

[POLÍTICA DE SEGURIDAD]

Incorporación de TIC en Procesos Educativos
2013 - 2019



Formamos el Capital Intelectual para la Sociedad del Conocimiento

[Universitaria Virtual Internacional]
[2013]



ALIRIO BARBOSA PEÑA

Presidente Junta Directiva

ÁLVARO CANO AGUILLÓN

Rector

LUIS ALFONSO GONZÁLEZ BERNAL

Director de Planeación y Acreditación

ROBERTO JURADO J.

Vicerrector Académico

ROGER RUÍZ PLAZA

Vicerrector Administrativo

FABIÁN JAIMES LARA

Vicerrector de Investigaciones y Tecnologías

ARIEL LEMUS PORTILLO

Vicerrector de Proyección y Responsabilidad Social

TABLA DE CONTENIDO

1.	INTRODUCCION.....	5
2.	JUSTIFICACION	6
3.	OBJETIVOS.....	6
4.	ALCANCE	7
5.	POLITICAS DE SEGURIDAD	8
5.1.	Responsables	8
5.2.	Ingreso y salida de equipos	9
6.	POLITICAS ADMINISTRATIVAS U ORGANIZACIONALES	9
7.	POLITICAS PARA GESTION DE ACTIVOS.....	10
7.1.	Inventario de activos	10
7.2.	Clasificación de la información	11
7.3.	Rotulado de la Información	13
8.	POLITICAS PARA SEGURIDAD DE LOS RECURSOS HUMANOS.....	13
9.	POLITICAS DE SEGURIDAD FISICA	14
9.1.	Controles de Acceso Físico	15
9.2.	Dispositivos de Seguridad de la Información.....	15
9.3.	Protección de Oficinas, Recintos e Instalaciones	28
9.4.	Ubicación y Protección del Equipamiento y Copias de Seguridad.....	29
9.5.	Mantenimiento de Equipos	29
9.6.	Políticas de Escritorios y Pantallas Limpias.....	30
9.7.	Retiro de los Bienes	31
10.	POLÍTICAS DE GESTIÓN DE LAS TELECOMUNICACIONES Y OPERACIONES	31
10.1.	Documentación de los Procedimientos Operativos	32
10.2.	Procedimientos de Manejo de Incidentes.....	33

11.	POLÍTICAS DE CONTROL DE ACCESO A LOS DATOS	37
11.1.	Reglas de Control de Acceso.....	37
11.2.	Registro de Usuarios.....	38
11.3.	Administración de Privilegios	39
11.4.	Administración de Contraseñas de Usuario	40
11.5.	Responsabilidades del Usuario	41
11.6.	Equipos Desatendidos en Áreas de Clientes.....	42
11.7.	Acceso a Internet.....	43
11.8.	Identificación y Autenticación de los Usuarios.....	43
11.9.	Sistema de Administración de Contraseñas	44
11.10.	Control de Acceso a las Aplicaciones.....	45
12.	POLÍTICAS PARA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE	46
12.1.	Procedimiento de Control de Cambios.....	46
13.	POLÍTICAS PARA GESTIÓN DE INCIDENTES	47
14.	POLÍTICAS PARA LA CONTINUIDAD DE LA OPERACIÓN	48
15.	POLÍTICAS PARA EL CUMPLIMIENTO Y NORMATIVIDAD LEGAL	48

1. INTRODUCCION

El objetivo de la seguridad informática es proteger los recursos informáticos valiosos de la institución, tales como la información, el hardware o el software. A través de la adopción de las medidas adecuadas, la política de seguridad informática ayuda a la organización cumplir sus objetivos, protegiendo sus recursos financieros, sus sistemas, su reputación, su situación legal, y otros bienes tanto tangibles como inmateriales. Debe verse a la seguridad informática, no como un objetivo en sí mismo, sino como un medio de apoyo a la consecución de los objetivos de la institución.

La política de seguridad informática es una invitación a cada uno de los miembros de la institución a reconocer la información entre otras como uno de los activos principales. Esta política debe concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la institución.

Este documento recoge las políticas y procedimientos relacionadas con la infraestructura tecnológica de Universitaria Virtual Internacional en cuanto a los lineamientos referentes a temas como manejo de correo electrónico, estudio y manejo de nuevas adquisiciones, responsabilidades administrativas, integración con diferentes áreas de la organización, lineamientos sobre gestión de incidencias y revisión de aspectos relevantes frente a mecanismos preventivos y correctivos, todo bajo los conceptos de seguridad informática.

Desarrollar una política de seguridad informática significa planear, organizar, dirigir y controlar las actividades tecnológicas para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de la institución.

2. JUSTIFICACION

La seguridad informática aplica técnicas fundamentadas para preservar la información y los diferentes recursos informáticos con que cuenta la Universitaria Virtual Internacional. La política de seguridad informática es el conjunto de normas, reglas, procedimientos y prácticas que regulan la protección de la información contra la pérdida de forma accidental como intencionada, al igual que garantizan la conservación y buen uso de los recursos informáticos con que cuenta la Universitaria Virtual Internacional.

3. OBJETIVOS

Establecer la política institucional en materia de Seguridad Informática que apoye la Seguridad de la Información, entendida como la preservación de la integridad, confidencialidad y disponibilidad, así como instrumentar y coordinar acciones para minimizar daños a la infraestructura tecnológica y a los sistemas informáticos. El objetivo principal de la Seguridad Informática será proteger desde el ámbito tecnológico la información electrónica institucional, los recursos informáticos y los servicios tecnológicos necesarios para que la Universitaria Virtual Internacional pueda cumplir con su misión.

Los objetivos que se desean alcanzar luego de implantar esta política son los siguientes:

- Establecer un esquema de seguridad con perfecta claridad y transparencia bajo la responsabilidad en la administración del riesgo.
- Comprometer a todo el personal de la Universitaria Virtual Internacional con los procesos de seguridad informática, agilizando la aplicación de los controles con dinamismo y armonía.
- Que la prestación del servicio de seguridad gane en calidad.
- Convertir a todo el personal de la Universitaria Virtual Internacional en interventores y facilitadores de los procesos de seguridad informática.

