Manual de procedimientos sobre las tecnologías de información y comunicación

Universidad Adventista Dominicana (UNAD)

Vicerrectoría de Planificación y Desarrollo

Departamento de Tecnología y Comunicación

Edición 2025

Versión actualizada

Bonao, República Dominicana

Tabla de contenido

Misión, visión y valores 4
- Misión 4
- Visión 4
- Valores 4
  - Excelencia 4
  - Compromiso 5
  - Creatividad 5

Voto de aprobación 6
Introducción 7
Objetivo 7
Objetivos específicos 7
Disposiciones y procedimientos institucionales de tecnologías de la información 8
Responsabilidades 8
Glosario 8
Procedimiento de clasificación de la información 15
- Objetivo 15
- Procedimiento general de clasificación de información 15
  - Información confidencial 16
  - Información para uso interno 16
  - Información para uso público 16
- Almacenamiento de la información 17
  - Información confidencial 17
  - Información para uso interno 17
  - Información para uso público 17
- Tránsito o distribución de la información 17

Procedimiento de seguridad de la información 18
- Objetivo 18
- Procedimiento general de seguridad de la información 18
- Revisión de los servicios de tecnologías de información y comunicación 18
- Registro y gestión de eventos de seguridad 19
  - Servidores 20
  - Equipo de Red 20
  - Máquinas de escritorio 20
  - Recolección de Información 21
  - Alteración datos personales 22
  - Severidad del incidente 22

Procedimiento de prevención, detección y corrección de virus 22

Procedimiento para la prevención, detección y corrección de virus 22
Procedimiento de conexión de Acceso Remoto 23
Procedimiento de control de acceso físico al Data center 24
Procedimiento para la administración de claves de usuario 24
Procedimiento para el uso de dispositivos móviles 28
Objetivo 28
Procedimiento para para el uso de dispositivos móviles 28
Acceso al correo electrónico 29
Acceso a la red 29
Acceso a intranet 29
Acceso a los sistemas de información 30

Misión, visión y valores

Misión

Formar y especializar profesionales excelentes, innovadores, con valores cristianos basados en la filosofía adventista, comprometidos a servir a Dios, a la patria y al mundo.

Visión

Ser un referente por la excelencia en la formación y especialización profesional con valores cristianos.

Valores

Los valores de este quinquenio (2025–2029) están definidos bajo tres perspectivas, con el fin de abarcar lo que comprende nuestra filosofía institucional.

Excelencia

Perspectiva aspiracional. La excelencia en la UNAD es necesaria para satisfacer en su totalidad los estándares de alta calidad de los diferentes grupos de interés que componen nuestra institución.

Perspectiva fundamental. Nuestro modelo es el Creador del universo, quien hizo todo con excelencia, “bueno en gran manera”. Fundamentados en esto, formamos profesionales de alta calidad.

Perspectiva operacional. Trabajamos con excelencia y damos lo mejor de nosotros en el cumplimiento de nuestras responsabilidades y en nuestras relaciones, porque de esta forma cumplimos nuestra misión y brindamos servicios con eficacia y eficiencia en las diferentes áreas de nuestra institución.

Compromiso

Perspectiva aspiracional. En la UNAD todos nos sentimos comprometidos con el servicio, lo que nos impulsa a desarrollar acciones para suplir las necesidades y aliviar el dolor de las personas, llevando esperanza en el cumplimiento de la misión.

Perspectiva fundamental. Dios, en su infinito amor, cumplió su promesa: envió a su Hijo amado para servir y entregar su vida para librarnos de la muerte. Nos enseñó el compromiso del servicio a los demás mediante la entrega desinteresada de nuestros dones y talentos.

Perspectiva operacional. Demostramos compromiso e interés por los problemas de la sociedad que nos rodea. Mostramos disposición y pasión para atender las tareas encomendadas y el servicio a los demás, poniendo nuestros dones y talentos a disposición de la iglesia y de la sociedad.

Creatividad

Perspectiva aspiracional. Usamos la creatividad para impulsar cambios y mantenernos a la vanguardia, innovando las teorías, los modelos, las metodologías y las formas de hacer en un mundo tan cambiante y exigente.

Perspectiva fundamental. Dios hizo al hombre con capacidad creativa y de innovación. Jesucristo vivió en este mundo sirviendo y enseñando de una manera diferente, y generó un impacto positivo en la mente y el corazón de las personas.

Perspectiva operacional. Buscamos soluciones creativas en todas las áreas de la UNAD y para los problemas de la sociedad, generando y difundiendo el conocimiento. Hacemos uso sabio de la tecnología para optimizar nuestro desempeño en el cumplimiento de nuestra misión.

