# PLAN DE CONTINGENCIA

# RED DE DATOS UDNET

## Actualizado: febrero de 2020

## Tabla de contenido

## 1. OBJETIVOS

### 1.1. Objetivo General:

Definir los lineamientos para el manejo de incidentes, en el marco de los eventos que afecten la disponibilidad, confidencialidad e integridad de la información, para garantizar la continuidad de los servicios de informática y telecomunicaciones, con el fin de brindar un servicio eficiente, eficaz y oportuno a la Universidad Distrital Francisco José de Caldas, con los servicios prestados por la Red de Datos UDNET, minimizando el impacto negativo sobre una normal ejecución de los procesos y procedimientos institucionales.

### 1.2. Objetivos específicos:

1. Identificar los activos de información, es decir 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.
2. Identificar la contingencia de cada problema previsible que permita continuar la operatividad y funcionamiento de los sistemas de informática y telecomunicaciones.
3. Socializar los procesos y procedimientos que hacen parte del plan de contingencia, para aumentar la visibilidad y comunicación de los posibles incidentes y requerimientos especiales, tanto a la Entidad como al personal de la Red de Datos UDNET y demás áreas encargadas de temas de TI dentro de la Institución

## 2. ALCANCE DEL DOCUMENTO

El presente documento contiene las actividades para solución de contingencias con respecto a la infraestructura de telecomunicaciones, seguridad, almacenamiento, procesamiento y data center administrada por la Red de Datos UDNET desde donde se presta soporte técnico y atención.

## 3. 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 (CPS) 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, gran parte del crecimiento se ha hecho de manera desordenada, no consultada y sin una proyección a mediano y largo plazo. UDNET ha venido adelantando una revisión permanente del estado de la infraestructura TI, lo cual indica que se deba hacer proyección en dos sentidos: 1) modificación, retoma, cambio de equipos, cambio de situaciones 2) crecimiento a mediano y largo plazo.

## 4. CONSIDERACIONES ANTES DE LA CONTINGENCIA

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

| Ítem | Actividades | Responsable |
|---|---|---|
| 1 | · Ubicación de los edificios donde se encuentran los *Data Centers*, los cuartos de comunicaciones y los equipos y componentes tecnológicos. | Planeación UDNET |
| 2 | · Ubicación dentro del edificio donde se encuentran ubicados los equipos, servidores o componentes de telecomunicaciones que han fallado. | Planeación UDNET |
| 3 | · Tener plenamente identificados los elementos y materiales de la construcción, para en caso de un incidente de mayor magnitud o una catástrofe, poder responder ante la situación. | Planeación, Recursos Físicos |
| 4 | · Se deben tener identificados los tableros eléctricos, si se cuenta con UPS para soporte del equipo afectado, si la infraestructura cuenta con planta eléctrica que apoye por un tiempo prudencial el funcionamiento de los equipos. | Recursos Físicos |
| 5 | · Se debe identificar el sistema contra incendios y se debe capacitar al personal sobre la manera de usarlo. | Recursos Físicos, UDNET |
| 6 | · Se debe conocer el protocolo de acceso al Centro de Gestión Olimpo y a los diferentes Centros de Datos ubicados en las demás sedes. | UDNET |
| 7 | · Tener un presupuesto y una contingencia de repuestos, partes o materiales, para suplir los elementos afectados. | Planeación y Vicerrectoria Administrativa |
| 8 | · Contar con plantas de potencia regulada, que suministren energía *in situ*. | Recursos Físicos |
| 9 | · Supervisar periódicamente el nivel de combustible, agua, baterías y demás elementos necesarios, para que las plantas eléctricas funcionen adecuadamente ante cualquier eventualidad. | Recursos Físicos |
| 10 | · Realizar periódicamente un mantenimiento preventivo de las plantas y UPS. | Recursos Físicos |
| 11 | · Contar con equipo contra incendios cerca de las plantas eléctricas. | Recursos Físicos |

