UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS
RED DE DATOS – UDNET

PLAN DE CONTINGENCIA

1. Objetivos

Objetivo General:

Garantizar la continuidad de los servicios de informática y telecomunicaciones a través de la elaboración y ejecución de políticas, procesos, procedimientos ante cualquier eventualidad o desastre que pueda ocurrir.

Objetivos específicos:

1. Definir los lineamientos de recuperación y acciones a seguir ante una eventualidad
    a. **Actividad:** Generar un documento en el que se dicten las directrices, criterios o lineamientos generales a seguir antes, durante y después de una eventualidad o desastre.

2. Identificar los elementos, sistemas, aplicaciones o funciones de la red de datos UDNET que sean críticos ante cualquier eventualidad o desastre y evaluarlos de acuerdo al impacto que generen dentro de la Universidad.
    a. **Actividad:** Realizar un panorama de riesgos de los sistemas, aplicaciones, elementos y funciones de red del área de la Red de Datos, en donde se evalúe el impacto, la consecuencia y se digan los controles existentes frente a esta eventualidad.

3. Identificar la contingencia de cada problemas previsibles que permita continuar la operatividad y funcionamiento de los sistemas de telecomunicaciones.
    a. **Actividad:** Documento en donde se especifique nombre de la contingencia, recursos y costos asociados a cada una, priorización de ejecución cada alternativa

4. Socializar los procesos y procedimientos que hacen parte del plan de contingencia.
    a. **Actividad 1:** Capacitar sobre el plan de contingencia a los responsables de los sistemas críticos.
    b. **Actividad 2:** Capacitar al usuario final de cada sistema sobre el plan de contingencia.
5. Actualización de Plan de contingencia
    a. **Actividad:** Actualizar periódicamente el documento de acuerdo a los cambios que se vayan presentando.

2. Evaluación y diagnóstico:

El crecimiento permanente y acelerado de la Universidad en cuanto a cobertura, ampliación de servicios, ubicación geográfica, aumento de personal docente, y de apoyo administrativo (OPS) para atender diferentes frentes, entre otros, ha hecho que la infraestructura de telecomunicaciones e informática, se desarrolle con características de resolver situaciones urgentes, las cuales se convierten en soluciones permanentes cuyo uso las institucionaliza, sin estar enmarcadas en planes de desarrollo institucional. Debido a esto, el crecimiento se ha hecho de manera desordenada, no consultada y sin una proyección a mediano y largo plazo. Es urgente llevar adelante una evaluación que permita identificar el estado actual de las telecomunicaciones y la informática, que permita hacer proyecciones en dos sentidos: 1) modificación, retoma, cambio de equipos, cambio de situaciones 2) crecimiento a mediano y largo plazo. Para la evaluación se propone ejecutar la ***METODOLOGIA DE AUTODIAGNÓSTICO DE LA INFRAESTRUCTURA TECNOLÓGICA DE CONECTIVIDAD*** propuesta por ALCALDIA MAYOR DE BOGOTA – SECRETARIA GENERAL, aplicando los formularios enunciados a continuación:

1. RED ELECTRICA Y EQUIPOS DE RESPALDO ELECTRICO
2. CABLEADO ESTRUCTURADO
3. CENTRO DE COMPUTO (DATA CENTER)
4. EQUIPOS ACTIVOS
5. CANALES DE COMUNICACIONES Y ACCESO A INTERNET
6. SISTEMA DE COMUNICACIONES DE VOZ
7. SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION
8. SERVICIOS DE RED

3. Organización

En caso de una eventualidad o desastre que conlleve la necesidades de contingencia de nivel operativo el personal responsable del equipo, aplicación o funciones de la red se hará cargo de la aplicación de este, sin embargo si es un desastre natural o público se contactará con la entidad encargada de resolver la eventualidad.

4. Matriz DOFA

Se tomó esta herramienta administrativa como parte de un análisis estratégico para verificar en que nos encontramos cuales son nuestras puntos a favor y en contra de esta manera podemos identificar los posibles riesgos latentes.