Voto de aprobación

El presente manual cuenta con el respaldo de la siguiente resolución de la Junta de Gobierno de la Universidad Adventista Dominicana (UNAD):

Tabla 1
Resolución de la Junta de Gobierno que respalda el manual

Órgano	Junta de Gobierno de la Universidad Adventista Dominicana (UNAD)
Resolución	JG 2025-032
Reunión	Junta Ordinaria del 18 de marzo de 2025

RESUELVEN: Aprobar la actualización de documentos, estatutos, manuales, emblemas, entre otros, y hacer un acervo indexado de documentos institucionales.

Introducción

El presente manual de procedimientos sobre las tecnologías de información y comunicación instruye a todos los funcionarios de la Universidad Adventista Dominicana (UNAD), que son responsables y/o usuarios de la plataforma de tecnologías de información y comunicación para garantizar una gestión oportuna, segura, confidencial, pertinente y respetuosa de las normas y estándares internacionales.

Para asegurar el cumplimiento del presente Manual, las disposiciones y los procedimientos, han sido agrupados en tres categorías: Seguridad, Usuarios y gestión de tecnologías de información y comunicación.

En todo momento se debe garantizar el cumplimiento de los lineamientos establecidos en la Política de tecnologías de información y comunicación.

Objetivo

Brindar las orientaciones procedimentales a las representaciones de la UNAD en las Unidades y departamentos , para una adecuada gestión de la plataforma de tecnologías de información y comunicaciones.

Objetivos específicos

1. Brindar a la UNAD, un marco regulatorio acorde a los desafíos y retos de la cooperación técnica en materia de tecnologías de información y comunicación alineado con los estándares internacionales.
2. Cumplir con las disposiciones institucionales contenidas en las políticas de tecnologías de la información y comunicación.
3. Ejecutar las orientaciones contenidas en el presente Manual, de forma comprobable, documentada y verificable.

Disposiciones y procedimientos institucionales de tecnologías de la información

La UNAD, mediante el presente Manual establece los procedimientos institucionales para asegurar que la plataforma de tecnologías de la información y comunicación que se gestione de manera segura, confidencial, integral, oportuna y de acuerdo con los estándares internacionales.

Responsabilidades

La implementación y el cumplimiento del presente Manual son responsabilidad de todos los miembros de la UNAD y personas vinculadas al mismo que sean autorizadas a acceder a la plataforma tecnológica de información y comunicación.

Glosario

Activo de información: La UNAD, considera como activo de información, según todo aquello que tenga valor informativo para la organización, incluyendo soporte digital y físico, tales como:

a. Los datos creados o utilizados por un proceso de la organización en medio digital, en papel o en otros medios.
b. El hardware y el software utilizado para el procesamiento, transporte o almacenamiento de información.
c. Los servicios utilizados para la transmisión, recepción y control de la información.
d. Las herramientas o utilidades para el desarrollo y soporte de los sistemas de información.
e. Personas que manejen datos, o un conocimiento específico muy importante para la organización (manejo de información crítica y conocimiento).

Adware: Es un malware que usualmente está enquistado en el navegador, pero podría también estar en el otra parte del sistema, para presentar anuncios no deseados en el dispositivo.

Amenaza persistente avanzada (APT por sus siglas en inglés): Es un ataque dirigido a largo plazo, para lograr obtener información confidencial crítica.

Authentication cisco server (ACS): Es un sistema de control de acceso que opera como servidor RADIUS (es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP) y TACACS+ (permite a un servidor de acceso remoto comunicarse con un servidor de autenticación para determinar si el usuario tiene acceso a la red), administrando la autenticación del usuario, el control de acceso a dispositivos y políticas de control centralizadas en la red.

Base de Datos: Conjunto de información, organizada y almacenada en un medio sea físico, o digital.

Bring Your Own Device (BYOD): Es una nueva tendencia tecnológica que permite a los trabajadores llevar sus dispositivos portátiles personales para llevar a cabo tareas del trabajo y conectarse a la red y recursos corporativos.

Broadcast: Es la difusión masiva de información o paquetes de datos a través de redes informáticas. El término se utiliza en la informática y en las telecomunicaciones.

Buffers: es un espacio de memoria en el que se almacenan datos evitando que el programa que los necesita se quede sin datos durante una transferencia.

Buffer overflow: Es un desbordamiento de la capacidad de almacenamiento de los datos en la memoria de la computadora, más allá de los límites de un buffer de longitud-fija.

Código Malicioso (Malware): Cualquier programa que se instala en un sistema operativo, cuyo fin es interferir con el correcto funcionamiento del mismo.

Confidencialidad: La cualidad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Controlador de dominio: Servidor que brinda el servicio de autenticación de usuarios y máquinas en un entorno de red, puede ser centralizado o distribuido.

