|  |
| --- |
| OBJETIVO |

Suministrar e identificar políticas y procedimientos que realicen los usuarios, funcionarios, trabajadores, contratistas y/o proveedores para continuar las operaciones en el caso de incidentes no que afecten la disponibilidad, la confiabilidad e integridad de los recursos informáticos tales como equipos, software y redes de datos de la. Este documento las funciones y responsabilidades de los usuarios y asigna autoridad a los responsables de la seguridad informática en la Universidad.

|  |
| --- |
| ALCANCE |

Recursos, servicios tecnológicos y de comunicaciones en las sedes de la Universidad

|  |
| --- |
| RESPONSABILIDAD |

* 1. **JEFE OFICINA DE INFORMATICA.**

Es el responsable de que este instructivo se cumpla y de asegurar el entrenamiento del personal para el conocimiento y aplicabilidad del mismo.

* 1. **JEFES DE LAS DEPENDENCIAS**

Son los responsables de los activos de información en las dependencias y de velar que su personal ejecute y cumpla las políticas de este Plan de Contingencia en acompañamiento con la Oficina de Informática

|  |
| --- |
| GLOSARIO |

Para facilitar la comprensión del presente documento, se definen los siguientes términos.

**Hardware**. El hardware está formado por los componentes físicos. Es la parte "dura", es decir, las partes que configuran la máquina y que le dan una serie de características.

**Software**. El software está compuesto por los programas que dirigen el funcionamiento de un ordenador. Es la "parte lógica" de la máquina que permite enlazar todos los elementos de [hardware](http://www.ciudadfutura.com/mundopc/glosario/h/hardware.htm) de la manera más efectiva posible, permitiéndole realizar cualquier tipo de trabajo

**Comunicación**: Es cuando se transmite información desde un equipo a cualquier otro. Para que se pueda realizar una transmisión de información, son necesarios tres elementos: El emisor, quien origina la información; el medio de transmisión: que permite la transmisión de esa información; el receptor: quien recibe la información.

**Servicio**: Son programas que están disponibles en los servidores y que son utilizados por los usuarios de la red bajo una solicitud.

**Correo electrónico** También conocido como “E-mail”. Es una software que puede utilizarse para el envío y recepción de mensajería entre usuarios, entendiendo por mensajería cualquier texto, archivo, programa, etc.

**Virus**: Son pequeños programas de computadora cuya principal cualidad es la de poder auto replicarse, está escrito intencionalmente para instalarse en la computadora de un usuario sin el conocimiento o el permiso de este para producir efectos dañinos.

**LAN** (Local Area Network) : Se refiere a redes de computadoras que no traspasan de un ámbito delimitado por un área física determinada, como por ejemplo un edificio, una compañía, etc.

**Red de computadoras**: A nivel más elemental una red no es más que un conjunto de maquinas (computadoras, impresoras y otros recursos), un medio compartido (tal como un cable con el que se interconectan todas las computadoras y las impresoras), junto con una serie de reglas (protocolo) que rigen el acceso a dicho medio.

**WAN** (Redes de Area Extensa). Al ampliarse el alcance de las LAN, traspasando las fronteras que delimitan su espacio físico, se convierten en una rede de área extensa (WAN). Generalmente se denomina WAN a un conjunto de redes LAN; situadas en espacios físicos distantes, que se interconectan entre si mediante medios de transmisión de datos (enlaces de radio, fibra óptica, microondas, cable, MODEM, etc.).

**Usuarios**: Se refiere a todos los empleados, contratistas, consultores, trabajadores temporales, y cualquier otra persona o entidad que por razón de su trabajo se le permita acceso, se le asignen derechos de uso y utilicen los recursos que componen los medios electrónicos de almacenamiento y transmisión de datos de la universidad del Atlántico

Igualmente se clasifica como usuario a cualquier empleado, contratista, consultor, o trabajador temporal de compañías asociadas a la universidad del Atlántico, a quienes se les preste cualquier tipo de servicio que implique la utilización de los medios electrónicos de transmisión de datos de la universidad del Atlántico.

**Red Internet**:: Conjunto de computadoras y entidades alrededor del mundo, interconectadas entre si, con el propósito de intercambiar correo e información de carácter general.

**Backup:** Son copias de respaldo o de seguridad del sistema o de los datos, que puede ser utilizada en caso de producirse un fallo generalizado, caída del sistema, o el daño o eliminación accidental de archivos. Gracias a la información contenida en el backup, podremos restaurarlo al estado en que se encontraba en el momento de realizar esta copia de seguridad.

**Comprimir:** Proceso que compacta archivos para guardarlos en una unidad de almacenamiento limitada. Al comprimir un archivo con un programa de compresión de archivos como PowerArchiver, Winzip o Winace, se crea un archivo que contiene toda la información del original, pero en un tamaño más reducido.