4. ALCANCE

Se definen políticas y lineamientos con el propósito de cumplir con los objetivos de la institución en seguridad informática; y para ello se establecen:

- **Políticas de seguridad:** Para definir controles que proporcionan directivas y consejos de gestión para mejorar la seguridad de los activos de información.
- **Políticas Administrativas u Organizarles:** Que define controles para facilitar la gestión de la información en la Universitaria Virtual Internacional.
- **Políticas para Gestión de Activos:** Que establece controles para catalogar los activos y protegerlos eficazmente.
- **Políticas Para Seguridad de los Recursos Humanos:** Que permite establecer controles para reducir los riesgos de error humano, robo, fraude y utilización abusiva de los equipamientos.
- **Políticas de Seguridad Física.** Establece controles para impedir la violación, deterioro y la perturbación de las instalaciones y datos.
- **Políticas de Gestión de las Telecomunicaciones y Operaciones:** Define controles para garantizar un funcionamiento seguro y adecuado de los dispositivos de tratamiento de la información.
- **Políticas de Control de Acceso a los Datos:** Identificar medios para impedir accesos no autorizados y registro de los accesos efectuados.
- **Políticas para Adquisición, Desarrollo y Mantenimiento de Software:** Controles para establecer racionalización de gastos, aspectos a tener en cuenta al momento de adquisiciones y establecimiento de estándares.
- **Políticas para Gestión de Incidentes:** Clasificación de los incidentes según el grado en que afecten el normal funcionamiento del negocio. Controles para gestionar las incidencias que afectan a la seguridad de la Información.
- **Políticas para la Continuidad de la Operación:** Controles para reducir los efectos de las interrupciones de actividad y proteger los procesos esenciales de la Universitaria Virtual Internacional contra averías y siniestros mayores.
- **Políticas para el Cumplimiento y Normatividad Legal:** Controles para prevenir los incumplimientos de las leyes penales o civiles, de las obligaciones reglamentarias o contractuales

5. POLITICAS DE SEGURIDAD

Controles para proporcionar directivas y consejos de gestión para mejorar la seguridad de los activos de información, para lo cual se debe disponer de los recursos necesarios para garantizar el correcto desarrollo de los lineamientos planteados en cada política propuesta.

5.1. Responsables

- El **Responsable de Seguridad Informática** cumplirá funciones relativas a la seguridad de los sistemas de información, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente política.
- Los **Propietarios de la Información** son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.
- El **Responsable del Área de Recursos Humanos** o quién desempeñe esas funciones, cumplirá la función de notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la política de seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Asimismo, tendrá a su cargo la notificación de la presente política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los compromisos de confidencialidad (entre otros) y las tareas de capacitación continua en materia de seguridad.
- El **Responsable del Área Informática** cumplirá la función de cubrir los requerimientos tecnológicos establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Institución. Por otra parte tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

- El **Responsable del Área Legal** verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la institución con sus empleados y con terceros. Asimismo, asesorará en materia legal a la Institución, en lo que se refiere a la seguridad de la información.
- Los **Usuarios de la información** y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.
- La **Unidad de Auditoría Interna**, es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta política.

5.2. Ingreso y salida de equipos

- Los equipos externos que ingresen a la Universitaria Virtual Internacional deben ser registrados por el número de serial que lo identifica, marca, propietario y hora de ingreso.
- Para los equipos que salgan de la Universitaria Virtual Internacional se debe verificar en la planilla el registro de ingreso confrontando el número de serial, marca y fecha y complementar esta información con la hora de salida y la firma de quien sale con dicho equipo.
- En caso que el equipo saliente sea de propiedad de la Universitaria Virtual Internacional debe tener autorización expresa por el vicerrectoría de investigación y tecnologías.

6. POLITICAS ADMINISTRATIVAS U ORGANIZACIONALES

Controles para facilitar la gestión de la información en la Universitaria Virtual Internacional, garantizando que existan responsabilidades claramente asignadas en

todos los niveles de la Universitaria Virtual Internacional, Todos los empleados y particulares que tengan acceso a los activos de información de la Universitaria Virtual Internacional, tendrán el compromiso de cumplir las políticas, normas y procedimientos que se dicten en esta materia, así como reportar los incidentes que detecten.

7. POLITICAS PARA GESTION DE ACTIVOS

Controles para catalogar los activos y protegerlos eficazmente. Toda la información sensible, así como los activos donde ésta se almacena o procesa, deben ser inventariados, asignarles un responsable y clasificarlos de acuerdo con los requerimientos en materia de seguridad de la información. A partir de esta clasificación se deben establecer los niveles de protección orientados a determinar, a quién se le permite el manejo de la información, el nivel de acceso a la misma y los procedimientos para su manipulación. La clasificación debe revisarse periódicamente y atender a los cambios que se presenten en la información o la estructura que puedan afectarla.

7.1. Inventario de activos

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.

El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad semestral.

El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable de Unidad Organizativa.

7.2. Clasificación de la información

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

Se establece el criterio de clasificación de la información en función a estas características:

- **Confidencialidad:**

- a. Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de la Institución o no. Tipo: PUBLICO
- b. Información que puede ser conocida y utilizada por todos los empleados de la Institución y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la Institución o terceros. Tipo: RESERVADA – USO INTERNO
- c. Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la Institución o a terceros. Tipo: RESERVADA - CONFIDENCIAL
- d. Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de la Institución, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros. Tipo: RESERVADA SECRETA

- **Integridad**

- a. Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria de la Institución.
- b. Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para la Institución o terceros.

- c. Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para la Institución o terceros.
- d. Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves a la institución o a terceros.

• **Disponibilidad:**

- a. Información cuya inaccesibilidad no afecta la operatoria de la Institución.
- b. Información cuya inaccesibilidad permanente durante a una semana podría ocasionar pérdidas significativas para la Institución, el Sector Público Nacional o terceros.
- c. Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas a la Institución, al Sector Público Nacional o a terceros.
- d. Información cuya inaccesibilidad permanente durante una hora podría ocasionar pérdidas significativas a la Institución, al Sector Público Nacional o a terceros.

Al referirse a pérdidas, se contemplan aquellas mesurables (materiales) y no mesurables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.).

Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:

- CRITICIDAD BAJA: Ninguno de los valores asignados superan el 1.
- CRITICIDAD MEDIA: Alguno de los valores asignados es 2
- CRITICIDAD ALTA: alguno de los valores asignados es 3

Sólo el Propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

- Asignarle una fecha de efectividad.
- Comunicárselo al depositario del recurso.
- Realizar los cambios necesarios para que los Usuarios conozcan la nueva clasificación.

Luego de clasificada la información, el propietario de la misma identificará los recursos asociados (sistemas, equipamiento, servicios, etc.) y los perfiles funcionales que deberán tener acceso a la misma.

7.3. Rotulado de la Información

Se definirán procedimientos para el rotulado y manejo de información, de acuerdo al esquema de clasificación definido. Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información:

- Copia ○ Almacenamiento
- Transmisión por correo, fax, correo electrónico
- Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, etc.).

8. POLITICAS PARA SEGURIDAD DE LOS RECURSOS HUMANOS

Controles para reducir los riesgos de error humano, robo, fraude y utilización abusiva de los equipamientos. Desde la vinculación del personal, se deben tener controles que permitan verificar la idoneidad e identidad, ética profesional y conducta. Los términos y condiciones de empleo o trabajo debe establecer la responsabilidad de los empleados, por la seguridad de los activos de información, que van más allá de la finalización de la relación laboral o contractual, por lo que se debe firmar un acuerdo de confidencialidad que se hace extensivo a los contratistas y terceros que tengan acceso a la información.

Deben existir mecanismos de información y capacitación para los usuarios en materia de seguridad, así como de reporte de incidentes que puedan afectarla. Los empleados deben cooperar con los esfuerzos por proteger la información y ser responsables de actualizarse en cada materia, así como consultar con el encargado de la seguridad de la información, en caso de duda o desconocimiento de un procedimiento formal, ya

que esto no lo exonera de una acción disciplinaria que deba llevarse a cabo cuando se incurra en violaciones a las políticas o normas de seguridad.

