitaria", son responsables de llamar a Operadores de Área Soporte TICs ULOO o "Help Desk" en caso de estar implementado, ante eventualidades de falla o interrupción de la Continuidad Operativa en el Servicio de Red y/o Servidores. No están facultados para aplicar medidas correctivas sin el apoyo de Funcionarios de Área Soporte TICs ULOO y Área Ingeniería de Sistemas.

4. CONTEXTO

La Unidad de Desarrollo Tecnológico dentro de su Organigrama Institucional, cuenta con el Área de Ingeniería de Sistemas. Esta unidad esta encargada de velar por el correcto funcionamiento y Continuidad Operativa de las redes locales de Campus Velásquez, Campus Saucache, Campus Azapa, Sitios Remotos de la Ciudad de Arica, Sitios Remotos de la Ciudad de Iquique y Sitios Remotos de la Región Metropolitana. Además, debe realizar el monitoreo de los Enlaces Inter-Redes dentro de la Ciudad de Arica (Red Intercampus Saucache – Velásquez, Red Intercampus Saucache – Facultad de Agronomía Azapa, Red Intercampus Saucache – Museo San Miguel de Azapa, Red Intercampus Saucache – Sitio Remoto Instituto de Alta Investigación, Red Sitio Intercampus Saucache – Sitio Remoto Edificio Yungay, Red Intercampus Saucache – Sitio Remoto Museo Colón, Red Intercampus Saucache – Sitio Remoto Departamento Independencia, Red Intercampus Saucache – Sitio Remoto Parcela Lluta KM 19), en la Ciudad de Iquique (Red Intercampus Saucache – Sitio Remoto Sede Esmeralda, Red Intercampus Saucache – Sitio Remoto Pedro Aguirre Cerda, Red Intercampus Saucache – Sitio Remoto Baquedano, Red Intercampus Saucache – Sitio Remoto Covadonga, Red Intercampus Saucache – Sitio Remoto Ramírez, Red Intercampus Saucache – Sitio Remoto Tomás Bonilla) y en la Región Metropolitana (Red Intercampus Saucache – Sitio Remoto José Victorino Lastarria, Red Intercampus Saucache – Sitio Remoto Quebec Providencia).

Hay que señalar, que el Transporte de Datos hacia los Campus y Sitios Remotos de la

Ciudad de Arica, Ciudad de Iquique y Región Metropolitana, los realiza la Empresa Movistar. Cuando hay una situación de Contingencia (Problema Enlace de Fibra Oscura), se realiza levantamiento de Ticket a la Mesa Tecnológica de Movistar, para tener antecedentes de la reposición del Servicio.

Dentro del esquema existente (Red UTANET), hay diferentes tecnologías de redes implementadas, tales son las a nivel local Alámbricas (Cableado Estructurado), Inalámbricas (Servicios WiFi, Enlaces Point to Point), Tecnología Intercampus y el acceso a Internet. Área Ingeniería de Sistemas se encarga de controlar los servicios de Red disponibles, con tal de aprovechar al máximo los recursos de Bandwidth contratados.

De acuerdo a los antecedentes presentados, se debe tener presente la premisa de mantener la disponibilidad de las redes y los servicios que de ellas se utilicen. Mediante un plan de contingencia se logran tomar las acciones específicas cuando surjan problemas o una condición que no esté considerado en el proceso de planeación y ejecución normal. Dentro de las acciones a tomar son:

De prevención: Conjunto de acciones a realizar para prevenir cualquier contingencia que afecte la Continuidad Operativa, ya sea en forma parcial o total. Esta vela por reducir el impacto, permitiendo restablecer a la brevedad posible los diferentes aspectos reducidos.

Detección: Deben contener el daño en el momento, así como limitarlo tanto como sea posible contemplando todos los desastres naturales y eventos no considerados.

Recuperación: Abarcan el mantenimiento de partes críticas entre la pérdida de los recursos, así como de su recuperación o restauración.