DEBILIDADES	FORTALEZAS
➢ Resistencia al cambio por parte de todos los estamentos universitarios. ➢ Deficiencia de personal para realizar las tareas y los proyectos del proceso a tiempo. ➢ Huelgas, protestas, toma de instalaciones que hacen que retrasen o interrumpan los servicios ➢ En un alto porcentaje el proceso cuenta con personal contratado mediante orden de prestación de servicios, esto hace que exista alta rotación de personal que tiene la experiencia y los conocimientos especializados y cuando realizan estos cambios retrasan los procesos.	➢ Contar con una red adecuada para la interconexión que soporta los diferentes procesos académicos y administrativos. ➢ Existen planes de adquisición de Tecnología a corto y mediano plazo. ➢ Existe recurso humano Académico y Administrativo, capaz de aportar conocimiento y experiencias Informáticas.

➢ Limitados recursos económicos para mejorar la red institucional ➢ Limitados recursos económicos para la puesta en marcha de una red de alta velocidad que soporte la interconexión interna y externa. ➢ El personal contratado mediante orden de prestación de servicios maneja equipos y procesos críticos lo que requiere capacitaciones de la infraestructura que maneja. Por ser de este tipo de contratación la Universidad no permite capacitaciones, sino transferencia de conocimiento por lo que este nunca puede ser certificado. ➢ Limitada infraestructura física y lógica en cuanto a equipos de cómputo, plataforma tecnológica y desarrollo de software. ➢ Desconocimiento parcial de los recursos existentes en telecomunicaciones y tecnologías de la información. ➢ Se han desarrollado al interior de la universidad aplicaciones y/o sistemas de información de manera parcializada algunas sin una dirección central. ➢ Falta de comunicación interna ya que las áreas no conocen las funciones y resultados de las demás. ➢ Falta de aplicar una cultura organizacional y un sistema de calidad que permita el flujo de información adecuada entre las áreas de la universidad.	➢ Existe una infraestructura de RED aprovechable en la Universidad ➢ Se cuenta con infraestructura de hardware y software para cubrir las necesidades del cliente. ➢ Se cuenta con personal capacitado en áreas técnicas. ➢ Se cuenta con desarrollos propios que se convierten en servicios que solventan las necesidades del cliente.
OPORTUNIDADES	**AMENAZAS**
➢ Asignación de dineros por parte de la estampilla. ➢ Implementar y mejorar la infraestructura física, tecnológica, de conectividad y de medios educativos adecuada y coherente, para garantizar el desarrollo de las funciones misionales de la universidad, la comunicación y el bienestar institucional. ➢ Nuevas formas de aprendizaje y apropiación del conocimiento generado por el avance vertiginoso de las tecnologías de la información y las comunicaciones ➢ Reconocimiento del papel de las nuevas tecnologías de la información y la comunicación para incrementar los aprendizajes. ➢ Creciente dotación de infraestructura física y lógica necesaria para recibir formación.	➢ Nuevas exigencias de ampliación de cobertura sin el correspondiente crecimiento en recursos humanos, físicos y tecnológicos ➢ Saturación de la red. ➢ La rotación de los empleados de la empresa suele ser amplia, lo que influye directamente en el número de asociados y en la continuidad de las actividades que realizan ➢ Cambios tecnológicos acelerados.

➢ Se podría dejar en planta al que existe en este momento como (OPS) el cual es el personal idóneo para hacer levantamiento de información y para cumplir con los objetivos del proceso. ➢ Implementar convenios interuniversitarios que permitan el intercambio de conocimientos por medio de las plataformas administradas por el proceso. ➢ Implementar la opción de dar clases virtuales que permitan que estudiantes del extranjero puedan acceder a la educación que brinda la universidad. ➢ Realizar relaciones interinstitucionales para compartir conocimientos y tecnología que puedan ayudar a mejorar las TICS de la institución.	➢ No ampliación de la estampilla cuando se venzan los términos del acuerdo.