- Al momento de asignar un equipo informático a un usuario, este debe hacerse responsable de el mismo y comprometerse a reportar cualquier falla y entregarlo en perfecto estado
- Los propietarios de la información deben definir los niveles de acceso de cada usuario.
- Los nuevos empleados deben firmar un acuerdo de confidencialidad
- Se deben realizar capacitaciones periódicas sobre los sistemas de información y el uso de la misma
- Se debe realizar capacitación a empleados sobre aspectos de seguridad informática.
- Los usuarios de servicios de información, al momento de tomar conocimiento directo o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Responsable de Seguridad Informática.

9. POLITICAS DE SEGURIDAD FISICA

Controles para impedir la violación, deterioro y la perturbación de las instalaciones y datos industriales. Deben establecerse áreas seguras para la gestión, almacenamiento y procesamiento de información; éstas deben contar con protecciones físicas y ambientales acordes a los activos que protegen.

Esta seguridad debe mantenerse en los momentos de mantenimiento, cuando la información o los equipos que la contienen deben salir de la Institución o cuando se deben eliminar o dar de baja, para lo cual deben existir procedimientos especiales.

- Los equipos de cómputo deben ser apagados todos los días, exceptuando los servidores
- Se deben definir áreas seguras para el alojamiento físico de servidores

9.1. Controles de Acceso Físico

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Responsable de Seguridad Informática junto con el Responsable del Área Informática, a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

- Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.
- Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se mantendrá un registro protegido para permitir auditar todos los accesos.

9.2. Dispositivos de Seguridad de la Información

A continuación se presenta de forma general, la colección de recursos que constituye la infraestructura tecnológica y los dispositivos de seguridad que soportan y garantizan el funcionamiento del músculo tecnológico y de la Institución misma:

A. Hosting Dedicado

Este servicio permite a la Institución contar con servidores dedicados alojados en el Data Center para uso exclusivo de las plataformas “core” institucionales (portales web, aulas virtuales, intranet, sistemas de información académico-administrativofinanciero,

bases de datos). Es administrado por personal altamente calificado, con las condiciones técnicas de un data center, mantenimiento, monitoreo y conexión a Internet permanente a través de enlaces de alta velocidad y con las ventajas de expansión en el momento requerido, y que garantizan un servicio permanente y confiable.

El Data Center Triara de la empresa Claro Colombia está ubicado en un lugar estratégico de gran desarrollo empresarial en la Sabana de Bogotá, es un sitio que cumple con estrictas normas de construcción y seguimiento a rigurosos estándares de operación, para garantizar que los sistemas de información y comunicaciones allí alojados estén siempre disponibles, proporcionando a la Fundación Universitaria Católica del Norte un espacio con las condiciones tecnológicas adecuadas para atender los requerimientos de la estrategia de su negocio.

Las características generales de dicho Data Center son las siguientes:

- Único Data center en la región diseñado con especificaciones TIA/EIA 942 - Tier IV, ofrece una disponibilidad de sitio de 99,995% (Infraestructura, Clima y Potencia).
- 1000 m2 de área útil de IDC en su primera fase con capacidad de 3000 m2, desarrollado con características físicas y funcionales para ofrecer niveles superiores de redundancia en todos los subsistemas que lo componen.
- Monitoreo 7x24x365

Del Subsistema Arquitectónico:

- Selección del terreno en un área apropiada para Data center Tier IV:
- Terreno certificado con un historial de no inundaciones en los últimos 100 años.
- Ubicación fuera de conos de aproximación aérea.
- Ubicación del edificio en una zona de bajo impacto sísmico.
- Diseño estructural Antiincendios, resistente a inundaciones, vendavales y descargas eléctricas.
- Muros resistentes a ondas explosivas

B. Servicios plataforma computacional

Con este servicio Claro Colombia nos asigna una plataforma computacional (hardware, software, conectividad, servicios TI), para todas las aplicaciones de misión crítica en la institución.

Se incluyen diferentes niveles de administración, desde el sistema operativo, llegando incluso hasta la administración de aplicaciones específicas por parte del equipo de operación de servicios en el data center.

Algunas de las actividades que realiza el equipo de operaciones sobre los servicios hosting virtualizado, comprende:

- Administración de Hardware (stocks, repuestos y garantías).
- Administración de los servicios de telecomunicaciones (WAN, Internet)
- Administración de los servicios de networking e infraestructura IDC
- Administración de esquemas de balanceo de carga (de ser requerido)
- Administración de políticas y herramientas de seguridad
- Administración de Sistemas Operativos
- Administración de políticas de endurecimiento de sistemas operativos
- Conformación y distribución de esquemas de plantillas de seguridad
- Control de Vigencias de Licenciamiento
- Administración de software base (antivirus, agentes de backup y software de gestión)
- Administración de software de apoyo (p.j. FTP, DNS, Relay de Correo)

El dimensionamiento de los servicios, se realiza de acuerdo a estrictos procedimientos de análisis de capacidad, en donde se especifican los niveles de disponibilidad requeridos, plataformas involucradas, previsiones de crecimiento/decrecimiento, distribución de servicios, incorporación de nuevos desarrollos, entre otras variables.

Los servicios de Hosting y computación tienen definidas unas características de servicio de acuerdo a cada requerimiento, partiendo de unos servicios y componentes básicos como:

- **Servidores:** Físicos y Virtuales de diferentes especificaciones técnicas. Homologados con los mejores fabricantes y configurados en esquemas de alta disponibilidad y desempeño.
- **Software:** Licenciamiento acorde a los requerimientos de la solución. Incluyendo soporte y actualizaciones con sus fabricantes, distribuidores o agentes autorizados. Licenciamiento Microsoft por consumo.
- **Conectividad:** Servicios de conexión Internet, MPLS o de datos desde las sedes de nuestros clientes a nivel local, regional o mundial hasta la nube de nuestros data center. Diferentes opciones de configuración LAN, según disponibilidad y tráfico dimensionado. Configuraciones dedicadas a las redes de gestión y monitoreo.
- **Seguridad:** Servicios de Firewall e IPS (protección contra intrusos) para sus perímetros de conectividad, para sus capas lógicas. VPN's SSL e IPSec, Antivirus.
- **Almacenamiento:** A través de opciones de plataformas con discos FC, SAS y SATA.
- **Backup y continuidad:** Soluciones y políticas de backup para el almacenamiento local o externo de servidores ubicados en nuestros data center. Opciones de replicación sincrónica o asíncrona de almacenamiento entre nuestros data center. Toma y respaldo de imágenes de servidores físicos y virtuales.
- **Servicios de red:** Balanceo de carga para servidores y/o aplicaciones a nivel local o global, NTP, DNS, Relay de Correo, Replicación de servidores, sistemas operativos, aplicaciones.
- **Servicios:** Administración y operación de plataformas de hardware, aplicaciones, gestión y monitoreo. Control y gestión de cambios, eventos e incidentes. Monitoreo avanzado, Reporting, Análisis de vulnerabilidad y remediación.