5. ESCENARIOS DE CONTINGENCIAS

Se consideraran los escenarios de desastre a nivel de redes, entre otros los siguientes.

a) La no disponibilidad de acceso desde Internet hacia/desde Red UTANET los cuales se resumen por las siguientes causas:

- Contingencias frente ataques externos por denegación de servicios (DoS).
- Contingencias frente a cortes de Fibra o Servicios de red en algún tramo entre UTA y el proveedor de Servicios Internet (Consorcio REUNA).

- Fallas en Enlaces Internacionales e intermitencias en Proveedores de Contenido.
- Fallas por baja en la Performance de la red en el acceso hacia/desde Internet.

b) Fallas en los accesos a los Servidores y sus sistemas o aplicaciones del Datacenter de la Universidad. Entre otros se puede indicar:

- La no disponibilidad de acceso a las Redes locales, y/o Servidores locales de Intranet, Correo Institucional, DNS, Base de Datos, entre otros Servicios.
- La no disponibilidad en las redes Intercampus, o bajas en su prestación, o en su Bandwidth (Ancho de Banda).

a) Fallas o pérdidas de enlace a nivel enlace principal (Backbone) dentro de cada uno de los Campus o Sitios Remotos.

6. PLANES DE CONTINGENCIAS

Se cuentan con los planes de contingencias para los siguientes eventos:

- Plan de Contingencia frente ataques externos por denegación de servicios (DoS).
- Plan de Contingencia frente fallas de equipos Intermedio de comunicaciones en el Datacenter.
- Plan de Contingencia frente caídas de Enlaces o bajas en las tasas de Transferencias a nivel Local, Interred (Intercampus, Sitios Remotos) e Internet.
- Plan de Contingencia frente a falla en el Firewall Institucional.
- Plan de Contingencia para corte prolongado de energía en el Datacenter y sus puntos de enlace en el Backbone central.
- Plan de Contingencia frente a actos vandálicos, terroristas, no acceso forzoso al Datacenter.
- Plan de Contingencia para usuarios en caso de paro o toma prolongada de la Universidad.
- Planes de Contingencia para incendios dentro del Datacenter.
- Planes de Contingencia para inundaciones en el Datacenter.
- Plan de Contingencia frente a sismos de mediana o gran envergadura.

Plan de Contingencia frente ataques externos por denegación de servicios (DoS)

➢ **Prevención:**

- Mantener actualizado el sistema operativo, Firmware (IOS) de los equipos conectados directamente a la Red Internet.
- Mantener un Sistema de información de Eventos por consola de las señales registradas en un servidor de Syslog.
- Aplicar reglas de control (Políticas de Seguridad) para las situaciones de ataques más comunes y dejarlas en modo DENY.
- Mantener y Verificar el estado de respaldo eléctrico (UPS) para esas Infraestructuras, verificando tiempo de respaldo.
- Realizar un plan de mantenimiento para los Dispositivos de Telecomunicación y Servidores que presten esos Servicios.
- Mantener comunicación con Mesa Tecnológica de Proveedor de Servicios de Internet (REUNA).

➢ **Detección:**

- Verificar Status en Consola de Firewall Institucional y Sistemas de Monitoreos de Área Ingeniería de Sistemas (Correo Electrónico, Gráficas MRTG).
- Verificar incrementos excesivos de tráficos de datos hacia o desde Internet por medio Sistemas de Monitoreos de Área Ingeniería de Sistemas. Mantener comunicación con Mesa Tecnológica de Proveedor de Servicios de Internet (REUNA).

➢ **Recuperación:**

- Informar a Mesa Tecnológica de Proveedor de Servicios de Internet (REUNA) el ataque DoS para tomar medidas que contrarresten el ataque a la disponibilidad, bloqueando la fuente del ataque, o el servicio de red. Seguir las instrucciones de Especialistas de REUNA.

Plan de Contingencia frente fallas de equipos Intermedio de Telecomunicaciones, Core, Distribución y Acceso

➢ **Prevención:**

SECRETARIA DE LA UNIVERSIDAD

- Tener operativo en configuración de alta disponibilidad (HA) Firewall Institucional, Equipos Core y Distribución.
- Mantener actualizado el sistema operativo, Firmware (IOS) de los equipos conectados directamente a la Red Internet.
- Mantener en Monitoreo Dispositivos Switch y Router principales que dan acceso a Servicio de Internet e Intranet.