Data center (centro de procesamiento de datos): Es una instalación, construcción o inmueble de gran tamaño donde se albergan y mantienen numerosos equipos electrónicos como servidores, ventiladores, conexiones y otros recursos necesarios que se utilizan para mantener una red o un sistema de computadoras, información, conexiones y datos.

Demilitarized Zone (DMZ): Zona en la que se brinda servicios al mundo de internet, y que se encuentra física o lógicamente separada de la red interna de una organización.

Denegación de Servicios (DOS por sus siglas en inglés): Es cuando los recursos de un servicio son consumidos por un único usuario, en detrimento del resto de usuarios legítimos.

Dirección de Protocolo de Internet (IP Address): Es una representación numérica, para identificar un equipo conectado en una red IP, o para identificar un conjunto de equipos (red).

Disponibilidad: La cualidad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Equipo de Red: Cualquier dispositivo activo, que facilita la comunicación entre dos equipos finales, sea que estén en el mismo segmento de red; o que se encuentren en segmentos de redes diferentes.

Evento de seguridad de la información: La ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o la falla de salvaguardas, o una situación previamente desconocida que pueda ser relevante para la seguridad.

File Server: Herramienta de tecnologías de información y comunicación que ofrece el servicio de almacenamiento de contenidos digitales de forma oportuna, segura, confidencial, integra.

Firewalls: Es un dispositivo de seguridad, el cual regularmente es utilizado para segmentar el mundo público del mundo privado. Mediante un conjunto de reglas definidas, se establece el tráfico permitido y cuál es denegado, y el sentido del mismo.

Gestión de TI: Es el proceso de manejo y supervisión de todos los asuntos relacionados con las operaciones y recursos de tecnología de la información dentro de una organización. Más específicamente, aquellos relacionados al tratamiento, almacenamiento y protección de la información. Este es un proceso que involucra la recolección, almacenamiento, selección, comparación y distribución de datos.

Gusano: Es un malware, con capacidad de propagar copias de sí mismo a equipos no infectados, de manera autónoma.

Hacking: Actividades que buscan ganar acceso indebido a un equipo informático (PC, Tablet, Smartphone, equipos de red, otros) que pueden provocar compromiso en su funcionamiento, o robar información.

Hardware: Cualquier elemento activo que forme parte de la Infraestructura de Comunicación y Sistemas de Información existentes, tales como Equipos de Cómputo, Servidores, Switches, Routers, Access Point, Firewalls, Dispositivos de Almacenamiento como SAN y NAS, Equipos de Videoconferencia, Plantas Telefónicas, y demás relacionados.

Herramientas de administración remota (RAT por sus siglas en inglés): Es un software, que permite tomar control visual, y ejecutar acciones en un equipo remoto; desde un equipo local.

Host: Es el hospedaje o anfitrión, es cualquier computadora o máquina conectada a una red mediante un número de IP (dirección del Protocolo de Internet) definido y un dominio, que ofrece recursos, información y servicios a sus usuarios.

Integridad: La cualidad de salvaguardar la exactitud y estado completo de los activos

Interconexión de Sistemas Abiertos (OSI por sus siglas en inglés): La Organización Internacional para la Estandarización (ISO) ha diseñado el modelo de referencia de Interconexión de Sistemas Abiertos (OSI) que utiliza capas estructuradas. El modelo OSI describe una estructura con siete capas para las actividades de red.

Internet Control Message Protocol (ICMP): Es una red de protocolo que es responsable de reportar errores a través de la generación y envío de mensajes a la dirección IP de origen cuando hay problemas de red que son encontrados por el sistema.

Malware (Código Malicioso): Cualquier programa que se instala en un sistema operativo, cuyo fin es interferir con el correcto funcionamiento de este.

Malware polimórfico: Es lo mismo que el malware, con la característica que cambia una parte de su código, pero otra permanece igual en cada cambio, para no ser detectado.

Phishing: Es una técnica de ciberdelincuencia que utiliza el fraude, el engaño y el timo para manipular a sus víctimas y hacer que revelen información personal confidencial.

Plataforma tecnológica: es un conjunto de normas, herramientas de hardware y software que deben permitir:

a. Garantizar la conectividad e interoperabilidad entre las instituciones.
b. Permitir el funcionamiento y desarrollo de sistemas institucionales.
c. Capacidad de trabajo interactivo entre usuarios mediante la implementación de sistemas colaborativos por medios electrónicos.

Polimórfico: propiedad por la que es posible enviar mensajes sintácticamente iguales a objetos de tipos distintos. El único requisito que deben cumplir los objetos que se utilizan de manera polimórfica es saber responder al mensaje que se les envía.