| | | |
|---|---|---|
| 12 | · Contar con el mapa eléctrico de las áreas donde están ubicadas las plantas y UPS y que cuenten con conexiones a tierra, físicas e independientes a la de los servicios de telecomunicaciones. | Recursos Físicos |
| 13 | · Contar con UPS con capacidades necesarias en todos los cuartos de comunicaciones y Centros de Datos de las diferentes sedes. | Recursos Físicos |
| 14 | · Realizar periódicamente mantenimientos preventivos a las UPS, para su óptimo funcionamiento. | Recursos Físicos |
| 15 | · Determinar semestralmente el tiempo efectivo y real de respaldo de la UPS, con respecto a las diferentes cargas. | Recursos Físicos |
| 16 | · Contar con los respectivos procedimientos, para reportar los incidentes a las áreas y dependencias involucradas, al igual que a los usuarios afectados. | SIGUD |
| 17 | · Contar con un plan de ejecución de respaldos de emergencia a la información de configuraciones, bases de datos, aplicaciones y sistemas de información, junto a los demás servicios de TI existentes. | UDNET |

## 5. CONSIDERACIONES DURANTE LA CONTINGENCIA

Cualquier incidente, evento especial o desastre que ocurre, tiene la capacidad de interrumpir una o varias actividades del proceso normal de la Institución. Es por esta razón que se debe ejecutar un plan para responder en el menor tiempo posible y así impactar en un porcentaje muy bajo las actividades de TIC que intervienen en el evento.

Para ello es necesario:

- Establecer e informar a la comunidad afectada sobre el 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 los procedimientos específicos a cada situación, para aplicarlos al momento de la eventualidad.
- En caso de que se involucren sistemas eléctricos:

- Comunicarse con la División de Recursos Físicos para la supervisión de las plantas eléctricas y realizar las comunicaciones, de ser necesarias, con la entidad encargada del suministro eléctrico en la sede afectada.

- Monitorear las UPS cada 10 minutos para activar y realizar las acciones correspondientes.

- En caso de se necesite por más tiempo de recuperación y por lo tanto, actividad en las UPS, apagar los equipos no prioritarios o que no demanden uso mientras se resuelve la contingencia.

- En caso de una catástrofe natural o pública, se debe seguir el plan de contingencia general de la Universidad / Distrital y contactar a las autoridades locales, regionales o nacionales a las que haya lugar, para la inmediata reacción y recuperación.

- En caso de ser necesario, desactivar o desconectar equipos o servicios, para evitar daños o pérdida de información.

- Buscar asegurar la capacidad de las comunicaciones internas y externas.

- Asegurar los *backups* de los sistemas que atienden servicios críticos, para la posterior recuperación de los mismos.

## 6. CONSIDERACIONES DESPUÉS DE LA CONTINGENCIA

- Restablecer el funcionamiento de los equipos y servicios críticos.

- Restablecer el funcionamiento de los equipos y servicios que se inactivaron preventivamente, de manera paulatina, supervisada y controlada siguiendo el orden de importancia.

- Validar el correcto funcionamiento de los servicios y equipos afectados.

- Evaluar el impacto y nivel daño e identificar la cobertura y el costo del impacto.

- Restablecer los *backups* en caso de ser necesario.

- Cambiar la parte del equipo o del componente afectado o pedir garantía inmediata.

- Actualizar el mapa de riesgos, de ser necesario.

- Notificar a los usuarios afectados sobre el restablecimiento de los servicios y la condición en que quedaron.

- Diligenciar el formato de registro de incidentes, en el cual se anotará lo sucedido, la manera en la que se resolvió el incidente y los tiempos de respuesta aplicados.