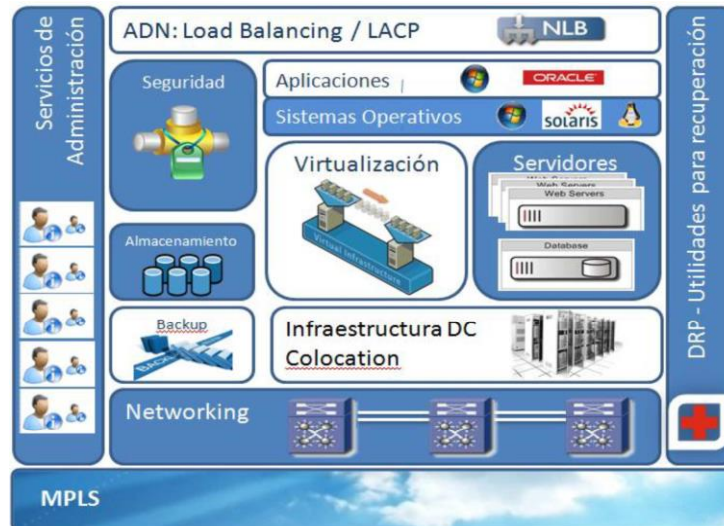


Ilustración. Esquema general de soluciones Hosting y plataforma computacional

C. Soluciones de almacenamiento y respaldo (Backup)

- **Almacenamiento**

Las soluciones de almacenamiento están diseñadas para la gestión de información crítica, con el mayor rendimiento e integradas completamente a soluciones de conectividad, se constituyen en la mejor alternativa de almacenamiento para datos críticos en la Universitaria Virtual Internacional.

Estas soluciones incluyen el suministro de hardware, software, comunicaciones y servicios por parte del Data Center, permitiendo alojar datos estructurados y no estructurados, en ambientes SAN.

Con una sólida arquitectura de respaldo y recuperación, resuelve el espectro completo de desafíos de disponibilidad de datos (99.9%) y mantiene accesibles los datos de la institución.

Características Principales del servicio de almacenamiento:

- **Escalable:** Capacidad de expansión de fácil actualización para un mejor rendimiento.

- **Rápida:** Alto rendimiento y tiempos de respuesta rápidos para bases de datos, correo electrónico y aplicaciones técnicas.
- **Confiable:** Disponibilidad continua de datos y redundancia a nivel del sistema para satisfacer las necesidades del negocio y aplicaciones de misión crítica. Orientación al estricto cumplimiento de niveles de servicio.

Niveles de almacenamiento ofrecido:

- **Nivel 1:** Almacenamiento externo SAN (Discos FC 15K en sistema de almacenamiento HighEnd, para Bases de Datos). Este servicio es utilizado por la Universitaria Virtual Internacional para almacenar la información de las principales Bases de Datos: Oracle, SQL Server, PostgreSQL.
- **Nivel 2:** Almacenamiento externo SAN (Discos SATA 7.2K Rpm en sistemas de almacenamiento Modular, para Aplicaciones). Este es utilizado por la Universitaria Virtual Internacional para almacenar la información de los principales sistemas de Información (a nivel de directorios): Suite Academusoft/Gestasoft, Portales, Intranet, Biblioteca Virtual, Revista Virtual, Mesa de Ayuda, Brújula Planeación y Calidad.

- **Tipos de arreglo ofrecido:** Raid 5

Además del almacenamiento presentado a cada servidor, contamos con la disponibilidad de 1500GB de almacenamiento, para poder garantizar el backup diario de todas las bases de datos y componentes específicos, para luego llevarla de forma directa a cinta.

- **Backup**

Para respaldar la información de la plataforma, nos ofrece su servicio de Backup administrado, para la generación periódica de toma de respaldo de los archivos y/o carpetas indicadas por institución, en un plan total para la capacidad de Backups definida para los servidores de la red LAN del servicio de hosting dedicado, en medios magnéticos con las siguientes características:

La información de la Universitaria Virtual Internacional, será respaldada en unidades PTL de acuerdo al tipo de Backups a realizar, utilizando infraestructura del Data Center para tal fin.

Los Backups serán ejecutados con la siguiente periodicidad:

Descripción	Diaria	Semanal	Quincenal
Política Retención Almacenamiento PTL	Incremental	Total	Total
	7 días	4 semanas	12 meses
	Si	Si	Si

Tabla. Descripción ejecución Backups

Incluye Backups a través de PTL para 750GB, respaldo por LAN para un servidor. Respaldo del Sistema Operativo: System State, Folders, Bases de datos en frío. Backups con cintas compartidas. También incluye backup en disco incremental diario con retención de 7 días en disco, total semanal con retención de 4 semanas en disco y total mensual con retención de 12 meses en PTL. El Backup incremental diario NO puede superar el 25% del Total o Full Backup.

D. Servicios administrados de Seguridad

Los servicios de seguridad administrados por personal especialista en Data Center se constituyen en un conjunto de estrategias de suministro de plataforma, administración y monitoreo, buscando garantizar alta disponibilidad, la seguridad lógica de la red, de equipos, servicios, información y programas de cómputo.

Esto se logra mediante la estructuración de servicios como una única solución de seguridad, el trabajo de un grupo de expertos en seguridad que realizan constantemente acuerdos entre las partes involucradas (usuarios y responsables), análisis, documentación y tareas de mantenimiento con el fin de garantizar la confianza y tranquilidad requeridas.

La solución que nos ofrece actualmente la empresa Claro Colombia se orienta hacia el aseguramiento de procesos y al acompañamiento en tres frentes principales:

- **Requerimientos regulatorios y de certificación**

Asistencia y aseguramiento de procesos orientados al cumplimiento de regulaciones nacionales e internacionales.


- ISO 27001 ○ Basilea II ○ SARO ○ SAS 70
- Sarbanes-Oxley
- Regulaciones de seguridad de la Contraloría General.

- **Disminuir la complejidad operacional**

Busca optimizar la administración de seguridad en la institución y transferirle estos beneficios disminuyendo la conectividad de TI, consolidando y estandarizando infraestructura y realizando las inversiones en dispositivos de seguridad integrando múltiples proveedores.

- **Control de amenazas**

Dicha solución integra al Centro de Operaciones de Seguridad – SOC, el cual está permanentemente revisando las políticas de seguridad acordadas con la Universitaria Virtual Internacional, vigilando constantemente las posibles vulnerabilidades y fallas en los sistemas y componentes de la solución, en conjunto con nuestro Centro de Operaciones de Red – NOC. La integración de estas políticas de seguridad con las soluciones de conectividad, así como la revisión de métricas desempeño y el comportamiento, marcan la total integración de la solución.

Firewall	
<ul style="list-style-type: none"> Centralizado (en la nube CLARO Colombia) para 3000Kbps Provee un filtro y la administración de políticas de seguridad que protegen eficientemente la red de institución. Ubicado en los IDC Claro Colombia, se administra bajo políticas estándar de seguridad definidas por el SOC. Maximiza el desempeño de nuestra solución. 	