5. Panorama de riesgos

IDENTIFICACION DEL RIESGO			ANALISIS DEL RIESGO			MANEJO DEL RIESGO
RIESGO	**CAUSAS**	**CONSECUENCIA**	**PROBABILIDAD**	**IMPCTO**	**ZONA DE RIESGO**	**ACCIONES /CONTROLES**
Pérdida de la configuración de los equipos telefónico	* Usuarios malintencionados * Falta de capacitación al usuario final * Mal uso de los teléfonos	* Inestabilidad en la continuidad de los servicios * Incomunicación total o con dificultades * Pérdida de tiempo al realizar el desplazamiento hasta el sitio para su reparación	**BAJA**	**ALTO**	**MODERADO**	* Manuales para los usuarios finales * Adquisición de una plataforma segura (encriptación de llamadas)
Fallas en la comunicación telefónica IP	* Ancho de banda insuficiente entre la sede central y la sede remota. * daño en la configuración de los equipos * Retardo entre enlaces	Deficiencia en el servicio	**BAJA**	**ALTO**	**MODERADO**	* Aumento de ancho de banda * Calidad de servicio en teléfonos y en regiones * Optimización de ancho de banda (compresión de voz)
Errores de configuración el los aparatos telefónicos	* Falta de capacitación * Falta de conocimiento en el procedimiento de instalación y configuración del aparato telefónico * Errores en el administrador	* Deficiencia en el servicio * Deficiencia en el uso de los aparatos telefónicos	**BAJA**	**BAJO**	**ACEPTABLE**	* Pruebas o laboratorios para aplicar configuración en la plataforma
Uso inadecuado de los códigos de servicios especiales	* Divulgación de claves por parte de los usuarios * Usuarios malintencionados	* Interceptación de la información	**BAJA**	**MEDIO**	**TOLERABLE**	* Cambio de código de servicios especiales según su uso * Cambio de código por cambio de usuario

Errores del administrador	* Personal inadecuado para la labor que desempeña * Falta de capacitación	* Deficiencia en el servicio * Daño en el software * Daño en la configuración de los aparatos telefónicos * Daño en el software de los aparatos telefónicos	**BAJA**	**MEDIO**	**TOLERABLE**	* Se contrata personal idóneo para las labores a desempeñar
Daños a equipos de red	* Fallas eléctricas * Terminación de vida útil * Falta de mantenimientos * Condiciones ambientales inapropiadas	* Caída de la red que atiende el equipo dañado	**MEDIA**	**ALTO**	**IMPORTANTE**	* Instalación de UPS * Mantenimientos programados * Seguimiento de las fechas de vida útil de los equipos. EOS (end of sale), EOL (end of life time) * Adecuación de cuartos de telecomunicaciones TR (telecommunication room)
Pérdida de la configuración de los equipos	* Fallas de hardware en la memoria no volátil NVRAM * Reinicio inesperado del sistema * Olvido por parte del administrador para salvar la configuración	* Caída de la red que atiende el equipo dañado	**BAJA**	**ALTO**	**MODERADO**	* Adquisición de nuevos equipos * Realización de backup de los equipos más importantes
Fallas en la certificación del cableado	* EMI y RFI (interferencia electromagnética e interferencia por radiofrecuencia) * Mala instalación de cableado (ponchado, cable maltratado)	* Mal desempeño de los puntos cableados * Existe conectividad limitada o nula	**BAJA**	**MEDIO**	**TOLERABLE**	* Capacitación en los procesos del cableado * Diseño previo que evite o aislé las fuentes de EMI y RFI
Caída de enlace de datos	* Problemas en la red del proveedor de servicios de telecomunicaciones TSP	Sedes sin servicio de red contra el nodo central	**BAJA**	**ALTO**	**MODERADO**	Se sigue el procedimiento de comunicación Help Desk con el proveedor
Problemas con el direccionamiento IP	* Instalación no autorizada de equipos que entregan direcciones IP * Caída de servidor DHCP	Los equipos que toman IP en un segmento de red equivocado no pueden navegar	**MEDIA**	**ALTO**	**IMPORTANTE**	* Se detectan los equipos y se desactivan
Ataque a los equipos de red	* Equipos de telecomunicaciones desactualizados en hardware y/o software * Sistemas de conexión para la administración no seguros	Denegación del servicio	**MEDIA**	**ALTO**	**IMPORTANTE**	*Actualización del software de los equipos que se encuentran con tiempo de vida activo * Reemplazo de los equipos cuyo tiempo de vida ya caduco
Daño en los servidores	* Falta de mantenimiento de los servidores * Instalaciones físicas inadecuadas * Condiciones ambientales inapropiadas	* Interrupción de los servicios que el servidor soporta	**BAJA**	**ALTO**	**MODERADO**	* Mantenimientos programados (2 preventivos en el año) * Adecuación del espacio físico con estándares internacionales
Pérdida de la información de la SAN	* Mal apagado de la SAN * Fallas eléctricas * Daño en disco	* Pérdida de información	**BAJA**	**ALTO**	**MODERADO**	* Mantenimientos preventivos * Garantía de los discos * Backups en medio magnético
Daños de sistemas operativos en los servidores	* Mala administración * Daños en disco * Ejecución errónea del mantenimiento	* Interrupción de los servicios que el servidor soporta	**BAJA**	**ALTO**	**MODERADO**	* Revisión de logs * Supervisión de mantenimientos