## 7. MATRIZ DOFA

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

| DEBILIDADES | FORTALEZAS |
|---|---|
| ➢ Resistencia al cambio por parte de todos los estamentos universitarios.<br>➢ Deficiencia de personal para realizar las tareas y los proyectos del proceso a tiempo.<br>➢ Huelgas, protestas, toma de instalaciones que hacen que retrasen o interrumpan los servicios<br>➢ 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.<br>➢ Limitados recursos económicos para mejorar la red institucional<br>➢ Limitados recursos económicos para la puesta en marcha de una red de alta velocidad que soporte la interconexión interna y externa.<br>➢ 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.<br>➢ Limitada infraestructura física y lógica en cuanto a equipos de cómputo, plataforma tecnológica y desarrollo de software.<br>➢ Desconocimiento parcial de los recursos existentes en telecomunicaciones y tecnologías de la información.<br>➢ Se han desarrollado al interior de la universidad aplicaciones y/o sistemas de información de manera parcializada algunas sin una dirección central.<br>➢ Falta de comunicación interna ya que las áreas no conocen las funciones y resultados de las demás. | ➢ Contar con una red adecuada para la interconexión que soporta los diferentes procesos académicos y administrativos.<br>➢ Existen planes de adquisición de Tecnología a corto y mediano plazo.<br>➢ Existe recurso humano Académico y Administrativo, capaz de aportar conocimiento y experiencias Informáticas.<br>➢ Existe una infraestructura de RED aprovechable en la Universidad<br>➢ Se cuenta con infraestructura de hardware y software para cubrir las necesidades del cliente.<br>➢ Se cuenta con personal capacitado en áreas técnicas.<br>➢ Se cuenta con desarrollos propios que se convierten en servicios que solventan las necesidades del cliente.<br>➢ Desarrollo de la educación virtual como apoyo a procesos académicos y administrativos<br>➢ Modelo de Gestión por procesos |

| | |
|---|---|
| ➢ Falta de cultura organizacional y un sistema de calidad que permita el flujo de información adecuada entre las áreas de la universidad. | |
| **OPORTUNIDADES** | **AMENAZAS** |
| ➢ Asignación de dineros por parte de la estampilla y otras fuentes<br>➢ Implementar y mejorar la infraestructura física, tecnológica, y de conectividad, para garantizar el desarrollo de las funciones misionales de la universidad, la comunicación y el bienestar institucional.<br>➢ Apoyo en el desarrollo de nuevas formas de aprendizaje y apropiación del conocimiento generado por el avance vertiginoso de las tecnologías de la información y las comunicaciones.<br>➢ Aplicación de tecnologías de la información y la comunicación para incrementar los aprendizajes y la interacción de la comunidad.<br>➢ Creciente dotación y actualización de infraestructura física y lógica.<br>➢ Vinculación de manera permanente a la institución, de personal técnico calificado.<br>➢ Implementar convenios interuniversitarios que permitan el intercambio de conocimientos. | ➢ Ampliación de cobertura sin el correspondiente crecimiento en recursos humanos, físicos y tecnológicos.<br>➢ Saturación de la red.<br>➢ Alta rotación de personal técnico<br>➢ Cambios tecnológicos acelerados.<br>➢ No contar con fuentes de financiación de manera permanente y constante |

## 8. 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<br>* Falta de capacitación al usuario final<br>* Mal uso de los teléfonos | * Inestabilidad en la continuidad de los servicios<br>* Incomunicación total o con dificultades<br>* Pérdida de tiempo al realizar el desplazamiento hasta el sitio para su reparación | **BAJA** | **ALTO** | **MODERADO** | * Manuales para los usuarios finales<br>* 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.<br>* daño en la configuración de los equipos<br>* Retardo entre enlaces | * Deficiencia en el servicio | **BAJA** | **ALTO** | **MODERADO** | * Aumento de ancho de banda<br>* Calidad de servicio en teléfonos y en regiones<br>* Optimización de ancho de banda (compresión de voz) |