    - Datacenter Campus Saucache (Rack 1, Rack 2, Rack 4, Rack 5, Rack 6 y Rack 7).
    - Cuarto de Telecomunicaciones Core Secundario (Edificio Anexo Biblioteca Campus Saucache, 1er Piso).
    - Cuarto de Telecomunicaciones Registraduría (Edificio Integral Campus Saucache, 1er Piso).
    - Cuarto de Telecomunicaciones Dirección de Asuntos Estudiantiles (Edificio Integral Campus Saucache, 2do Piso).
    - Cuarto de Telecomunicaciones Dirección de Administración y Finanzas (Edificio Integral Campus Saucache, 2do Piso).
    - Cuarto de Telecomunicaciones Dirección de Gestión de Personas y Bienestar Laboral (Edificio Integral Campus Saucache, 3er Piso).
    - Cuarto de Telecomunicaciones Escuela de Diseño e Innovación Tecnológica (Edificio EUDEV Campus Saucache, 1er Piso).
    - Cuarto de Telecomunicaciones Facultad de Ciencias Sociales (Edificio FACSOJUR Campus Saucache, 3er Piso.
    - Cuarto de Telecomunicaciones Facultad de Educación y Humanidades (Edificio Principal Campus Saucache, 2do Piso).
    - Cuarto de Telecomunicaciones Facultad de Ciencias (Edificio DECFACI Campus Saucache, 1er Piso).
    - Cuarto de Telecomunicaciones Facultad de Ciencias de la Salud (Edificio FACSAL Campus Saucache, 1er Piso).
    - Cuarto de Telecomunicaciones Escuela de Medicina (Edificio Escuela de Medicina Campus Saucache, 1er Piso).
    - Cuarto de Telecomunicaciones Facultad de Ingeniería Informática (Edificio IECI Campus Saucache, 1er Piso).

- Cuarto de Telecomunicaciones Facultad de Ingeniería Industrial (Edificio ICI Campus Saucache, 1er Piso).
- Cuarto de Telecomunicaciones Facultad de Ingeniería Mecánica (Edificio IEM Campus Saucache, 2do Piso).
- Cuarto de Telecomunicaciones Facultad de Ingeniería Eléctrica-Electrónica (Edificio ICELO Campus Saucache, 1er Piso).
- Cuarto de Telecomunicaciones Facultad de Administración y Economía (Edificio FAE Campus Saucache, 2do Piso.
- Cuarto de Telecomunicaciones CORE (Edificio GORE Campus Velásquez, 2do Piso.
- Cuarto de Telecomunicaciones Departamento de Biología (Edificio Principal Campus Velásquez, 2do Piso).
- Cuarto de Telecomunicaciones Departamento de Química (Edificio Principal Campus Velásquez, 1er Piso).
- Cuarto de Telecomunicaciones Rectoría (Edificio Rectoría Campus Velásquez, 1er Piso).
- Cuarto de Telecomunicaciones Vicerrectoría de Administración y Finanzas (Edificio Rectoría Campus Velásquez, 1er Piso).
- Cuarto de Telecomunicaciones Dirección de Planificación y Proyectos (Edificio DIPLAN Campus Velásquez, 1er Piso).
- Cuarto de Telecomunicaciones Facultad de Ciencias Agronómicas (Edificio Decanatura Agronomía Campus Azapa, 1er Piso).

- Aplicar reglas de control (Políticas de Seguridad) para las situaciones de ataques más comunes y dejarlas en modo DENY.
- Mantener y Verificar el estado de respaldo eléctrico (UPS) para esas Infraestructuras, verificando tiempo de respaldo.
- Realizar un plan de mantenimiento para los Dispositivos de Telecomunicación y Servidores que presten esos Servicios.
- Tener Disponibilidad de Dispositivos de Telecomunicación Secundarios pre-configurados o con las configuraciones respaldadas (Servidor TFTP) para dar continuidad de operación.