Demora en la aprobación, revisión y ejecución de términos de referencia	* Demora en los procesos administrativos de contratación * Respuesta baja y lenta de proveedores * Solicitudes técnicas desactualizadas y obsoletas * Cambio tecnológico acelerado	Atraso en la contratación de insumos tanto humano como tecnológico provocando un retraso y fallas en las actividades de la red	**BAJA**	**ALTO**	**MODERADO**	
Pérdida de contraseñas de administrador	* Robo de contraseñas * Olvido de las contraseñas * Las contraseñas no se encuentran debidamente resguardadas * El administrador se vaya y no deje las contraseñas	* Tomar posesión de los servidores sin autorización * Pérdida de información * Cambio o pérdida de la configuración de los servicios	**BAJA**	**ALTO**	**MODERADO**	* Contraseñas escritas en sobre cerrado actualizadas cada año * Las contraseñas deben tener una combinación alfanumérica
Ataques a los servidores por medio de software malicioso	* No tenga instalado la licencia de antivirus * No se encuentre debidamente configurado el antivirus * No se encuentre actualizado el antivirus	* Daño en los archivos de configuración del servidor que podría ocasionar fallas en el servicio que se preste * Perdida de información * Daño en el sistema operativo	**MEDIA**	**ALTO**	**IMPORTANTE**	* Licenciamiento de antivirus * Backups a la información de los servidores
Vulnerabilidades o huecos de seguridad en software	No se tengan las últimas actualizaciones , parches, puertos cerrados, firewall	* Pérdida de información * Apoderamiento de la máquina * Robo de información * Servicios no disponibles	**BAJA**	**ALTO**	**MODERADO**	* Actualizaciones permanentes de los servicios y sistema operativo
Se acabe el espacio en el disco de los servidores	* No se tenga planeado el crecimiento de la información * Virus * Falta de revisión log	No se puede prestar los servicios que soporta el servidor	**MEDIA**	**ALTO**	**IMPORTANTE**	* Revisión de logs periódicamente * Liberación constante de archivos innecesarios
Publicar información desactualizada y/o errada.	* No se tienen identificadas o no existen las fuentes de información. * El usuario que publica NO tiene la experticia y conocimiento para hacerlo. * No existe la política y/o protocolo para revisar la información a publicar. * El usuario desconoce o no aplica la resolución 711 de 2008 para publicación Web * Problema en la estructura organizacional * Descuido del usuario * Errores en la digitalización * Falta de documentación * No existen políticas para el tiempo de información * Recurso humano capacitado flotante * Desfases entre el tiempo de contrato y tiempo operativo * Las oficinas no verifican la veracidad y al pertinencia de la información publicada	* Generar confusión en la comunidad. * Problemas jurídicos y legales. * Problema de transparencia institucional * Mala imagen institucional	**MEDIA**	**MEDIO**	**MODERADO**	* Revisión periódica por área web. * Proceso de concientización * Aprobación de las políticas * Contratos ajustados a tiempo de operación de la u