| IDENTIFICACION DEL RIESGO | | | ANALISIS DEL RIESGO | | | MANEJO DEL RIESGO |
|---|---|---|---|---|---|---|
| **RIESGO** | **CAUSAS** | **CONSECUENCIA** | **PROBABILIDAD** | **IMPCTO** | **ZONA DE RIESGO** | **ACCIONES /CONTROLES** |
| Errores de configuración el los aparatos telefónicos | * Falta de capacitación<br>* Falta de conocimiento en el procedimiento de instalación y configuración del aparato telefónico<br>* Errores en el administrador | * Deficiencia en el servicio<br>* 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<br>* Usuarios malintencionados | * Interceptación de la información | **BAJA** | **MEDIO** | **TOLERABLE** | * Cambio de código de servicios especiales según su uso<br>* Cambio de código por cambio de usuario |
| Errores del administrador | * Personal inadecuado para la labor que desempeña<br>* Falta de capacitación | * Deficiencia en el servicio<br>* Daño en el software<br>* Daño en la configuración de los aparatos telefónicos<br>* 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<br>* Terminación de vida útil<br>* Falta de mantenimientos<br>* Condiciones ambientales inapropiadas | * Caída de la red que atiende el equipo dañado | **MEDIA** | **ALTO** | **IMPORTANTE** | * Instalación de UPS<br>* Mantenimientos programados<br>* Seguimiento de las fechas de vida útil de los equipos. EOS (end of sale), EOL (end of life time)<br>* Adecuación de cuartos de telecomunicaciones TR (telecommunication room) |
| Pérdida de la configuración de los equipos | * Fallas de hardware en la memoria no volátil NVRAM<br>* Reinicio inesperado del sistema<br>* 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<br>* Realización de backup de los equipos más importantes |
| Fallas en la certificación del cableado | * EMI y RFI (interferencia electromagnética e interferencia por radiofrecuencia)<br>* Mala instalación de cableado (ponchado, cable maltratado) | * Mal desempeño de los puntos cableados<br>* Existe conectividad limitada o nula | **BAJA** | **MEDIO** | **TOLERABLE** | * entrenamiento en los procesos del cableado<br>* 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 ISP | * Sedes sin servicio de red | **BAJA** | **ALTO** | **MODERADO** | Exigencia de niveles de servicios ANS comunicación Help Desk con el proveedor |
| Problemas con el direccionamiento IP | * Instalación no autorizada de equipos que entregan direcciones IP<br>* 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<br>* configuración segura de puntos de red y puertos. |
| Ataque a los equipos de red | * Equipos de telecomunicaciones desactualizados en hardware y/o software<br>* 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<br>* Reemplazo de los equipos cuyo tiempo de vida ya caduco<br>*monitoreo |
| Daño en los servidores | * Falta de mantenimiento de los servidores<br>* Instalaciones físicas inadecuadas<br>* Condiciones ambientales inapropiadas | * Interrupción de los servicios que el servidor soporta | **BAJA** | **ALTO** | **MODERADO** | * Mantenimientos programados<br>* Adecuación del espacio físico con estándares internacionales |