SECRETARIA DE LA UNIVERSIDAD

➢ **Detección:**

- Verificar Status en Dispositivos de Telecomunicación Intermedio que se han especificado de acuerdo a su nivel de criticidad.
- Verificar incrementos excesivos de tráficos de datos hacia o desde Internet, por medio Sistemas de Monitoreos de Área Ingeniería de Sistemas.
- Verificar Status de Led y Configuración Lógica de Interfaces de Dispositivos de Telecomunicación Intermedio que se han especificado de acuerdo a su nivel de criticidad.

➢ **Recuperación:**

- Reiniciar Dispositivos, siempre y cuando no exista Acceso mediante Consola CLI.
- Verificar Eventos de Sucesos en Servidor SYSLOG.
- Realizar una Revisión Técnica, desde el punto de vista de Lógica o Electrónica del Dispositivo en falla.
- Habilitar Dispositivos de Telecomunicación Backup en caso de que Dispositivos diagnosticados presente fallas que no permitan la continuidad operativa.

Plan de Contingencia frente caídas de Enlaces o bajas en las tasas de Transferencias a nivel Local, Interred (Intercampus, Sitios Remotos) e Internet

➢ **Prevención:**

- Red Local, mantener los equipos clientes actualizados, con su Firewall local activo, antivirus en operación y actualizados, libre de gusanos o programas que provoquen una saturación de la red a nivel local, Interred o Internet.
- Mantener actualizado el sistema operativo, Firmware (IOS) de los equipos conectados directamente a la Red Internet.
- Registrar el uso de Bandwidth a través de Servidores MRTG (Servidor Área Ingeniería de Sistemas).
- Activar Sistema de Transporte de Datos Redundantes en caso de existir Cableado Backup de Enlaces.
- Establecer un Enlace Alternativo Redundante hacia Internet (Verificar Factibilidades Técnicas con Proveedor de Servicios de Internet REUNA y Proveedor que realiza Transporte de Datos).

➢ **Detección:**

- Verificar incrementos excesivos de tráficos de datos hacia o desde Internet, por medio Sistemas de Monitoreos de Área Ingeniería de Sistemas.
- Mantener comunicación con Mesa Tecnológica de Proveedor de Servicios de Internet (REUNA), en caso que el problema sea externo a la Red UTANET.

➢ **Recuperación:**

- Informar a Mesa Tecnológica de Proveedor de Servicios de Internet (REUNA) el evento detectado. Seguir las instrucciones de Especialistas de REUNA.
- Informar a la Dirección del restablecimiento de los Servicios para que se pueda emitir un comunicado a la Comunidad Universitaria en caso de que el problema haya afectado en forma prolongada la Continuidad Operativa de Servicios.

Plan de contingencia frente a falla en el Firewall Institucional

➢ **Prevención:**

- Verificar Operación de la Configuración HA (alta disponibilidad), desactivando el Master y ver Operación del sistema con la unidad Slave.
- Realizar un plan de mantenimiento para los Dispositivos de Telecomunicación y Servidores que presten esos Servicios.
- Tener configuraciones respaldadas (Servidor TFTP) para dar continuidad de operación.
- Mantener un Sistema de información de Eventos por consola de las señales registradas en un servidor de Syslog.
- Mantener un Dispositivo Firewall en caso que falle Firewall Institucional (Master).

➢ **Detección:**

- Detección de falla en Dispositivo, cuando no existe acceso a Internet, para los usuarios (Medio Alámbrico, Inalámbrico).

- Detección de falla en Dispositivo si no es posible ingresar al Firewall mediante las Credenciales de Acceso.
- Detección de falla en Dispositivo si no es posible ingresar al Firewall mediante Servicio Web.

➢ **Recuperación:**

- Como primera opción reiniciar Firewall, en caso de no haber resultados positivos, realizar procedimientos:
  - Reinicio de Firewall mediante Consola Cli.
  - Reinicio de Firewall mediante Interruptor de Apagado On/Off, estando atento a las notificaciones del Inicio del Dispositivo.
  - Revisar eventos Log de Firewall Institucional (Registro de Sucesos).
  - Habilitar Dispositivos Firewall Backup en caso de que Dispositivo diagnosticado presente fallas que no permitan la continuidad operativa.