Características del Firewall de nuestra solución

FIREWALL

Centralizado de 8192K

365 Días de Gestión y Monitoreo DOC/SOC	45 Días de Logs	100 Reglas/Políticas
3 Cambios de reglas/políticas por mes	1 Plataforma Centralizada /Alta Disponibilidad	750 Sesiones concurrentes para 5MB
1		Reporte Mensual x Mail: -Reporte de reglas configuradas -Top 10 puertos por ancho de banda -Resumen de eventos -Distribución de protocolos por día durante el mes

Tabla. Características Firewall

IPS	
<ul style="list-style-type: none"> Centralizado (en la nube del data center) para 3000Kbps Ubicado en los IDC, se administra y gestiona bajo políticas estándar de seguridad definidas por el SOC. Provee inteligencia adicional al nuestra solución de Firewall Administrado. 	

Esta estrategia permite agregar un nivel superior de seguridad a la red de la Universitaria Virtual Internacional, estableciendo una sólida metodología de prevención y defensa ante ataques.



Ilustración. Descripción proceso IPS

Servicios que incluye nuestra solución:

Centralizado					
Incluye detección prevención de intrusos y/o ataques basados en: <ul style="list-style-type: none"> Suscripción (Grupo mundial de investigación de amenazas) Políticas o perfiles de alto, mediano y bajo control 	Especializado en tráfico común (por ej., http, smtp, ftp, tráfico SQL entre otros). <ul style="list-style-type: none"> No soporta protocolos cifrados 	Funcionalidades de Anti spyware perimetral (evita la infección y reproducción)	Control de tráfico especializado para telefonía IP (H323, SIP)	Plataforma en Alta Disponibilidad <ul style="list-style-type: none"> Gestión y monitoreo 7 * 24 Personalización de alertas de notificaciones por ocurrencia de eventos (Opcional) 200 sesiones concurrentes por cada MB de BW 	Reporte mensual enviado por E-mail <ul style="list-style-type: none"> Resumen Top de eventos. Top de origen de eventos Top de destino de eventos Resumen de la tendencia de los eventos de seguridad
45 Días de Logs Soporta direccionamiento valido desde CPE, No soporta direccionamiento invalido (requiere traslación de direcciones invalidas a validas en el CPE o en equipo de punto central)					

Tabla. Descripción servicios IPS

CONTROL DE NAVEGACIÓN

- Centralizado (en la nube del data center)
- Servicio de filtrado url, se crean perfiles y permite la navegación a un grupo de usuarios hacia unas categorías de navegación y restringe hacia otras.



ADMON. ANCHO DE BANDA

- Centralizado (en la nube del data center)
- Permite controlar el ancho de banda utilizado por IPs en particulares, protocolos, grupos y/o servicios. Dicho servicio nos permite garantizar rapidez y calidad de servicio (QoS) para la salida a internet.



VPN'S

- VPN IPSec
- VPN SSL para servicios Hosting y/o Colocation
- Por medio de este servicio se realiza la administración de los servidores que se encuentran en la modalidad de Hosting dedicado virtualizado.



E. Centro de Operaciones de Seguridad – SOC

El Centro de Operaciones de Seguridad del data center - SOC está conformado por un grupo de expertos en seguridad. Orientado a controlar, monitorear y ajustar las políticas de seguridad de las soluciones que así lo requieren.

Alcance del SOC

Las principales actividades en capacidad de desarrollo por parte del equipo SOC y sus integrados, son:

- | | |
|--|--|
| <ul style="list-style-type: none">▪ Levantamiento de información.▪ Análisis de vulnerabilidades y remediación.▪ Definición de las políticas y reglas de seguridad.▪ Configuración de servicios.▪ Aseguramiento de la calidad.▪ Consultorías para el establecimiento de planes de recuperación ante desastres y esquemas de continuidad del negocio. | <ul style="list-style-type: none">▪ Administración de la configuración.▪ Administración de cambios.▪ Gestión de problemas.▪ Monitoreo de los equipos.▪ Monitoreo de políticas.▪ Monitoreo de seguridad 7X24X365.▪ Apoyo en la implementación de políticas y configuraciones de seguridad.▪ Apoyo en la operación de contingencia (DRP). |
|--|--|

Adicionalmente, algunos de los controles sugeridos por algunas normas internacionales al respecto, realizados y homologados dentro de las buenas prácticas del SOC son:

COBIT DS 5.19.	Detección y prevención y correlación de eventos
COBIT DS 7.5.	Monitorización
COBIT DS 9.	Gerenciamiento de Configuraciones
COBIT DS 10.	Gerenciamiento de Problemas e Incidentes
NTC-ISO/IEC 27001	Protecciones contra códigos maliciosos
NTC-ISO/IEC 27001	Sistemas de control de acceso a información

F. Disponibilidad

Actualmente los servicios contratados por la Universitaria Virtual Internacional, incluyen:

- Conectividad a Internet por medio de 1 enlace desde Datacenter con alta disponibilidad de 3000Kbps
- Dispositivos perimetrales, Firewall Dedicado.
- Dispositivo de seguridad de alto desempeño, que está instalado en el Datacenter con el fin de aislar, controlar y auditar el tráfico que circula hacia y desde los servidores en hosting.
- Monitoreo 24 x 7 de la funcionalidad del firewall e IPS.
- Soporte técnico las 24 horas los 365 días del año, cubriendo los aspectos de conectividad a Internet hasta la interface de conexión con la red privada de la institución.
- Backups de la configuración del firewall.
- Updates y hot fixes: se actualizan proactivamente en el firewall a medida que sean liberados por el fabricante, los updates y hot fixes que afecten la funcionalidad del firewall. Igualmente se aplican a nivel de Sistemas Operativos y plataforma de virtualización.
- Cambios de políticas mensuales: servicio de administración de los dispositivos de seguridad, cubriendo los cambios de políticas.

- Todos los servidores se gestionan mediante el servicio de VPN (Virtual Private Network/Red Privada Virtual).

Alcance de los niveles de disponibilidad en DataCenter

Servicio	Disponibilidad	Cubrimiento
Hosting y Seguridad	99.7%	DataCenter
MPLS	99.7%	DataCenter
Internet DataCenter	99.7%	DataCenter

Tabla Disponibilidad DataCenter

Acuerdos de niveles de servicios de Operación

Indicador	Meta	Descripción
Satisfacción	85%	Es un indicador perceptual que señala el nivel de complacencia que tienen los usuarios del servicio con este y con el prestador del mismo.
Seguridad	100%	Ejecución exitosa del Schedule de Backups. Ejecución exitosa de las restauraciones solicitadas por demanda o programadas. Oportunidad en la ejecución del plan de recuperaciones.
Ordenes de trabajo	90%	Oportunidad en la ejecución de las órdenes de trabajo, según la clasificación respectiva.
Plan de Producción	97%	Ejecución oportuna y con calidad de los procesos programados en el plan de producción.
Reportes de Gestión	95%	Oportunidad en la entrega de los reportes mensuales, incluye puntualidad en su entrega y calidad en el mismo.
Disponibilidad Sistemas de Información	99.7%	Llevar el registro de la disponibilidad de los sistemas de información: Suite Academusoft/Gestasoft, Portal e Intranet de SharePoint, Biblioteca Virtual, Revista Virtual, Mesa de Ayuda, Brújula Calidad y Planeación.