Ransomware: Es un malware, que busca impedir el acceso de los recursos del dispositivo, por parte del usuario, para extorsionarlo y presionarlo a pagar un rescate.

Roaming: Capacidad de enviar y recibir llamada en redes móviles fuera del área de servicio local.

Rogueware: Es un malware, que intenta hacerse pasar por otra aplicación verdadera mediante nombre o apariencia.

SAP (System Applications and Products in Data Processing): Es un sistema informático que utilizan las empresas para administrar correctamente las diferentes acciones de la empresa como la producción, la logística, el inventario, los envíos y la contabilidad.

Scareware: Es un malware, que se adquiere mediante publicidad engañosa, o amenazas inexistentes.

Script: Es un guión que dirige una escena o secuencia. En programación el script contiene instrucciones escritas en código que sirven para ejecutar diversas funciones dentro de un programa.

Seguridad: Mecanismo que garantiza algún buen funcionamiento, previniendo que este falle, se frustre o se violente.

Seguridad informática: Todo mecanismo que garantiza el buen funcionamiento de los servicios informáticos de la empresa, previniendo que estos fallen, se frustren o se violenten.

Servidores: Software que se instala en un sistema operativo, para atender consultas de los clientes. Puede atender consultas locales, como consultas remotas, para lo cual es necesario que esté conectado en red.

Sistema de gestión: El conjunto de elementos (personas, sistemas manuales o automatizados, normativa, equipos y otros) que interactúan de manera sistémica para el logro de la adecuada gestión institucional en términos de eficiencia y eficacia.

Sistema de gestión de la seguridad de la información: La parte del sistema de gestión global, basada en un enfoque hacia los riesgos, para establecer, implementar, operar, dar seguimiento, revisar, mantener y mejorar la seguridad de la información, para ayudar a alcanzar los objetivos organizacionales.

Sistema de información: Aplicación o herramienta informática que le permite al usuario ingresar, almacenar, procesar y obtener información, de manera automatizada.

Site: En lo referente a internet se refiere a un sitio Web.

Software: Conjunto de programas digitales, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

Spam: Es cualquier forma de comunicación no solicitada que se envía de forma masiva (correo electrónico masivo no solicitado). Sin embargo, el "spamming" también existe a través de mensajes instantáneos, de texto (SMS), redes sociales o incluso mensajes de voz. Enviar spam es ilegal.

Spyware: Es un malware, que se instala en el equipo permaneciendo oculto, que le permite seguir y obtener información en línea de la actividad del usuario; algunas más avanzadas, pueden activar micrófonos y cámaras sin que el usuario se entere.

Troyano: Es un malware que tiene la característica de asemejarse a un código legítimo, para pasar inadvertido, cuyo objetivo no es dañar el funcionamiento del equipo, sino tener acceso a él remotamente.

Virtual private network (VPN): Es una herramienta digital que redirige tu tráfico de internet a través de un túnel seguro, ocultando la dirección IP y encriptando los datos. Así es como una VPN mantiene los datos privados y protege frente a ciberataques potenciales.

Virus: Es un malware, con la capacidad de replicarse, que es desencadenado por una acción del usuario.

Procedimiento de clasificación de la información

Objetivo

Establecer, aplicar y clasificar las categorías de la información, tanto la impresa como la electrónica, de los sistemas informáticos que son administrados por la UNAD, y las plataformas de información y comunicación.

Procedimiento general de clasificación de información

Toda la información gestionada por la UNAD, se clasifica en tres grupos, con base en su contenido. Estos grupos corresponden a:

1. Información confidencial.
2. Información para uso interno.
3. Información para uso público.

A continuación, se detalla la normativa para clasificar la información en cada uno de estos grupos:

Información confidencial

Este grupo de información posee un alto nivel de restricción para su acceso. Es de uso restringido para un grupo específico de personas, definido en forma explícita por la vicerrectoría del área responsable de la recopilación o generación de esa información.

Dicha información no puede ser divulgada a personas que no sean las autorizadas, por tener como consecuencia graves daños para la institución, o por el concorcio relacionado con la UNAD. Estos daños pueden significar el comprometer la imagen institucional, el relacionamiento con otras instituciones y oportunidades de negocios entre otros aspectos.

El carácter de información confidencial será dado por la instancia de la Administación que maneje esta información con base en criterios técnicos justificados. Los datos personales se consideran información confidencial.

Información para uso interno

Este grupo de información no es de alcance público y posee un nivel medio de restricción para su acceso, la misma es gestionada a través de la plataforma tecnológica de información y comunicación de la UNAD, misma que es de uso para el personal previamente autorizado. Esta información no puede ser divulgada por tener como consecuencia daños menores para la UNAD, o para el consorcio.