**Descomprimir**.: Proceso inverso a la compresión, en la que en un archivo comprimido se restablece toda la información de la misma forma y tamaño original.

|  |
| --- |
| POLITICAS Y CONDICIONES DE OPERACIÓN |

Para la Oficina de Informática de la universidad del Atlántico el buen manejo de los recursos informáticos es uno de las grandes metas que se espera alcanzar a corto/mediano plazo para contar con sistemas de red más eficientes y estables. En este sentido, la oficina de informática ha notado la necesidad de políticas para controlar los tres siguientes elementos:

* **Ancho de Banda y Disponibilidad de Espacio en Servidor**

Ha sido claramente comprobado que archivos de música MP3, archivos de video y otras descargas similares pueden saturar el ancho de banda y reducir considerablemente el espacio disponible en disco. Estas descargas de archivos, si no se monitorean debidamente, pueden reducir considerablemente las velocidades de acceso a las redes de la universidad entera afectando negativamente la productividad y los tiempos de respuesta de las aplicaciones.

* **Amenazas a la seguridad de la información y los datos**

La navegación y descarga de archivos expone a la organización al contagio y la proliferación de virus informáticos que pueden llegar a tener consecuencias devastadoras en un ambiente laboral.

Una forma muy efectiva de conseguir seguridad en una red es mediante la instalación de poderosos sistemas de Firewall que refuerzan la seguridad lógica. Otro método es educar a los usuarios sobre el peligro de descargar archivos adjuntos y otra información desconocida a sus equipos de trabajo.

* **Comportamiento inescrupuloso y uso indiscriminado de los recursos**

Igualmente, el uso no controlado de los recursos informáticos incentiva las acciones inescrupulosas al no existir ningún tipo de control o reglamentación que determine lo aceptable y lo no aceptable en una organización.

Cualquier empresa que tenga un grupo de empleados utilizando computadores conectados a la red enfrenta el dilema de educar usuarios para reducir el uso del Internet y las redes para fines personales y familiares y crear conciencia de la responsabilidad que cada individuo posee para con la organización.

Independientemente del entorno organizacional en que se opere, es recomendable emplear un enfoque formal y por escrito en el que cada empleado tenga la oportunidad de familiarizarse con las normas y las acciones permisibles de acceso al ciberespacio. Esto es indispensable también para reducir riesgos de responsabilidades adquiridas por terceros y protege en un momento dado la propiedad intelectual de la organización y la privacidad de la información privilegiada

Un desastre puede definirse como la interrupción prolongada de los recursos informáticos y/o de comunicación que limiten a los usuarios del sistema acceder a la información que les interesa.

Una interrupción del flujo de información puede ser activada por las siguientes causas:

* Fuego
* Explosión
* Inundación
* Tormenta de alta intensidad
* Gases o material peligroso
* Robo
* Interrupción del fluido eléctrico
* Fallas en la comunicación
* Huelgas
* Rotura de conductos de agua
* Hacker, virus, spam, etc.

**5.2 CONDICIONES PREVIAS QUE SE HAN DE CUMPLIR PARA DESARROLLAR EL PLAN DE CONTINGENCIA**

1. Generar una descripción de todos los usuarios del sistema
2. Generar una nómina del personal considerado clave dentro de las operaciones del sistema informático con los datos mínimos siguientes: Nombre, Dirección de vivienda, Teléfonos, usuario de acceso y claves. Esta información deberá ser de extrema confidencialidad.
3. Cada usuario del Sistema Informático que labore en la Oficina de Informática tendrá asignada una cuenta de controlador de dominio de acceso en forma individual e intransferible, quien responderá personalmente por el uso que se le dé a la misma
4. La Oficina de Informática, a través de la persona que ocupa el puesto de Administradores de Base de datos, serán responsables de la generación y custodio del backups de los sistemas de las bases de datos que administra
5. Se deberá establecer una coordinación con documento escrito, entre el Administrador de Base de Datos de la Universidad del Atlántico y la entidad que provea el servicio de custodia y resguardo del contenido del backup en forma bilateral u otro medio de resguardo de la información.
6. No se entregará ningún backup a persona que no esté debidamente identificada como personal con autorización para tal efecto. Estas autorizaciones deberán definirse en la Dirección de Informática y el Proveedor de almacenamiento de los backups con el conocimiento de la Rectoría de la Universidad del Atlántico
7. Se buscará constantemente los mejores mecanismos para optimizar las operaciones de backups, resguardo y restauración cuando sea necesario
8. Es recomendable efectuar una simulación de un desastre por lo menos una vez al año, para capacitar al personal y mantener una actitud vigilante de los procedimientos diseñados para el efecto
9. La descripción y los programas fuentes de las aplicaciones que se vayan realizando también deberán agregarse a los backups.
10. Los diagramas de la red eléctrica, de ubicación de equipo, inventario de hardware y software, etc. Deberá incluirse en el backup’s
11. Una vez identificada la ocurrencia de un evento de ésta naturaleza, la persona que lo detecte debe reportar a su jefe inmediato superior quien lo hará del conocimiento de la Dirección de Informática quien a su vez deberá garantizar de que esté informada la Rectoría de la Universidad del Atlántico. Esta comunicación deberá hacerse a través de los canales informales y formales