Tabla Acuerdos de niveles de servicios de operación

9.3. Protección de Oficinas, Recintos e Instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones.

Se establecen las siguientes medidas de protección para áreas protegidas:

- Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.
- Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia. Se agregará protección externa a las ventanas, en particular las que se encuentran en planta baja o presenten riesgos especiales.
- Separar las instalaciones de procesamiento de información administradas por la Universitaria Virtual Internacional de aquellas administradas por terceros.
- Restringir el acceso público a las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible.
- Almacenar los materiales peligrosos o combustibles en los siguientes lugares seguros a una distancia prudencial de las áreas protegidas de la Institución.
- Almacenar los equipos redundantes y la información de resguardo (back up) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal.

9.4. Ubicación y Protección del Equipamiento y Copias de Seguridad

El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

- Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.
- Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.
- Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida. Y adoptar controles adecuados para minimizar el riesgo de amenazas potenciales, por: robo o hurto, incendio, explosivos, humo, inundaciones o filtraciones de agua (o falta de suministro), polvo, vibraciones, efectos químicos, interferencia en el suministro de energía eléctrica (cortes de suministro, variación de tensión), radiación electromagnética, derrumbes.

9.5. Mantenimiento de Equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

- Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal de la Dirección de Tecnologías y Apoyo. La dirección mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.
- Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.

- Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
- Registrar el retiro de equipamiento de las instalaciones de la Universitaria Virtual Internacional para su mantenimiento.
- Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

9.6. Políticas de Escritorios y Pantallas Limpias.

Se adopta una política de escritorios limpios para proteger documentos en papel y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Se aplicarán los siguientes lineamientos:

- Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- Guardar bajo llave la información sensible o crítica de la Institución (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.
- Desconectar de la red / sistema / servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o copia de las llaves de seguridad utilizadas en el sector a su cargo. Tales elementos se encontrarán protegidos en sobre cerrado o caja de seguridad para impedir

accesos no autorizados, debiendo dejarse constancia de todo acceso a las mismas, y de los motivos que llevaron a tal acción.

- Proteger los puntos de recepción y envío de correo electrónico y postal y las máquinas de fax no atendidas.

9.7. Retiro de los Bienes

El equipamiento, la información y el software no serán retirados de la sede de la Institución sin autorización formal. Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de la Institución, las que serán llevadas a cabo. El personal será puesto en conocimiento de la posibilidad de realización de dichas comprobaciones.

10. POLÍTICAS DE GESTIÓN DE LAS TELECOMUNICACIONES Y OPERACIONES

Controles para garantizar un funcionamiento seguro y adecuado de los dispositivos de tratamiento de la información. Deben documentarse los procedimientos y responsabilidades de administración y seguridad que sean necesarios en cada ambiente tecnológico y físico, garantizando un adecuado control de cambios y el seguimiento a estándares de seguridad que deben definirse, así como el seguimiento a los incidentes de seguridad que puedan presentarse. Debe buscarse una adecuada segregación de funciones.

Deben garantizarse una adecuada planificación y aprobación de los sistemas de información que consideren o provean las necesidades de capacidad futura. Deben considerarse protecciones contra software malicioso y un adecuado mantenimiento y administración de la red, así como un adecuado cuidado de los medios de almacenamiento y seguridad en el intercambio de información.

10.1. Documentación de los Procedimientos Operativos

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Responsable de Informática o dueño de cada proceso.

Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

- Procesamiento y manejo de la información.
- Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.
- Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
- Restricciones en el uso de utilitarios del sistema.
- Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.
- Instrucciones especiales para el manejo de “salidas”, como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.
- Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

Se preparará adicionalmente documentación sobre procedimientos referidos a las siguientes actividades:

- Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.
- Instalación y mantenimiento de las plataformas de procesamiento.
- Monitoreo del procesamiento y las comunicaciones.
- Inicio y finalización de la ejecución de los sistemas.
- Programación y ejecución de procesos.

- Gestión de servicios.
- Resguardo de información.
- Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.
- Reemplazo o cambio de componentes del ambiente de procesamiento y comunicaciones
- Uso del correo electrónico.

10.2. Procedimientos de Manejo de Incidentes

Reporte de incidentes:

1- Todos los incidentes relacionados con la seguridad de la información tendrán que ser reportados mediante el centro de soporte, el cual informará al área encargada de la seguridad de la información esto, siempre y cuando se presenten indicios que involucren la seguridad de la información.

2- Se socializara entre funcionarios, proveedores y estudiantes los medios de comunicación establecidos para comunicar estos incidentes.

3- Los incidentes confirmados como incidentes de seguridad de la información tendrán que ser clasificados dentro del centro de soporte como incidente de seguridad de la información, allí se documentaran y evidenciaran todas las acciones realizadas ante el incidente.

4- Se le informara a las personas que reportan el incidente el estado de avance y el resultado obtenido una vez gestionado y concluido el incidente.

Clasificación de incidentes:

Según sea el caso se clasificaran los incidentes dentro de las siguientes categorías:

- Acceso no autorizado

- Modificación de recursos no autorizado (Plagios, Base de datos)
- Uso inapropiado de recursos (Divulgación)
- No disponibilidad (Denegación de Servicio)
- Otros

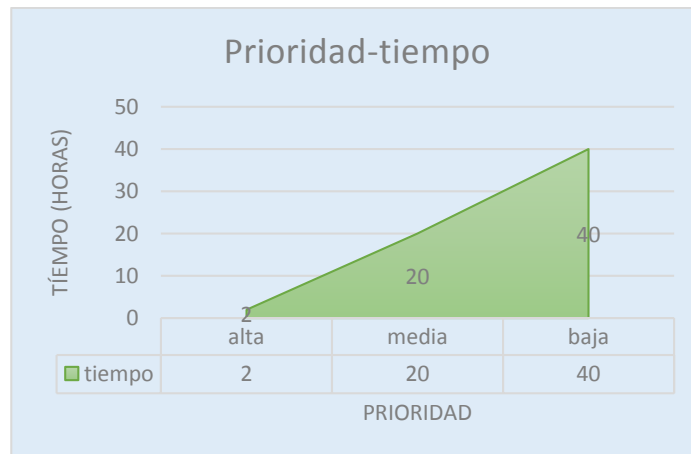
Estas categorías estarán consignadas dentro del centro de soporte como ítems que permitirán su fácil recordación.

Clasificación y tiempos de respuesta:

Para realizar una gestión adecuada de los incidentes se determinara un nivel de prioridad. Esto se determinara teniendo en cuenta los siguientes factores:

- Impacto
- Prioridad

Con el fin de atender los incidentes de la manera más adecuada se establecerán tiempos máximos de respuesta que se determinaran a partir del nivel de prioridad que se le dé al incidente. El centro de soporte permitirá el control de estos tiempos mediante un tiempo de respuesta parametrizado en la plataforma, teniendo siempre en cuenta la prioridad y el impacto del incidente.