El carácter de información para uso interno será dado por la instancia de la UNAD, que administre esta información con base en criterios técnicos justificados.

Información para uso público

Esta información puede ser usada por cualquier usuario dentro de la Institución. La divulgación de esta no provoca daños la UNAD, o para el consorcio, no compromete la imagen institucional, la relación con otras instituciones.

El carácter de información para uso público será dado por la instancia de la UAND, que administre esta información con base en criterios técnicos justificados.

Almacenamiento de la información

Información confidencial

Los documentos en formato electrónico deben ser almacenados en la carpeta dentro del directorio correspondiente de la unidad responsable en el File Server. Los documentos impresos que sean considerados confidenciales, deben ser almacenada en una caja fuerte, en un mueble de seguridad, o en un mueble metálico bajo llave.

Información para uso interno

Los documentos en formato electrónico pueden ser almacenados en el File Server o en la Intranet. Los documentos impresos que sean considerados confidenciales, deben ser almacenados en una caja fuerte, en un mueble de seguridad, o en un mueble metálico bajo llave.

Información para uso público

Los documentos en formato electrónico o impreso clasificados como uso público, pueden ser almacenados sin restricciones y se puede publicar en el Sitio Web de la UNAD y redes sociales.

Tránsito o distribución de la información

La distribución de los documentos internos debe estar controlada a través de un mecanismo que asegure el tratamiento adecuado de la información entregada y es aplicado el criterio del responsable de este en la decisión final de entrega a terceros. No se restringe la entrega de ningún tipo de documento público.

Procedimiento de seguridad de la información

Objetivo

Establecer las prácticas para garantizar que toda la información contenida en los repositorios y sistemas informáticos que son administrados por la UNAD, se capta, mantiene, trata y desecha conforme a las mejores prácticas de seguridad de la información.

Procedimiento general de seguridad de la información

La UNAD tendrá la obligación de mantener la seguridad y confidencialidad de la información de la que es responsable, aplicando medidas técnicas, digitales, análogas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. Las medidas se adoptarán teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, alcance, contexto y fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

Se establece para estos fines una estructura de normalización, seguimiento, control y mejora del Sistema de Seguridad de la Información Institucional mediante una seguridad física y estructural basada en las mejores prácticas, con el fin de asegurar la protección de los activos de información de usos no autorizados, modificación, daños o destrucción accidental o intencional.

Revisión de los servicios de tecnologías de información y comunicación

El equipo de tecnología, realizará una revisión de los servicios de tecnología de información que aplica para la Sede y la Extensión o del Consorcio en el caso de los sistemas o servicios tecnológicos corporativos. En el caso del consorcio que cuente con servicios específicos, la administración deberá velar su respectiva verificación y gestión tecnológica. Tanto para el caso de los servicios tecnológicos corporativos, así como los específicos ya sea la UNAD o el consorcio, esta revisión deberá realizarse al menos una vez al año.

La UNAD, deberán considerar en sus revisiones, los siguientes aspectos:

1. La especificación del periodo de conservación de cada uno de los activos de información identificados.
2. Especificar claramente el responsable de cada activo de información.
3. Especificar los controles del proceso que garantizan el cumplimiento de los niveles de confidencialidad, integridad y disponibilidad de cada activo de información.
4. Para aquellos activos cuyo nivel de confidencialidad corresponda a los niveles de máxima seguridad, asegurar que se incluyen como parte del inventario de activos de Seguridad de la Información.
5. El tratamiento de la información del Instituto tendrá las siguientes características de: confidencialidad, integridad, disponibilidad y seguridad.

Registro y gestión de eventos de seguridad

La UAND cuenta con mecanismos para detectar actividades sospechosas, no autorizadas y posibles violaciones en el uso de los sistemas de información provistos por la institución. La UNAD, implementa medidas para detectar y alertar de potenciales incidentes de seguridad que puedan afectar los activos de información del CONSORCIO, de acuerdo con el Procedimiento de gestión de incidentes de seguridad, contenido en el presente Manual, en el caso de los servicios de tecnologías corporativos; en el caso específico, las representaciones deberán de implementar las medidas correspondientes.

La UNAD vela por el respeto de los siguientes lineamientos:

Almacenamiento de forma precisa y consistente de las bitácoras que considere relevantes para colaborar en análisis posteriores que colaboren en el reforzamiento de los controles de seguridad.

Las bitácoras de los servidores deben al menos tener la retención que se indica a continuación:

Controladores de Dominio, 1 mes.

Bases de Datos, 3 meses.

Servidores ubicados en la DMZ que publican contenido en Internet, 1 mes.