Publicar información malintencionada	* Acceso no autorizado. (hacer daños por medio de terceros) * Usuario autorizado que publica información no institucional, o con fines personales * No se revisa la información a la hora de la activación o la publicación. * Sufrir un ataque al sitio que modifique la información publicada * Falta de responsabilidad y prudencia en el uso de la información	* Daño a la imagen institucional * Generar confusión * Perjudicar el buen nombre de oras instituciones y/o personas * filtración de información * Inconsistencia en la información	**BAJA**	**ALTO**	**MODERADO**	* Realizar capacitaciones * Realizar manuales * Revisión periódica por parte de la persona encargada
Problemas legales	* Utilizar software sin licenciamiento * No respetar las normas y leyes de derechos de autor * Problemas de cultura	* Cárcel * Multas * Sanciones * Desprestigio para la institución	**MEDIA**	**ALTO**	**IMPORTANTE**	* Adquirir los programas con licenciamiento * Política de publicaciones * Aplicación de la resolución 711 * Capacitación a los usuarios * Casos de éxito
No se puede acceder a la información publicada	* Errores en los formatos de la presentación de la información * Errores técnicos que hacen que los servicios fallen * El usuario no tiene las herramientas para ver la información * Manejo de software incompatible * Incompatibilidad de versiones	* Generar confusión * Problemas legales * Demora en los procesos	**BAJA**	**MEDIO**	**TOLERABLE**	* Capacitación al usuario * Manuales para presentación de la información y conversión de la información * Estándares de publicación * Revisiones y pruebas de versión a los documentos a publicar * Recomendaciones a los usuarios del formato en el que se encuentra publicada la información
Publicar información malintencionada en los mecanismos de retroalimentación del Portal	* Usuarios malintencionados * Mal uso de las herramientas de retroalimentación * Ataques informáticos * mala configuración de las herramientas * Error humano * Versiones desactualizadas de programas	* Generar confusión * Problemas legales * Vulnerar principios fundamentales * Desprestigio de la institución *Interrupción de un servicio o portal	**BAJA**	**MEDIO**	**TOLERABLE**	* Hacer pruebas identificando errores para poner en producción * Crear protocolo para la publicación de la información * Capacitación a los usuarios * Manuales para el uso de los servicio
Demora en la publicación de la información	* Demora en el proceso de revisión y activación * Demora en el envío de las correcciones	* Venzan términos	**BAJA**	**BAJO**	**ACEPTABLE**	* Establecer un protocolo para la revisión y activación de información. * Capacitar a las personas que publican información

No se articule o active el mecanismo para recibir retroalimentación	* Problema de planeación * Problemas técnicos * No se habiliten los canales de comunicación y retroalimentación * No se informa de la habilitación * Problema cultural	* No exista la retroalimentación de la información publicada * Comunicación errónea	**BAJA**	**BAJO**	**ACEPTABLE**	* Definir claramente los mecanismos de retroalimentación y determinar si viabilidad técnica * Hacer pruebas o simulacros * Hacer capacitaciones * Realizar manuales de uso de los servicios
Mal funcionamiento de un aplicativo	* Deficiencias en el mantenimiento * Mal diagnóstico a la detención de la falla * Implementación de una solución no adecuada * Uso de actualizaciones y parches de seguridad que producen mal funcionamiento	* No se puede hacer uso correcto del servicio * Demoras en la respuesta a las solicitudes hechas con ese servicio	**BAJA**	**ALTO**	**MODERADO**	* Crear un ambiente de desarrollo por etapas que incluya desarrollo, pruebas y producción *Uso de estándares y procedimiento de detección de fallas * Hacer iteraciones para corregir las publicaciones
Daños en hardware, software o medios	* Fallas en el funcionamiento* Inadecuada manipulación de equipos y medios* Almacenamiento inadecuado de medios* Virus en el sistema	* Caída total o parcial del servicio* Problemas de actualización del sitio	**BAJA**	**ALTO**	**MODERADO**	* Redundancia en los equipos claves* Cultura en el manejo y almacenamiento de los equipos y medios* Mantenimiento preventivo y correctivo* Manejo de vida útil
Errores en los diseños de los módulos del portal	* Errores en el levantamiento de información * Errores en el diseño * Problemas de planeación * No uso de metodología * Inadecuada organización de herramientas e instrumentos	* Módulos sin funcionalidad ni aplicabilidad * Deficiencia en el funcionamiento * Saturación	**BAJA**	**MEDIO**	**TOLERABLE**	* Uso de estándares de desarrollo * Interacción con el usuario * Iteraciones de actualización * Revisiones y pruebas en entornos controlados
Inadecuada aplicación de las políticas de comunicación	* No existen políticas aprobadas * Falta de capacitación	* procesos erróneos * Desinformación * duplicidad en la información * inconsistencia en la información * No existe congruencia en la imagen institucional	**ALTA**	**ALTO**	**INACEPTABLE**	* Creación y socialización de las políticas de comunicaciones ajustadas a las necesidades de la institución. * Creación de la oficina o dependencia de comunicaciones * Articulación de la oficina de comunicaciones con el resto de las dependencias