Plan de Contingencia para corte prolongado de energía en el Datacenter y sus puntos de enlace en el Backbone central

➢ **Prevención:**

- Realizar pruebas de continuidad de servicio de los servidores centrales, mediante UPS y Generador Electrógeno (Datacenter).
- Realizar pruebas de continuidad de servicio de los Dispositivos de Telecomunicación, mediante UPS (Puntos de Enlace Nodos Centrales).
- Verificar que las UPS cuenten con las Mantenciones preventivas para respaldo de suficiencia energética.
- Verificar que Generador Electrógeno cuente con las Mantenciones preventivas y que disponga de Carga de Combustible para su funcionamiento y Estanque de Reserva, para el suministro de energía en caso de un evento eléctrico no programado.
- Mantención de los Tableros de Transferencia Automática.

➢ **Detección:**

- Verificar variación del suministro eléctrico de voltaje entrante.
- Monitoreo de UPS a través de Servidores MRTG (Servidor Área Ingeniería de Sistemas).

➢ **Recuperación:**

- Establecer contacto con ITO Eléctrico de la Institución para realizar las medidas de diagnóstico y recuperación en caso de que el evento eléctrico no programado haya sido en forma local.
- Establecer contacto con Proveedor de Servicio Eléctrico para recabar información acerca del evento eléctrico no programado (Corte Eléctrico en Estaciones Intermedias o Black out) y la reposición del servicio eléctrico.
- Informar a la Dirección del restablecimiento de los Servicios para que se pueda emitir un comunicado a la Comunidad Universitaria en caso de que el problema haya afectado en forma prolongada la Continuidad Operativa de Servicios.
- Habilitar Servicios en Datacenter y en Nodos Intermedios en caso de que se vieran afectados por el evento eléctrico no programado.
  - Activar Sistemas de servidores DNS, DHCP y Correo Institucional.
  - Sistema de Servidores Web, Intranet y Bases de Datos, verificar estado de los discos.
  - Habilitar Dispositivos CORE.
  - Habilitar Dispositivo Firewall.
  - Habilitar Dispositivos de Telecomunicación de Acceso e Intermedios.

Plan de Contingencia frente a actos vandálicos, terroristas y de no acceso físico al Datacenter por largos períodos de tiempo.

➢ **Prevención:**

- Mantener cerrado con llave todas las noches las rejas de los pasillos exteriores a las Dependencias de la Unidad de Desarrollo Tecnológico; responsabilidad de verificar y dejar activado estas cerraduras corre por parte de Vigilantes de la Universidad.
- Mantener acceso para la red de los servidores desde Internet, mediante el uso del servicio VPN.

- Realizar pruebas de continuidad de servicio de los servidores centrales, mediante UPS y Generador Electrógeno.
- Mantener buenas relaciones con los estudiantes y la Federación de estudiantes, para en el futuro en caso de toma o paro estudiantil lograr acceso al Datacenter.
- Tener un set de Dispositivos de Telecomunicación (Switch, Dispositivos Inalámbricos) Cableado de Datos, Conectores RJ45, Herramientas de instalación de Red.
- Mantener actualizada la Base de Datos de los Funcionarios que prestarán Servicios en caso de la Contingencia.
- Ampliar coberturas de conectividad inalámbrica de alta prestación y distancias medias dentro de la ciudad (Enlace Point to Point).

➢ **Detección:**

- En tiempo de efervescencia política estar atento a señales de los Estudiantes, Autoridad y diarios de alcance local.

➢ **Recomendaciones para Funcionarios y Personal de apoyo del equipo de gestión**

- Desinstalar Teléfonos IP, para ser utilizados posteriormente en ubicaciones externas a la Universidad. Solución Telefonía IP permite instalarlos en otras dependencias para que queden operativos.
- Desactivar por BIOS el uso todos puertos USB, Grabadores de CD/DVD y cualquier medio copia de información crítica o estratégica.
- Activar clave de disco duro y BIOS.
- Mantener actualizada la Base de Datos de los Funcionarios que prestarán Servicios en caso de la Contingencia.

Plan de contingencia para usuarios en caso de paro o toma prolongada de la Universidad.

➢ **Prevención:**

- Respaldar la información crítica contenida en las Estaciones de Trabajo.