Servidores

a. Usuario y/o máquina que generó el evento.

b. Fecha y hora en que se generó el evento.

c. Tipo de evento o servicio.

d. Intentos fallidos y exitosos de acceso al sistema.

e. Intentos fallidos y exitosos de acceso a los recursos del sistema.

f. Uso de privilegios elevados.

g. Uso de utilidades y aplicaciones.

h. Cambios en las configuraciones de sistema.

i. Intentos de acceso y modificación de bitácoras.

Equipo de Red

a. Origen del evento (dirección IP).

b. Descripción del evento.

c. Si la conexión fue permitida o denegada.

d. Fecha y hora del evento.

Máquinas de escritorio

a. Modificaciones a las configuraciones del usuario.

b. Uso de utilidades y aplicaciones.

c. Uso de privilegios elevados.

d. Intentos fallidos y exitosos de acceso al sistema.

e. Registro de intentos fallidos y exitosos de acceso a los recursos de información.

Recolección de Información

Actividades relacionadas con la recolección de información de acceso restringido, confidencial o datos personales, para uso posterior en actividades maliciosas en contra de la Institución o las personas físicas o jurídicas. Entre las cuales está:

a. La existencia del objetivo, y el entendimiento de la topología de red que lo rodea, así como la comunicación del objetivo con otros equipos.

b. Vulnerabilidades existentes en el objetivo, o en el ambiente de red donde se encuentra las cuales podrían ser explotadas.

c. Registros de DNS o transferencias entre zonas DNS.

d. Tráfico de reconocimiento ICMP para determinar qué equipos están activos y respondiendo.

e. Identificación de características del sistema (sistema operativo, versiones).

f. Escaneo de puertos de red disponibles en el sistema para identificar servicios relacionados.

g. Escaneo de uno o más servicios vulnerables en un rango de direcciones IPs disponibles.

h. Eventos de fuga de información o modificación no autorizada de la información.

i. Robo de propiedad intelectual perteneciente a la institución.

j. Brechas en los sistemas de bitácoras, borrado de bitácoras y fuga de la información. k. Robo de información criptográfica detectable.

Alteración datos personales

Actividades relacionadas con la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma.

Severidad del incidente

Si el evento reportado se puede catalogar como incidente de seguridad se procede a determinar de acuerdo con las siguientes descripciones la severidad del incidente reportado.

Procedimiento de prevención, detección y corrección de virus

Implementar las acciones para prevenir, detectar y corregir los virus informáticos en la plataforma tecnológica del Instituto.

Este procedimiento aplica a todas las estaciones de trabajo (computadores y portátiles) conectadas o que deseen conectarse a la red.

Procedimiento para la prevención, detección y corrección de virus

Toda computadora y portátil perteneciente al dominio de red la UNAD, debe tener instalado el antivirus corporativo.

2. No se permitirá la instalación de antivirus que no sea el corporativo.
3. El área de Soporte Redes en la GTIC-AD es la responsable de la administración del software antivirus corporativo y velará porque el proceso de actualización de versiones se lleve a cabo sin inconvenientes.
4. El área de Soporte TIC de la UNAD en la Sede es responsable de configurar correctamente el antivirus en las estaciones de trabajo. En el caso de las Representaciones el Administrador es el encargado, en caso de tercerizar este servicio, el Administrador es el responsable de coordinar con UNAD, para velar por el cumplimiento de las disposiciones institucionales en esta materia.

Procedimiento de conexión de Acceso Remoto

Definir normas para la conectividad desde equipos y/o redes del exterior hacia la red de la Universidad Adventista Dominicana (UNAD).

Este procedimiento aplica a todo usuario autorizado a utilizar el acceso por la Red Virtual Privada a la plataforma institucional.

1. El área de Soporte Redes es el único autorizado en proveer los mecanismos para establecer las conexiones remotas.
2. El único servicio de acceso remoto permitido hacia la red institucional es a través de la red privada virtual (VPN).
3. Las conexiones de VPN hacia la red institucional, deben controlarse a través de un nombre de usuario y clave.
4. . Cada usuario podrá tener una única conexión activa por VPN.
5. Es responsabilidad de los usuarios autorizados que utilicen el acceso remoto a las redes de la Institución, asegurarse de tener las mismas consideraciones como si estuvieran directamente conectados a la red de la Institución.
6. Todos los equipos que se conecten a las redes internas de la UNAD, a través de conexión remota, deben tener su antivirus al día.
7. El usuario autorizado no deberá proporcionar información de acceso remoto a ninguna otra persona.
8. En caso de que se trate de conexiones temporales, se deberá indicar en la solicitud la fecha en que debe finalizar el permiso de acceso a la VPN institucional.