| IDENTIFICACION DEL RIESGO | | | ANALISIS DEL RIESGO | | | MANEJO DEL RIESGO |
|---|---|---|---|---|---|---|
| **RIESGO** | **CAUSAS** | **CONSECUENCIA** | **PROBABILIDAD** | **IMPCTO** | **ZONA DE RIESGO** | **ACCIONES /CONTROLES** |
| Pérdida de la información del sistema de almacenamiento masivo | * no aplicar procedimiento adecuado para apagado del sistema de almacenamiento masivo<br>* Fallas eléctricas<br>* Daño en disco | * Pérdida de información | **BAJA** | **ALTO** | **MODERADO** | * Mantenimientos preventivos<br>* Garantía de los discos<br>* Backups en medio magnético<br>* manteniiento sistema eléctrico por parte de Rfisicos |
| Daños de sistemas operativos en los servidores | * Mala administración<br>* Daños en disco<br>* Ejecución errónea del mantenimiento | * Interrupción de los servicios que el servidor soporta | **BAJA** | **ALTO** | **MODERADO** | * Actualizaciones – update, upgrade -<br>*Revisión de logs<br>* Supervisión de mantenimientos<br>*monitoreo de desempeño |
| Demora en los procesos de contratación de aspectos técnicos. | * Demora en los procesos administrativos de contratación<br>* Respuesta baja y lenta de proveedores<br>* Cambio tecnológico acelerado | * Atraso en la contratación de recursos tanto humano como tecnológico provocando un retraso y fallas en las actividades de la red | **BAJA** | **ALTO** | **MODERADO** | Reiteración en el cumplimiento de acciones a los actores involucrados: oficinas de la Universidad y proveedores |
| Pérdida de contraseñas de administrador | * Robo de contraseñas<br>* Olvido de las contraseñas<br>* Las contraseñas no se encuentran debidamente resguardadas<br>* El administrador se retira y no deja las contraseñas | * Tomar posesión de los servidores sin autorización<br>* Pérdida de información<br>* Cambio o pérdida de la configuración de los servicios<br>*sin acceso a la administración del equipo involucrado | **BAJA** | **ALTO** | **MODERADO** | * Actualización anual o por inicio de nuevo contrato de sobres cerrados de Contraseñas.<br>* Las contraseñas deben tener una combinación alfanumérica |
| Ataques a los servidores por medio de software malicioso | * No tenga instalado la licencia de antivirus<br>* No se encuentre debidamente configurado el antivirus<br>* No se encuentre actualizado el antivirus | * Daño en los archivos de configuración del servidor que podría ocasionar fallas en el servicio que se preste<br>* Perdida de información<br>* Daño en el sistema operativo | **MEDIA** | **ALTO** | **IMPORTANTE** | * Licenciamiento de antivirus<br>* Backups a la información de los servidores<br>* monitoreo |
| Vulnerabilidades o huecos de seguridad en software | *No contar con actualizaciones, y parches de software, puertos mal administrados, no disponer de firewall adecuado. | * Pérdida de información<br>* Apoderamiento de la máquina por personal no autorizado<br>* Robo de información<br>* Servicios no disponibles | **BAJA** | **ALTO** | **MODERADO** | * Actualizaciones permanentes de los servicios y sistema operativo<br>* Monitoreo |
| Se acabe el espacio en el disco de los servidores | * No se tenga planeado el crecimiento de la información<br>* Virus<br>* Falta de revisión log | No se puede prestar los servicios que soporta el servidor | **MEDIA** | **ALTO** | **IMPORTANTE** | * Revisión de logs periódicamente<br>* Liberación constante de archivos innecesarios<br>*monitoreo |
| Falta de acceso físico a estación de trabajo | * Toma o cierre forzoso de sedes de la Universidad | * Los usuarios finales no podrán ingresar a sus equipos de trabajo | **MEDIA** | **ALTO** | **IMPORTANTE** | * Identificación de equipos atendidos generando listado de equipos, MAC, nombre de usuarios, funciones de equipo.<br>* Configurar encendido de equipo “wake up on lan”<br>* Configuración de escritorio remoto según se requiera<br>* Configuración acceso externo a la Universidad si se requiere. VPN |