- Realizar Encriptación de información privada o de índole estratégica en las Estaciones de Trabajo Fijas y Portátiles.
- Como alternativa ante Disponibilidad de Espacio Físico de Respaldo, es factible subir Información mediante Servicios de Almacenamiento en la Red UTALAN.
- Activar claves de BIOS en las Estaciones de Trabajo.
- Activar clave acceso a disco duro o ver mecanismo para hacerlo por BIOS.
- Guardar Estaciones de Trabajo Portátiles bajo llave, en muebles robustos y discretos.
- Guardar Estaciones de Trabajo Fijas (sólo la torre o case) en bodega fuertemente blindadas o bunker en caso de una prolongada ausencia ya sea voluntaria o forzada.
- Asegurar accesos a las oficinas, pasillos interiores, accesos por ventanas laterales, cielo o azoteas.
- Tomar los datos de número de serie, inventario, marca y modelo del equipo bajo su cargo y rasgos que lo caracterizan.
- Instalar sistemas de alarmas, cámaras de vigilancia las 24 horas del día en sectores críticos.
- Tener en las Estaciones de Trabajo Portátiles instalado y configurado acceso por VPN, un teléfono SofPhoneIP o Licencias SIP, para operar desde el exterior de la Universidad.
- Mantener actualizada la Base de Datos de los Funcionarios que prestarán Servicios en caso de la Contingencia.

➢ **Detección:**

- En tiempo de efervescencia política estar atento a señales de los Estudiantes, Autoridad y diarios de alcance local.

➢ **Medidas a tomar durante la Toma o Paro**

- En tiempos iniciales de 1 semana de paro o toma, dejar operativa la red y todos sus servicios anexos.
- Si se prolonga la toma, y ante instrucciones superiores, es factible de desactivar todo servicio de acceso a la red interna e internet, así como la red inalámbrica.
- Supervisar la operación de los Servidores de Correo, Web, Bases de Datos, DNS y otros en forma remota con accesos controlados por VPN o Servicio SSH.

SECRETARIA DE LA UNIVERSIDAD

- Los corte de energía en los automáticos y tableros principales por parte de operaciones y mantenimiento, deben ser informados al Área Ingeniería de Sistemas.
- Se deben mantener en lo posible todos los canales de comunicación abierto para la correcta coordinación de futuras medidas a implementar.

Plan De Contingencia contra Incendios en el Datacenter, o Sectores donde se ubican Dispositivos de Telecomunicación Críticos

➢ **Fuente de Combustión**

Los incendios son causados por el uso inadecuado de combustibles o instalaciones alámbricas defectuosas y el inadecuado almacenamiento y traslado de sustancias inflamables.

En la combustión influye la temperatura, superficie de contacto entre los elementos, para ello antes hay que saber qué tipo de combustión poseen los elementos.

Combustión Lenta: Se da en lugares con escasez de aire, comestibles muy comunes. Este tipo de combustión suele darse en sótanos y habitaciones cerradas, es muy peligrosa, pues en el caso de entradas de aire puede generarse una súbita aceleración del incendio y hasta una explosión.

Combustión Normal: Ocurre cuando el fuego se produce al aire libre o con aire suficiente para brindar aporte a elementos extraños que mantengan la combustión.

Combustión Rápida o Deflagración: Es una combustión rápida, con llama y sin explosión. Suele producirse en áreas enrarecidas y con temperaturas elevadas.

Explosión: Suele darse cuando existe una mezcla de vapor, gas-aire dentro de los elementos que poseen explosividad y en un recinto cerrado.

➢ **¿Que hacer Antes?**

- Verificar extintores y ubique cada uno de ellos según los materiales de combustión que puedan afectar a las instalaciones.

- Comprar un seguro contra incendios.
- Verificar las instalaciones por el personal del Departamento de Bomberos.
- Cree rutas de Salida en caso de Emergencia.
- Hacer Simulacros para verificar que cada persona conoce sus responsabilidades.
- Instalar detectores de humo.
- Colocar sistemas automáticos de rocío en áreas con mucho personal, no recomendable dentro Datacenter, pero si en las oficinas aledañas.
- En el Datacenter sellar completamente cualquier tipo de acceso de aire, e instalar un sistema de vacío, que se gatille al momento de detectar un incendio o humo.
- Revisar las Baterías de detectores de humo.
- Evitar conectar múltiples dispositivos en el mismo tomacorriente o en la misma línea de alimentación de electricidad.
- Evitar sobrecargar los cables con extensiones o equipos de alto consumo (Dimensionar correctamente zapatillas eléctricas, número de tomacorrientes).
- Cambiar cables eléctricos siempre que este perforados o con peladuras.
- Instalación de paredes contra fuego, puertas blindadas que permitan aislar el fuego en ciertas áreas.