Procedimiento de control de acceso físico al Data center

Establecer los lineamientos que deben ser considerados para el control de acceso al Centro de datos del Instituto y garantizar el resguardo de la información y la continuidad de los servicios de red bajo estrictas medidas de seguridad.

Esta política aplica a todos quienes trabajen en la UNAD, personal externo y visitas autorizadas, a la hora de ingreso al centro de datos.

Procedimiento para la administración de claves de usuario

1. El perímetro de seguridad del área del centro de datos deberá estar claramente definido, la ubicación y la resistencia de cada uno de los perímetros dependerán de los requisitos de seguridad de los activos dentro del perímetro y de los resultados de una evaluación de riesgos.
2. El perímetro del centro de datos deberá tener solidez física (por ejemplo, no debe tener zonas que puedan derribarse fácilmente); los muros externos del lugar deben ser sólidos y todas las puertas exteriores deberán estar convenientemente protegidas contra accesos no autorizados, mediante mecanismos de control, por ejemplo, barreras, alarmas, cerraduras, etc., puertas y ventanas deberán estar bloqueadas cuando se encuentren descuidadas.
3. Cualquier visitante incluyendo funcionarios, personal de contrato y empleados de terceros deberán utilizar algún tipo de identificación visible.
4. Los derechos de acceso a las áreas seguras deben ser regularmente revisados y actualizados, y revocados cuando sea necesario.
5. Se deben tomar en cuenta las regulaciones y normativas pertinentes en materia de salud y seguridad vigentes.

6. Se debe tomar en consideración cualquier amenaza de seguridad presentada por las instalaciones vecinas, por ejemplo, incendios, inundaciones o explosiones.
7. Solo personal autorizado puede ingresar al centro de datos, el acceso de personal externo al centro de datos debe quedar registrado, detallando motivo, nombre y apellido, identificación de la empresa, fecha, hora de entrada/ salida y quien autoriza el ingreso.
8. El ingreso al centro de datos debe tener acceso restringido, mediante autenticación por clave y tarjeta de acceso.
9. La clave de ingreso al centro de datos será definida por el usuario junto con el encargado de seguridad perimetral directamente en el sistema de acceso al centro de datos. Esta clave puede tener hasta un máximo de 6 a 8 dígitos.
10. El centro de datos debe estar protegido por puertas de seguridad que resistan fuego, intentos de ingreso a la fuerza, etc.
11. La puerta del centro de datos debe estar equipada con dispositivos que la cierren automáticamente.
12. Los materiales peligrosos o combustibles deberán ser almacenados a una distancia prudente de al menos 25 metros de un área segura. Los suministros a granel tales como los materiales de oficina no deben almacenarse dentro de un área segura.
13. El equipo de reserva y los medios de respaldo deberán estar ubicados a una distancia prudente para evitar daños producto de un desastre que afecten al emplazamiento principal.
14. No es permitido el ingreso de comidas o líquidos al centro de datos ya que puedan dañar la integridad de los equipos.

15. No se permite fumar dentro del centro de datos.
16. El centro de datos debe tener detectores de humo y equipo para mitigar incendios.
17. No se permiten las conexiones en cadena de varias Unidades de Distribución Energética (PDU por sus siglas en inglés) conocidas como regletas. Esto aumenta el riesgo de ocasionar un incendio y una potencial sobrecarga de los circuitos eléctricos, resultando en la pérdida de energía del PDU o del circuito completo.
18. Todos los elementos de soporte, tales como electricidad, abastecimiento de agua, aguas residuales, calefacción/ventilación, y aire acondicionado deberán ser adecuados para los sistemas que están apoyando. Los elementos de soporte deberán ser examinados regularmente y probados adecuadamente de manera de asegurar su funcionamiento apropiado y reducir cualquier riesgo de mal funcionamiento o falla.
19. . Deberá existir un suministro eléctrico apropiado conforme con las especificaciones del fabricante del equipo.
20. Se deberá contar con una fuente de energía ininterrumpida (UPS) para asegurar el correcto apagado o el funcionamiento continuo del equipo que soporta las operaciones críticas del negocio.
21. Los equipos de UPS y los generadores se deberán inspeccionar regularmente para asegurar que tienen la capacidad requerida y probarlos de acuerdo con las directrices del fabricante.
22. El equipo de telecomunicaciones deberá estar conectado con el proveedor al menos a través de dos rutas distintas para prevenir fallas en el servicio de una de las rutas de conexión imposibilitando los servicios de voz. Los servicios de voz se deberían

adecuar para alcanzar los requisitos legales locales para comunicaciones de emergencia.