Pérdida de la información	* Problema de cultura * Falta de capacitación * Inadecuada o inexistencia realización de copias de seguridad * Ataque informático a los sistemas * Ataques de virus informáticos * Inadecuado manejo de la información y las herramientas de la información * Robo o pérdida de dispositivos de almacenamiento con información	* Demora en los procesos * Uso indebido de la información * Problemas legales	**MEDIA**	**ALTO**	**IMPORTANTE**	* Cultura en el manejo y almacenamiento de los equipos y medios * Concientización al usuario sobre la clasificación y el manejo de la información * Definición de roles de usuario de acuerdo a la forma de acceder y hacer uso de la información * Implementación de políticas de copias de seguridad * Implementación de políticas de digitalización de la información
Publicación de información confidencial	* Falta de responsabilidad y prudencia en el uso de la información * Error humano * Error en la verificación de la información	* Robo * Problemas legales * Vulneración de derechos fundamentales	**BAJA**	**ALTO**	**MODERADO**	* Cultura en el manejo de información * Políticas claras de publicación de la información * Concientización al usuario sobre la clasificación y el manejo de la información * Definición de roles de usuario de acuerdo a la forma de acceder y hacer uso de la información

Las fallas a considerar dentro de este plan de contingencia son fallas en:

- La red eléctrica
- Red de datos
- Problemas con el servidor
- Estaciones y periféricos
- Servicios de internet

Además se realizó por medio de la metodología AMFE (Análisis Modal de Fallas y Efectos) un levantamiento de riesgos más específicos para el área de servidores perteneciente a la Red de Datos Ver anexo A.

ANTES

Siempre que exista un fallo o eventualidad se debe tener en cuenta la seguridad física y lógica de los componentes comprometidos por esta razón antes de cualquier evento se deben tener identificados los siguientes aspectos:

- Ubicación del edificio donde se encuentra el centro de gestión Olimpo, los cuarto de comunicaciones y el equipo o componente.
- Ubicación dentro del edificio donde se encuentran ubicados los equipos o componentes de telecomunicaciones que ha fallado.
- Elementos de la construcción se debe tener plenamente identificados en que material están realizada la infraestructura en caso de una catástrofe natural para así mismo responder ante la situación.
- Potencia eléctrica se deben tener identificados los tableros eléctricos, si tiene UPS el equipo afectado, si la infraestructura cuenta con planta eléctrica que soporte por un tiempo prudencial los equipos.
- Se debe identificar el sistema contra incendios y se debe capacitar al personal sobre la manera de usarlo.
- Se debe conocer el protocolo de acceso al Centro de Gestión Olimpo.
- Se deben conocer plenamente las políticas de seguridad de las telecomunicaciones de la red de datos UDNET.
- Identificar, conocer y mantener actualizado el plan de riesgos dónde está determinada la tolerancia del sistema.
- Tener un presupuesto o una contingencia de partes o materiales para suplir la parte afectada.

Planta de emergencia

- Contar con una planta de potencia regulada que suministre energía in situ.
- Supervisar periódicamente el nivel de combustible, agua, baterías todo lo necesario para que funcione adecuadamente ante cualquier eventualidad.
- Realizar periódicamente un mantenimiento preventivo.
- Contar con equipo contra incendios cerca de la planta eléctrica.
- Contar con el mapa eléctrico del área.
- Contar con tierras físicas independientes a la de los servicios de telecomunicaciones.

UPS

- Contar con UPS con capacidades necesarias en todos los cuartos de comunicaciones de las diferentes sedes.
- Realizar periódicamente un mantenimiento preventivo a las UPS para su óptimo funcionamiento.
- Contar con el mapa eléctrico en donde estén identificadas las UPS existentes.
- Determinar semestralmente el tiempo efectivo y real de respaldo de la UPS con respecto a las diferentes cargas.