➢ **¿Qué hacer Después?**

- No encender Estaciones de Trabajo hasta estar seguro.
- Verificar que no hayan Heridos.
- Hacer un inventario de los Dispositivos afectados.
- De haber situación de contingencia, reubicar instalaciones.
- Limpieza del polvo extintor de incendio a los Servidores, Dispositivos de Telecomunicación, y todo aparato y medios de cableado y fibra, conectores, retirando completamente todos los equipos anteriormente señalados de sala incluyendo gabinetes

➢ **En Todos los Casos**

- Mantener un inventario de todos los elementos físicos en su instalación.

- Crear copias de seguridad de los Datos más importantes.
- Mantener copias de seguridad de su software en un lugar externo a su ubicación actual.
- En caso de tener copias físicas de los Sistemas, asegúrese de guardarlas en un lugar adecuado, en donde no sea afectada por la luz, el agua o el calor.

Plan De Contingencia Contra Inundaciones

➢ Fuente de Inundación

La Inundación, es el exceso de agua por escurrimientos producido por su acumulación en terrenos planos, por falta de drenaje ya sea natural o artificial.

➢ ¿Qué hacer antes?

- Verificar donde se va a construir el Datacenter (¿Zona propensa a Inundación?).
- Instalación de un correcto sistema de drenaje, en caso de no poseerlo, revisar cuidadosamente el que se tenga.
- Hacerse asesorar por un Ingeniero Civil o un Arquitecto para la revisión de la Infraestructura.
- Construir el Datacenter a una altura mayor a la superficie del suelo exterior.
- Construir canales de desagües (cunetas) en caso de considerarse necesario.
- Para evitar problemas con inundaciones, se ha de instalar tarimas de un promedio de 100 cm de altura para la ubicación de los servidores. De esta manera se evitaran inconvenientes como el referido.
- En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.
- Subir las UPS por sobre 100 cm del nivel del piso o sobre piso técnico.
- Para prevenir los corto circuitos, asegurarse de que no existan fuentes de líquidos cerca a las conexiones eléctricas.

➢ En todos los Casos

- Se debe de proveer un cuidado especial a la humedad producida por los Sistemas de Aires Acondicionados.

- Revisar los desagües de las instalaciones antes de la temporada de invierno y darles mantenimiento.
- Procurar no arrojar basura a los desagües para evitar que esta se atore en ellos impidiendo el paso del agua.
- En caso de presentarse la inundación traslade todo lo que pueda a un lugar más elevado o a otras instalaciones fuera del perímetro de la inundación.
- Para cualquiera de los casos de sismo, inundación o incendio se debe de brindar charlas de evacuación, primeros auxilios y rescate de ser necesario para personal nuevo y ya existente.

Plan de contingencia frente a Sismos de mediana o gran envergadura

➢ **Prevención:**

- Todo el personal debe tener claro los puntos de salida de emergencia o de evacuación, áreas seguras y hacer lecturas de la señaléticas existentes, si no existen, se debe consultar al encargado de seguridad de la Institución.
- Ver cuáles son las zonas seguras y vías de evacuación dentro de la ciudad y cercano a la Universidad, para evitar ser alcanzado por maremotos o tsunami (Plano de Inundaciones).
- Fijar bien los objetos peligrosos, de alto peso, gabinetes, armarios en los puestos de trabajo y dejar despejadas las áreas de circulación regular.
- Asegurarse de saber cómo desconectar la energía en las oficinas y el Datacenter (Precaución, ya que los Sistemas seguirán operando pues poseen Sistema de alimentación ininterrumpida SIA o UPS).
- Verificar regularmente la operación de los sistemas de luces de emergencias, señalizaciones de salidas luminosas.
- Ver Factibilidad de un sistema alternativo de Acceso Internet, se recomienda que sea vía satelital para la comunicaciones de datos en caso de aislamiento por un largo período de tiempo (alimentación por Sistemas Fotovoltaicos).