23. Se deberán adoptar controles para reducir al mínimo el riesgo de amenazas físicas potenciales, por ejemplo, hurto, fuego, explosivos, humo, inundaciones (o falta de suministro de agua), polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, interferencia de las comunicaciones, radiación electromagnética y vandalismo.
24. Las condiciones ambientales, tales como temperatura y humedad, deberán ser supervisadas para verificar que las mismas no afectan negativamente el funcionamiento de las instalaciones de procesamiento de la información. Esta supervisión se realizará de forma diaria al inicio y al final de la jornada laboral y se registrará la temperatura y la humedad relativa reportada por el equipo de monitoreo.
25. Se deberán colocar pararrayos sobre todos los edificios y se deberán aplicar filtros de protección contra rayos a todas las líneas entrantes de energía y de comunicaciones.
26. Se deberán utilizar marcas claramente identificables en cables y equipo para reducir al mínimo los errores de manejo, tales como conexiones accidentales erróneas de los cables de red.
27. Se deberá utilizar una lista documentada de las conexiones para reducir la posibilidad de errores.
28. El equipo que se encuentra dentro del centro de datos deberá recibir el mantenimiento necesario de acuerdo con los niveles de servicio establecidos en el contrato de mantenimiento.

29. Sólo el personal de mantenimiento debidamente autorizado podrá realizar reparaciones y mantenimiento a los equipos.
30. Sólo el personal de mantenimiento debidamente autorizado podrá realizar reparaciones y mantenimiento a los equipos.
31. Se deberán implementar los controles adecuados en los casos en que sea necesario dar mantenimiento a equipos que contengan información confidencial, de manera que la información se mantenga convenientemente resguardada.
32. Se deberá cumplir con todos los requisitos impuestos por pólizas de seguros.

Procedimiento para el uso de dispositivos móviles

Objetivo

1. Establecer y asegurar la aplicación de los criterios esenciales sobre el uso de los dispositivos móviles provistos a los funcionarios del Instituto Interamericano de Cooperación para la Agricultura (IICA), de manera que se haga un uso conveniente y razonable de este tipo de recursos institucionales.

Procedimiento para para el uso de dispositivos móviles

2. Cada dispositivo móvil institucional es asignado mediante unas reglas a una persona responsable quien será garante de su custodia y buen uso.

El uso del dispositivo es exclusivo de la persona responsable, excepto en los casos en que se designe el dispositivo como de uso común para una respectiva dependencia, esto con el fin de evitar usurpación de identidad, mal uso o fuga de información institucional.

3. Los dispositivos móviles institucionales independientemente de su ubicación física deben estar bien resguardados, por parte de la persona responsable, de manera que se minimice al máximo la exposición a daños, pérdida o robo.

Acceso al correo electrónico

La cuenta de correo electrónico de los usuarios será definida como nombre.apellido@unad.edu.do El identificador (ID) del usuario estará compuesto por nombre.apellido, en caso de que ya exista, se utiliza nombre.nombre2.apellido ó en su defecto nombre.apellido.apellido2.

Cada vez que se ingrese o elimine un usuario de correo, la acción será registrada en el sistema automatizado de registro de solicitudes.

Acceso a la red

a. A la red institucional de la UNAD y el CONSORCIO, podrán ingresar únicamente los usuarios autorizados, quienes deberán superar el proceso de autenticación de Windows para acceder a la red institucional.
b. La clave definida por el equipo de tecnología (soporte técnico), deberá ser registrada con la IP-MAC a una herrienta de control de todos los dispositivos con su nombre de usuaruio, nombre red(V-lan), matrícula, nombre usuario o nombre del visitante y estará compuesta únicamente por letras y/o números.

Acceso a intranet

- Cada usuario institucional podrá ingresar a la intranet utilizando el usuario de correo electrónico.
- Para acceder a la intranet institucional el usuario podrá utilizar cualquier navegador, sin embargo, se recomienda utilizar Microsoft Edge o Google Chrome para que tenga acceso a todas las funcionalidades del sitio.

- La dirección (URL) será facilitada por el servidor de la UAND a los usuarios, misma que deberá ser ingresada automática en el navegador para que puedan ingresar a la intranet institucional.

Acceso a los sistemas de información

Las aplicaciones que se utilizan mediante la intranet, validarán la cuenta y contraseña del usuario de intranet, es decir, para que el usuario acceda al sistema debe ingresar a la intranet con su ID y clave y desde ahí podrá acceder a los sistemas para los que posea las autorizaciones correspondientes.

Las aplicaciones de escritorio (que no están en intranet), validarán su ingreso de acuerdo al ID y clave de red, esto significa que el usuario desde el escritorio de su PC, podrá ingresar a los diferentes sistemas indicando para cada uno, el mismo ID y clave que utiliza en la red. Si la clave de red es modificada, para acceder a los sistemas el usuario deberá utilizar la nueva clave, sin ejecutar ningún paso adicional.