Generales

- Contar con un directorio de los responsables del suministro eléctrico en cada sede.
- Contar con un procedimiento y un protocolo para reportar el incidente a las áreas involucradas
- Contar con un procedimiento o un protocolo para notificar a los usuarios afectados la probable baja de los servicios de telecomunicaciones.
- Contar con un instructivo de ejecución de respaldos de emergencia a la información del servidor WEB, mail, DNS, configuraciones de equipos principales y centrales.

DURANTE

Cualquier desastre o evento que ocurre tiene la capacidad de interrumpir una o varias actividades del proceso normal de la entidad, es por ello que se debe ejecutar un plan de contingencia adecuado para responder en el menor tiempo posible impactando en un porcentaje muy bajo las actividades o procesos que intervienen en el evento.

Estos puntos definidos en este plan ayudan a coordinar la recuperación de las operaciones afectadas por el riesgo.

- Establecer e informar a la comunidad afectada un periodo crítico de recuperación, en el cual los procesos deben ser recuperados antes de sufrir pérdidas significativas.
- Realizar un listado de las operaciones críticas que deberán ser prioridad en el momento de la recuperación.
- Seguir el protocolo, instructivo, procedimiento levantado para aplicarlo al momento de la eventualidad.
- Comunicarse con recursos físicos para la supervisión de la planta eléctrica.
- Monitorear las UPS cada 20 minutos para programar acciones mayores.
- En caso de ser necesario dar equipos activos y/o servicios de baja para evitar daños o pérdida de información.
- En caso de se necesite por más tiempo la UPS apagar los equipos no prioritarios o que no demanden uso mientras se resuelve e evento.
- En caso de una catástrofe natural o pública se debe seguir el plan de contingencia general de la Universidad Distrital.
- Asegurar la capacidad de las comunicaciones en caso de ser necesario.
- Asegurar los backups de los servidores críticos en caso de ser necesario.

DESPUÉS

- Brindar un tiempo prudencial para restablecer los equipos activos y servicios.
- Restablecer los equipos activos y servicios que se dieron de baja en forma paulatina.
- Validar el correcto funcionamiento de los servicios y equipos afectados.
- Aplicar en el formato de eventualidades la hoja de vida del riesgo presentado.
- Si el daño es significativo averiguar la cobertura y el costo del impacto.
- Restablecer los backups si es necesario.
- Cambiar la parte del equipo o del componente afectado o pedir garantía si la tiene.
- Actualizar el panorama de riesgos.
- Notificar a los usuarios afectados el restablecimiento de los servicios y la condición en que quedaron.
- Llenar el formato de registro de incidentes en el cual se antora lo sucedido y como se resolvió el incidente

6. Recuperación:

actividades post-ejecución de la medida de contingencia que permiten el retorno a las actividades normales. A partir del formato de documentación del evento ***"Ejecución o Aplicación del Plan de contingencia"*** se debe hacer el proceso de recuperación: se desarrollan las actividades necesarias y se documenta la recuperación sobre el formato pc 005 "Recuperación":

PROTOCOLO DE GESTIÓN DE INCIDENTES Y REQUERIMIENTOS DE SERVICIOS TIC DE LA RED DE DATOS DE LA UNIVERSIDAD DISTRITAL F.J.C.

1. Objetivo General

Brindar un servicio eficiente, eficaz y oportuno a los usuarios de la Universidad Distrital FJC, en la atención de sus solicitudes generales de TIC prestadas por la red de Datos, minimizando al máximo el impacto negativo sobre una normal ejecución de los procesos y el logro de los objetivos de la Entidad.

1.1. Objetivos específicos

Los objetivos establecidos para la Gestión de los Incidentes y Requerimientos, son:

- Asegurar que los métodos y procedimientos definidos sean usados para dar respuestas, realizar análisis, documentación, gestión continua y reporte pertinente y eficiente de los incidentes y requerimientos de servicios de TIC.
- Aumentar la visibilidad y comunicación de los incidentes y requerimientos, tanto a la Entidad como al personal de soporte de TIC.
- Optimizar la percepción del negocio sobre TIC a través de un esquema profesional en la pronta resolución y comunicación de los incidentes, cuando estos ocurran y en la atención de los requerimientos, cuando estos se generen.
- Alinear las actividades y prioridades de Gestión de incidentes y Requerimientos con las de la Universidad.
- Mantener y mejorar de forma continua la satisfacción del usuario con la calidad de los servicios de TIC.
- Proveer asistencia sobre quejas e información general de servicios de TIC.