➢ **Durante el sismo:**

- Reaccionar con serenidad y ponga en marcha plan de emergencia, si no lo sabe, averígüelo con el encargado de seguridad.
- En el evento de un desalojo rápido, evite correr, atropellar a otras personas; ayude

a quien lo necesite, mantener las salidas libre de objetos y use las vías de escapes señaladas.
- Apague todo foco de fuego, si es posible corte la energía del sector.
- No acercarse al edificio para evitar ser alcanzado por la caída de objetos peligrosos.
- Ir a lugares abiertos, lejos de cables eléctricos, edificios de altura, postes de alumbrado, árboles o el tráfico vehicular.
- Si no tiene posibilidades de evacuar rápidamente, protéjase debajo de una mesa, bajo el dintel de una puerta, pared o viga maestra, proteja su cabeza con los brazos.

➢ **Precauciones después del sismo:**

- Active plan de emergencia. Provisto por el encargado de seguridad de la Institución, hacer lectura de la información al respecto.
- Aléjese de las construcciones que se encuentren dañadas, no reingrese a su lugar de trabajo, hasta que personal especializado y responsable así lo indique.
- Debe estar preparado para sismos secundarios o replicas que se producen después de un terremoto de gran magnitud.
- Regrese a su hogar o a un lugar prefijado de reunión de la familia en caso de eventos antes señalado, en forma serena o calmada sin desesperarse. Durante este proceso se debe estar atento al tráfico vehicular, dar paso prioritario a vehículos de Emergencia y Seguridad.
- Mantenerse en contacto con la institución por medio de la radio de la Universidad, sistema de telefonía celular o móvil u otro medio activo.
- En caso que el lugar de trabajo se encuentre al nivel del mar, tome las vías de evacuación externas y alcance hasta la zona segura libre de efecto de un Tsunami.
- Reingresar a las oficinas y/o Datacenter luego del visto bueno del especialista en seguridad, constructor o lo que la autoridad determine.
- No reactivar ningún equipo inmediatamente, sin antes realizar limpieza del mismo, verificar los daños de las líneas de energía, conectividad a redes, estado activo y estable de las redes eléctricas, estado de las UPS. Solo encender los equipos electrónicos, cuando se vea una estabilidad en la alimentación eléctrica.
- En período post-sismo, se recomienda el ahorro de energía eléctrica, por lo tanto, bajo esa premisa, solo se activarán los equipos que la autoridad estime conveniente.
- Cuando se ha restablecido el Normal Funcionamiento de las Dependencias, el Datacenter se habilitará de la siguiente forma:

- Activar sistema de aire acondicionado, ver su capacidad de enfriamiento, ver si tiene fugas de aire frío al exterior desde los ductos, en caso necesario, se debe llamar al especialista o contratista para su reparación.
- Con el Normal funcionamiento del Sistema de Aire Acondicionado, la secuencia sigue con los Dispositivos de Telecomunicación (Switch Core, Switch de Distribución, Router), verificando su correcto funcionamiento.
- Verificar Servicio de acceso interno y externo (Intranet e Internet).
- Sistema Telefónico Alcatel.
- El sistema telefónico es prioritario reponerlo, se debe verificar el correcto funcionamiento de los Dispositivos de Telefonía IP en Rack 4 Datacenter Campus Saucache (Suministro Eléctrico, Patch Cord, Servidores Call Center, Call Manager).
- Servidores del Datacenter.
    - Activar Sistemas de servidores DNS, DHCP y Correo Institucional.
    - Sistema de Servidores Web, Intranet y Bases de Datos, verificar estado de los discos.
- Verificar Dispositivos de Telecomunicación Intermedios (Backbone).
- Verificar Operación en los Gabinetes Intermedios de Backbone y Switch de Acceso a los Usuarios.
- Verificar las Estaciones de Trabajo de los usuarios finales tanto a nivel de energía eléctrica como de datos.