|  |
| --- |
| DESCRIPCIÓN DE ACTIVIDADES |

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Descripción** | **Responsables** | **Documento/   Registros** |
|  | **PLAN DE CONTINGENCIA**   1. Almacenar la descripción de todos los usuarios del sistema informático que trabajan directamente en la Oficina de Informática, en el área de resguardo existente fuera de las instalaciones de la Oficina. 2. Almacenar la Nómina del Personal Clave (NPC), para poner en marcha un plan de restauración de las operaciones informáticas, fuera de las instalaciones que ocupa la Oficina de Informática 3. Generar un backup de las diferentes aplicaciones existentes en la Oficina de Informática con base a un criterio de periodicidad predefinido de acuerdo al grado de volatilidad de los datos. 4. Almacenar en el área disponible fuera de las instalaciones de la Oficina de Informática, los recursos que puedan atender oportunamente una emergencia, en el caso de hardware tal como discos duros, ventiladores, tarjeta de comunicaciones etc. O software como el caso de licencias de software de sistema operativo, aplicaciones, configuración de servidores etc) . 5. Cada usuario de la red tiene asignado un área de almacenamiento en el servidor de archivos para que deposite la información generada por el proceso de su gestión en la Oficina de Informática y los resultados obtenidos para el logro de los objetivos institucionales, de manera que se garantice su inclusión en el backup generado periódicamente. 6. El administrador de la red, hará entrega de cada backup, al delegado (preestablecido), de la institución responsable de su almacenamiento en un lugar diferente a las instalaciones de la Oficina de Informática, a través de un documento que describa el contenido del backup. 7. Cada backup deberá contar con una etiqueta externa que identifique su contenido y si el mismo es para archivo fijo o reutilizable (backup volátil, aplicando el criterio de abuelo, padre e hijo) 8. Cuando se cambie a las personas encargadas de efectuar los backup, resguardo y/o restauraciones, se deberá notificar a las partes involucradas con la prontitud que sea posible. 9. Se deberá dar la capacitación al personal de la Oficina de Informática, para sensibilizarlo de la importancia de mantener el resguardo de la información para garantizar la continuidad del acceso a la información relevante a cada área funcional de la Institución.   **PLAN DE RESTAURACION DE OPERACIONES**   1. Ante el evento de un incidente, el jefe de Informática, con su equipo de trabajo, hace una evaluación de la interrupción de las operaciones del servicio informático para diagnosticar las características de la situación. 2. En función del resultado del análisis preliminar se contacta y coordina con el personal pertinente, indicado en la Nómina de Personal Clave (NPC) para la atención de desastres informáticos. Así como informa sobre el incidente a sus superiores. Esta comunicación se deberá realizar con la prontitud que el caso amerite y mantener un sistema de información continuo hasta que los efectos del incidente queden restaurados en su totalidad. 3. Obtenido el diagnóstico descrito en párrafo anterior, el jefe de la oficina de Informática conjuntamente con su equipo de trabajo, define la estrategia a seguir para restaurar la continuidad del servicio informático. 4. Si fuera necesario se convocará al personal relacionado con la etapa de recuperación de las condiciones de operatividad de los sistemas informáticos (NPC). 5. Se contactará al servicio de resguardo de información y recursos informáticos previstos para atender un desastre. (Para ello, el jefe de Informática y/o el Administrador de Sistemas contará con los contactos correspondientes) 6. Una vez se restablezca la normalidad de las operaciones, se revisarán las bases de datos, servidores, impresoras, etc (de acuerdo a la cobertura de la incidencia), para cerciorarse de que realmente se a puesto a punto las condiciones tal como se encontraba el sistema antes del desastre. |  | **Registro en el (CAU)** |

|  |
| --- |
| NORMATIVIDAD Y DOCUMENTOS DE REFERENCIA |

NORMA TECNICA ISO 27001:2013

NTGP 1000

MECI 2015

|  |
| --- |
| CONTROL DE CAMBIOS |

|  |  |  |  |
| --- | --- | --- | --- |
| **VER** | **FECHA** | **ELABORÓ** | **DESCRIPCIÓN** |
| 0 | Mayo 2016 | Deyanira Morón | Versión Inicial |