Matriz de prioridades			
Prioridad/Impacto	Alto	Medio	Bajo
Alto	alta	alta	media
Medio	alta	media	baja
Bajo	media	baja	baja

Tabla Matriz de prioridades

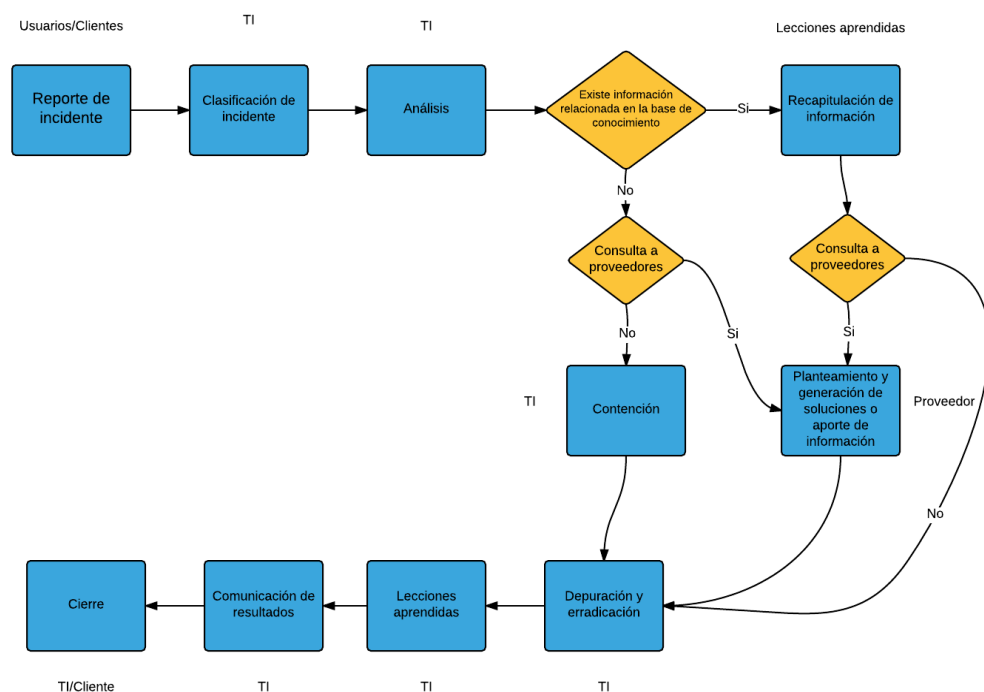
Tratamiento de incidentes:

- 1- Una vez reporta el incidente se procederá a recolectar evidencias que permitan la adecuada clasificación del mismo, dentro del centro de soporte se dará una clasificación inicial y una prioridad que puede cambiar si el incidente los amerita.
- 2- El responsable del tratamiento de incidentes se encargara de anexar las evidencias y hallazgos encontrados en el centro de soporte durante el primer contacto, con el fin de clasificar y priorizar de la manera más adecuada el incidente.
- 3- Con la recopilación de las evidencias se realizara un proceso de análisis investigación con el fin de orientar de manera más concisa la acción que se tomara frente al incidente. También se consultaran las lecciones aprendidas para recopilar información que permita dar una solución más rápida y si el caso lo amerita se contactara a los proveedores para plantear y generar soluciones o aportes de información.
- 4- Se realizara una contención con el fin de evitar propagaciones y la generación de posibles daños potenciales en información o arquitectura de TI. Para ello se establecerá en el momento la estrategia más adecuada para evitar los mencionados daños.
- 5- Después de realizada la contención se procederá a realizar la erradicación y depuración del incidente, posteriormente si es necesario se realizara un proceso para restablecer información, servicios o sistemas.
- 6- Una vez depurada la incidencia se adicionara como documento o como nota dentro del centro de soporte las **lecciones aprendidas**, estas tendrán que describir al detalle

en que consistió el incidente, cuáles fueron las herramientas utilizadas y cuál fue el procedimiento utilizado para dar solución a el incidente.

7- Se comunicara al colaborador que reportó el incidente los resultados obtenidos con la ya mencionada gestión.

8- Por último se realizara el cierre del incidente a satisfacción del usuario en el centro de soporte.



Responsabilidades:

Departamento de TI.

Los miembros del departamento de TI se encargaran de la recepción y gestión de los incidentes, también informaran los avances y hallazgos encontrados a los diferentes clientes y darán cumplimiento a la política de tratamiento de incidentes.

Cliente interno y externo.

Los clientes internos y externos tendrán la responsabilidad de reportar los incidentes mediante los medios de comunicación dispuestos para este fin.

Talento humano y TI.

Se encargaran de difundir de manera correcta la política de tratamiento de incidentes a todos los miembros que mantengan una relación con la organización.

11. POLÍTICAS DE CONTROL DE ACCESO A LOS DATOS

Medios para impedir accesos no autorizados y registro de los accesos efectuados. Deben establecerse medidas de control de acceso a las dependencias de cada entidad y a los diferentes niveles de la plataforma tecnológica, tales como la red, sistemas operativos y aplicaciones, así como a la información física que tenga un componente de seguridad. Estas medidas estarán soportadas en el desarrollo de la cultura de seguridad de las personas que laboran en la Universitaria Virtual Internacional y buscarán limitar y monitorear el acceso a los activos de información requeridos para el trabajo, de acuerdo con su clasificación y manejando controles, en dispositivos y servicios que permitan identificar los niveles de acceso que los usuarios deben tener.

Los usuarios serán responsables de realizar un adecuado uso de las herramientas de seguridad que se ponen a su disposición.

11.1. Reglas de Control de Acceso

Las reglas de control de acceso especificadas, deberán:

- Indicar expresamente si las reglas son obligatorias u optativas

Establecer reglas sobre la premisa “Todo debe estar prohibido a menos que se permita expresamente” y no sobre la premisa inversa de “Todo está permitido a menos que se prohíba expresamente”.

- Controlar los cambios en los rótulos de información que son iniciados automáticamente por herramientas de procesamiento de información, de aquellos que son iniciados a discreción del usuario
- Controlar los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por el administrador.
- Controlar las reglas que requieren la aprobación del administrador o del Propietario de la Información de que se trate, antes de entrar en vigencia, y aquellas que no requieren aprobación

11.2. Registro de Usuarios

El Responsable de Seguridad Informática definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender:

- Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.
- Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.
- Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad de la Institución, por ejemplo que no compromete la separación de tareas.
- Entregar a los usuarios un detalle escrito de sus derechos de acceso.
- Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.

Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.

- Mantener un registro formal de todas las personas registradas para utilizar el servicio.
- Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon de la Institución o sufrieron la pérdida/robo de sus credenciales de acceso.
- Efectuar revisiones periódicas con el objeto de cancelar identificadores y cuentas de usuario redundante, inhabilitar cuentas inactivas por más de 30 días.
- En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.
- Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.
- Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados.

11.3. Administración de Privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

- Identificar los privilegios asociados a cada producto del sistema, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos. Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.
- Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
- Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados.
- Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Responsable de Seguridad Informática

11.4. Administración de Contraseñas de Usuario

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

- Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración bien puede estar incluida en el Compromiso de Confidencialidad
- Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisionales, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.

- Generar contraseñas provisionales seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo cuando la reciban.
- Almacenar las contraseñas sólo en sistemas informáticos protegidos.
- Configurar los sistemas de tal manera que:
 - a. Las contraseñas tengan no menos a de 8 caracteres ,
 - b. Suspensión o bloqueen permanentemente al usuario luego de 3 intentos de entrar con una contraseña incorrecta (deberá pedir la rehabilitación ante quien corresponda),
 - c. Solicitar el cambio de la contraseña cada 30 días,
 - d. Impedir que las últimas 12 contraseñas sean reutilizadas.