| IDENTIFICACION DEL RIESGO | | | ANALISIS DEL RIESGO | | | MANEJO DEL RIESGO |
|---|---|---|---|---|---|---|
| RIESGO | CAUSAS | CONSECUENCIA | PROBABILIDAD | IMPCTO | ZONA DE RIESGO | ACCIONES /CONTROLES |
| | | | | | | * Virtualización escritorios y aplicaciones requeridos.<br>* Habilitación de administración remota de infraestructura de TI |
| Publicar en web información desactualizada y/o errada. | * No se tienen identificadas o no existen las fuentes de información.<br>* El usuario que publica NO tiene la experticia y conocimiento para hacerlo.<br>* No existe la política institucional de comunicaciones.<br>* El usuario desconoce o no aplica la resolución 711 de 2008 para publicación Web<br>* Descuido del usuario, Errores en la digitalización.<br>* alta rotación del Recurso humano por tipo de vinculación (CPS)<br>* Las oficinas no verifican la veracidad y la pertinencia de la información publicada | * Generar confusión en la comunidad.<br>* Problemas jurídicos y legales.<br>* Problema de transparencia institucional<br>* Mala imagen institucional | MEDIA | MEDIO | MODERADO | * Adelantar capacitaciones a responsables de publicación en web de las dependencias.<br>* entregar al líder de comunicaciones institucionales el perfil y clave de autorización de publicación.<br><br>*Adelantar elaboración de políticas publicación web.<br>* hacer revisiones y comunicaciones con las dependencias que tienen página |
| Publicar información malintencionada o falsa | * Acceso no autorizado. (hacer daños por medio de terceros)<br>* Usuario autorizado publica información no institucional, o con fines personales<br>* No se revisa la información a la hora de la activación o la publicación.<br>* Sufrir un ataque al sitio que modifique la información publicada<br>* el usuario publicador no verifica la veracidad de la información<br>*el usuario publica información si solicitar autorización a su jefe directo. | * Daño a la imagen institucional<br>* Generar confusión<br>* Perjudicar el buen nombre de las instituciones y/o personas<br>* filtración de información<br>* Inconsistencia en la información<br>* Problemas legales | BAJA | ALTO | MODERADO | * Realizar capacitaciones<br>* hacer campañas de responsabilidad en la publicación de información<br>* Revisión periódica de información publicada |
| Problemas legales | * Utilizar software sin licenciamiento<br>* No respetar las normas y leyes de derechos de autor<br>* Problemas de cultura | *violación a derechos de autor<br>* sanciones al representante legal y los responsables como: Cárcel, Multas.<br>* Desprestigio para la institución | MEDIA | ALTO | IMPORTANTE | * Instalación de software debidamente licenciado.<br>* Política de administración y uso de equipo de usuario final |
| No se puede acceder a la información publicada | * Errores en los formatos de la presentación de la información<br>* Errores técnicos que hacen que los servicios fallen<br>* El usuario no tiene las herramientas para ver la información<br>* Manejo de software incompatible<br>* Incompatibilidad de versiones | * Generar confusión<br>* Problemas legales<br>* Demora en los procesos | BAJA | MEDIO | TOLERABLE | * Capacitación al usuario<br>* instructivo para acceso<br>* Revisiones y pruebas de versión a los documentos a publicar |