2. Gestión de Incidentes y Requerimientos

Gestión de Incidentes es el lineamiento definido para el manejo del ciclo de vida de todos los Incidentes y asegura que la operación normal del servicio sea restaurada lo más pronto posible y que el impacto, a los servicios TIC ofrecidos en la Universidad, sea el mínimo.
Gestión de Requerimientos es el lineamiento definido y responsable de la gestión del ciclo de vida de todos los requerimientos de los usuarios de la Universidad, frente a los servicios de TIC.

3. Visión General

3.1. Gestión de Incidentes:

El lineamiento de Gestión de Incidentes, se enfoca en:

- Restablecer el nivel normal de operación del servicio tan pronto como sea posible, luego de que se ha reportado un incidente. Para ello, el Gestor de Incidentes debe coordinar y aunar esfuerzos junto con los grupos de la Operación (Administrador de servidores y almacenamiento, Administradores de herramientas colaborativas y otras aplicaciones, Administrador de redes y equipos de seguridad perimetral, Administrador de telefonía, Líder de Infraestructura Tecnológica, Líder de Ingeniería de Software) y dado el caso, junto con la Dirección de TIC de la Universidad, con el fin de buscar y dar soluciones.
- Reducir cualquier efecto adverso sobre las operaciones del negocio, siendo esto posible dada la coordinación realizada por el Gestor de Incidentes.
- Mantener el mejor nivel de calidad y disponibilidad posible del Servicio.

3.2. Gestión de Requerimientos:

El lineamiento de Gestión de Requerimientos, se enfoca en:

- Manejar todos los Requerimientos de Servicio frecuentes, de bajo riesgo y de bajo costo.
- Manejar los Requerimientos de Servicio reportados a la Dirección de TIC de la Universidad en el horario normal o hábil de trabajo.

3.3. Respecto a los Incidentes

De acuerdo a los siguientes incidentes se listan las actividades por roles de usuario

3.3.1. Falta de acceso físico a estación de trabajo

Las actividades relacionadas a continuación se realizarán en el caso de presentarse eventos imprevistos que impidan el acceso de usuarios finales a sus estaciones trabajo.

3.3.1.1. Actividades Preventivas

Responsable: Equipo Técnico de TIC

- ✓ Realizar inventario de equipos atendidos
- ✓ Generar listado de nombre de usuarios por Equipo
- ✓ Generar listado de nombre del Equipo
- ✓ Identificar Mac de Equipo
- ✓ Identificar estado de equipo (red, dominio, antivirus)
- ✓ Configurar encendido de equipo “wake up on lan”

3.3.1.2. Actividades para la solución del incidente

Responsable: Equipo Técnico de TIC

- Adecuaciones de conectividad.
- Configuración acceso remoto a equipo de usuario final.
- Configuración acceso externo a la Universidad si se requiere. (VPN y solución de virtualización)
- Entrega de Equipo a usuario sin acceso a trabajo previa asignación de nuevo puesto de trabajo.

Responsable: Usuario Final

- Recibir nuevo equipo si es necesario.
- Leer manual de conexión a escritorio remoto (Anexo 1) si es requerido y autorizado para realizar sus actividades
- Ver el video de manual de conexión VPN (Anexo 2) y leer manual solución de virtualización (Anexo 3) si es requerido y es autorizado para realizar sus actividades.

Glosario

- Red: Conexión de varios computadores mediante elementos que facilitan su comunicación.
- TIC: Tecnología de la Información y de las Comunicaciones
- Requerimiento: Solicitud para asignación de cualquier recurso tecnológico.
- Incidente: Es un evento sobre un recurso tecnológico o servicio que impide al usuario su normal y continua labor

Observaciones:

El presente plan se desarrolla a partir de las funcionalidades y servicios que administra y ofrece la Red de Datos de la Universidad Distrital, la cual está organizada en las siguientes áreas:
Área de Redes Convergentes: telecomunicaciones, telefonía IP y apoyo en automatización
Área de Plataformas: administración y gestión de plataformas computacionales (Linux, Windows) y servidores bajo la responsabilidad de UDNET
Área Web: Administración y gestión del Portal Web Institucional.
Área de Soporte: atención al usuario final en sistemas operativos, y equipos de computación