11.5. Responsabilidades del Usuario

Uso de contraseña: Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

- Mantener las contraseñas en secreto.
- Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el Responsable del Activo de Información de que se trate, donde:

- a. Sean fáciles de recordar.
 - b. No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
 - c. No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
- Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
 - Cambiar las contraseñas provisionales en el primer inicio de sesión (“log on”).
 - Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
 - Notificar cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

11.6. Equipos Desatendidos en Áreas de Clientes

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente. Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

El Responsable de Seguridad Informática debe coordinar con el Área de Recursos Humanos las tareas de concientización a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

Los usuarios cumplirán con las siguientes pautas:

- Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.

- Proteger las PC's o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

11.7. Acceso a Internet

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto.

El Responsable de Seguridad Informática definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por el Responsable de la Unidad Organizativa a cargo del personal que lo solicite. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios.

Se evaluará la conveniencia de generar un registro de los accesos de los usuarios a Internet, con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares.

Dicho control será comunicado a los usuarios de acuerdo a lo establecido en el punto "Compromiso de Confidencialidad". Para ello, el Responsable de Seguridad Informática junto con el Responsable del Área de Informática analizarán las medidas a ser implementadas para efectivizar dicho control, como ser la instalación de "firewalls", "proxis", etc.

11.8. Identificación y Autenticación de los Usuarios

Todos los usuarios (incluido el personal de soporte técnico, los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

En circunstancias excepcionales, cuando existe un claro beneficio para la Institución, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se documentará la justificación y aprobación del Propietario de la Información de que se trate.

11.9. Sistema de Administración de Contraseñas

Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático. Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad.

El sistema de administración de contraseñas debe:

- Imponer el uso de contraseñas individuales para determinar responsabilidades.
- Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de las mismas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
- Imponer una selección de contraseñas de calidad según lo señalado en el punto “Uso de Contraseñas”.
- Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto “Uso de Contraseñas”.
- Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
- Mantener un registro de las últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.
- Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.
- Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.

- Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.
- Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo claves de impresoras, hubs, routers, etc.).
- Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas.

11.10. Control de Acceso a las Aplicaciones

Restricción del Acceso a la Información: Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación de conformidad con la Política de Control de Acceso definida, sobre la base de los requerimientos de cada aplicación, y conforme a la Política de la Institución para el acceso a la información, (Ver 9.1. Requerimientos para el Control de Acceso).

Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

- Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación. El Propietario de la Información involucrada será responsable de la adjudicación de accesos a las funciones. En el caso de que las actividades involucradas en el otorgamiento de acceso revistan un carácter técnico elevado, las mismas serán llevadas a cabo por personal del área de sistemas, conforme a una autorización formal emitida por el Propietario de la Información.
- Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder, con la adecuada edición de la documentación de usuario.
- Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.

- Garantizar que las salidas de los sistemas de aplicación que administran información sensible, contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a las terminales y ubicaciones autorizadas.
- Revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.

Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

12. POLÍTICAS PARA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE

Controles para garantizar que la Política de Seguridad esté incorporada a los sistemas de información. Asegurar que se haga un adecuado análisis e implementación de los requerimientos del software desde su diseño, ya sea interno o adquirido, que incluya garantías de validación de usuarios y datos de entrada y salida, así como de los procesos mismos, de acuerdo con la clasificación de los activos a gestionar en la herramienta. Además se establecerán controles para cifrar la información confidencial y se buscará evitar la posibilidad de una acción indebida por parte de un usuario del sistema. Igualmente, se deben asegurar los archivos del sistema y mantener un control adecuado de los cambios que puedan presentarse.

La implantación de nuevas herramientas de Hardware y Software, de sistemas de información y de otros recursos informáticos, deben cumplir con las políticas definidas

12.1. Procedimiento de Control de Cambios

A fin de minimizar los riesgos de alteración de los sistemas de información, se implementarán controles estrictos durante la implementación de cambios imponiendo el cumplimiento de procedimientos formales. Éstos garantizarán que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

Para ello se establecerá un procedimiento que incluya las siguientes consideraciones:

- Verificar que los cambios sean propuestos por usuarios autorizados y respete los términos y condiciones que surjan de la licencia de uso.
- Mantener un registro de los niveles de autorización acordados.
Solicitar la autorización del Propietario de la Información, en caso de tratarse de cambios a sistemas de procesamiento de la misma. Identificar todos los elementos que requieren modificaciones (software, bases de datos, hardware).
- Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.
- Obtener aprobación formal por parte del Responsable del Área Informática para las tareas detalladas, antes que comiencen las tareas.
- Solicitar la revisión del Responsable de Seguridad Informática para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.
- Efectuar las actividades relativas al cambio en el ambiente de desarrollo.
- Obtener la aprobación por parte del usuario autorizado y del área de pruebas mediante pruebas en el ambiente correspondiente.
- Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
- Mantener un control de versiones para todas las actualizaciones de software.
- Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.
- Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria.
- Garantizar que sea el implementador quien efectúe el pasaje de los objetos modificados al ambiente operativo, de acuerdo a lo establecido en “Control del Software Operativo”.

13. POLÍTICAS PARA GESTIÓN DE INCIDENTES

Procedimiento a seguir en caso de ocurrencia de incidentes. De acuerdo a una clasificación de los incidentes según el grado en que afecten el normal funcionamiento del negocio.

Asegurar que se haga una adecuada evaluación del impacto en la Institución frente a los eventos relevantes, realizar planes de atención de incidentes y mejora de procesos, para aquellos eventos que resulten críticos para la supervivencia del mismo. Estos planes deben considerar medidas técnicas, administrativas y de vínculo con entidades externas; deben probarse y revisarse periódicamente; y deben estar articulados en toda la Institución con los diferentes tipos de recursos tecnológicos y no tecnológicos.

14. POLÍTICAS PARA LA CONTINUIDAD DE LA OPERACIÓN

Controles para reducir los efectos de las interrupciones de actividad y proteger los procesos esenciales de la empresa contra averías y siniestros mayores.

Se debe evaluar el impacto de los diferentes procesos en la Institución y realizar planes de mitigación y continuidad para aquellos que resulten críticos. Los planes de mitigación y continuidad deben considerar medidas tanto técnicas como administrativas y de vínculo con entidades externas; deben probarse y revisarse periódicamente, y deben permanecer articulados con los diferentes recursos tecnológicos y no tecnológicos existentes en toda la Institución.

15. POLÍTICAS PARA EL CUMPLIMIENTO Y NORMATIVIDAD LEGAL

Controles para prevenir los incumplimientos de las leyes penales o civiles, de las obligaciones reglamentarias o contractuales. Garantizar que se dé cumplimiento adecuado a la legislación vigente para lo cual analizará los requisitos legales aplicables a la información que se gestiona incluyendo los derechos de propiedad intelectual, los tiempos de retención de registros, privacidad de la información, uso inadecuado de recursos de procesamiento de información, uso de criptografía y recolección de evidencias.