| IDENTIFICACION DEL RIESGO | | | ANALISIS DEL RIESGO | | | MANEJO DEL RIESGO |
|---|---|---|---|---|---|---|
| **RIESGO** | **CAUSAS** | **CONSECUENCIA** | **PROBABILIDAD** | **IMPCTO** | **ZONA DE RIESGO** | **ACCIONES /CONTROLES** |
| Demora en la publicación de la información | * Demora en el proceso de revisión y activación<br>* Demora en el envío de las correcciones | * Venzan términos | **BAJA** | **BAJO** | **ACEPTABLE** | * Establecer un protocolo para la revisión y activación de información.<br>* Capacitar a las personas que publican información |
| No se articule o active el mecanismo para recibir retroalimentación | * Problema de planeación<br>* Problemas técnicos<br>* No se habiliten los canales de comunicación y retroalimentación<br>* No se informa de la habilitación<br>* Problema cultural | * No exista la retroalimentación de la información publicada<br>* Comunicación errónea | **BAJA** | **BAJO** | **ACEPTABLE** | * Definir claramente los mecanismos de retroalimentación y determinar si hay viabilidad técnica<br>* Hacer pruebas o simulacros<br>* Hacer capacitaciones<br>* Realizar instructivos de uso de los servicios |
| Mal funcionamiento de un aplicativo | * Deficiencias en el mantenimiento<br>* Mal diagnóstico a la detención de la falla<br>* Implementación de una solución no adecuada<br>* Uso de actualizaciones y parches de seguridad que producen mal funcionamiento | * No se puede hacer uso correcto del servicio<br>* 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<br>*Uso de estándares y procedimiento de detección de fallas<br>* Hacer iteraciones para corregir las publicaciones |
| Daños en hardware, software o medios | * Fallas en el funcionamiento* Inadecuada manipulación de equipos y medios<br>* Almacenamiento inadecuado de medios<br>* Virus en el sistema | * Caída total o parcial del servicio* Problemas de actualización del sitio | **BAJA** | **ALTO** | **MODERADO** | * Redundancia de equipos críticos<br>* Cultura en el manejo y almacenamiento de los equipos y medios<br>* Mantenimiento preventivo y correctivo<br>* Manejo de vida útil |
| Pérdida de la información | * Problema de cultura<br>* Falta de capacitación<br>* Inadecuada o inexistencia realización de copias de seguridad<br>* Ataque informático a los sistemas<br>* Ataques de virus informáticos<br>* Inadecuado manejo de la información y las herramientas de la información<br>* Robo o pérdida de dispositivos de almacenamiento con información | * Demora en los procesos<br>* Uso indebido de la información<br>* Problemas legales | **MEDIA** | **ALTO** | **IMPORTANTE** | * Cultura en el manejo y almacenamiento de los equipos y medios<br>* Concientización al usuario sobre la clasificación y el manejo de la información<br>* Definición de roles de usuario de acuerdo a la forma de acceder y hacer uso de la información<br>* Implementación de políticas de copias de seguridad<br>* Implementación de políticas de digitalización de la información |

| IDENTIFICACION DEL RIESGO | | | ANALISIS DEL RIESGO | | | MANEJO DEL RIESGO |
|---|---|---|---|---|---|---|
| **RIESGO** | **CAUSAS** | **CONSECUENCIA** | **PROBABILIDAD** | **IMPCTO** | **ZONA DE RIESGO** | **ACCIONES /CONTROLES** |
| Publicación de información no autorizada | * Falta de responsabilidad y prudencia en el uso de la información<br>* Error humano<br>* Error en la verificación de la información<br>* Publicación de información sin autorización del jefe directo | * Robo<br>* Problemas legales<br>* Vulneración de derechos fundamentales | **BAJA** | **ALTO** | **MODERADO** | * Políticas claras de publicación de la información<br>* Sensibilizar al usuario sobre la clasificación de la información<br>* Definición de roles de usuario de acuerdo a la forma de acceder y hacer uso de la información<br>* Cumplimiento de normatividad vigente |

**Trabajo remoto al puesto de trabajo original**

- Asegurar los backups de los servidores críticos en caso de ser necesario.
- 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 oficina, previa asignación de nuevo puesto de trabajo.

El usuario final deberá:

- Utilizar equipo diferente al asignado para su trabajo cotidiano, si es necesario.
- Contar con usuario y contraseña para conexión VPN, para acceso externo a la red de la Universidad.
- Contar con escritorio virtual.

## 9. GLOSARIO

- Red: Conexión de varios computadores mediante elementos que facilitan su comunicación.
- Incidente: Es un evento sobre un recurso tecnológico o servicio que impide al usuario su normal y continua labor**.**
- Backup: Copia de seguridad o respaldo.
- TIC: Tecnología de la Información y de las Comunicaciones.
- VPN: Virtual Private Network. Es una red de telecomunicaciones privada, establecida entre sujetos que utilizan, como tecnología de transporte, un protocolo de transmisión público y compartido, como Internet.

- Log: se refiere a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular (aplicación, actividad de una red informática, etc.).
- UPS: (Uninterruptible Power Supply) Sistemas de alimentación ininterrumpida, dispositivo que, gracias a sus baterías u otros elementos almacenadores de energía, durante un apagón eléctrico puede proporcionar energía eléctrica por un tiempo limitado a todos los dispositivos que tenga conectados.

## 10.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 telecomunicaciones: Redes y conectividad, 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.