

RESOLUCION C. S. N° 132

JOSÉ C. PAZ, 09 NOV 2022

VISTO:

El Estatuto aprobado por Resolución del MINISTERIO DE EDUCACIÓN N° 584/2015, la Resolución C.S N° 202/2019, la Resolución CE N° 1669/2022 del Comité Ejecutivo del Consejo Interuniversitario Nacional y, el Expediente 1194/2022 del registro de esta UNIVERSIDAD, y

CONSIDERANDO

Que la generación de conocimiento constituye una función sustantiva de esta UNIVERSIDAD, orientada a la contribución a los procesos productivos y destinada a la equidad, a la inclusión, y al avance de la ciencia en todas sus dimensiones, propendiendo a generar espacios académicos específicos que organicen esta actividad y promoviendo el trabajo interdisciplinario (ver Art. 15 del ESTATUTO UNIVERSITARIO)

Que el conocimiento es uno de los activos más importantes de las Instituciones y se adquiere gracias al análisis y el proceso de los datos e información que se generan en archivos digitales, papeles o en bases de datos a través del uso de sistemas informáticos, con el fin de dar cumplimiento a la misión estratégica y que por lo tanto además de la información generada por las funciones académica, de investigación y de extensión, la información de gestión también constituye un activo de valor sustancial para esta UNIVERSIDAD.

UNPAZ
M

Que a través de la Decisión Administrativa 641/2021 de la Jefatura de Gabinete de Ministros “Requisitos mínimos de Seguridad de la Información para Organismos del Sector Público Nacional”, se promueve una conducta responsable en materia de ciberseguridad en organismos del Estado, estableciendo un marco organizativo y operacional respecto de medidas a tomar para el fortalecimiento de la seguridad de los sistemas, datos y servicios prestados.

Que en el actual contexto de transformación digital en el que se encuentran avanzando las Instituciones Universitarias Públicas, se hace indispensable para su organización velar por la seguridad de su información, implementando medidas y controles a fines de asegurar su integridad, confidencialidad y disponibilidad.

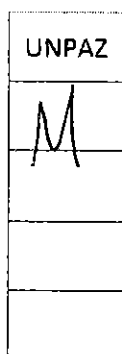
Que en línea con la norma citada anteriormente, la Comisión de Conectividad y Sistemas de Control del Consejo Interuniversitario Nacional (CIN) creó bajo Resolución CE 1620/2021 la Subcomisión de Ciberseguridad.

Que la mencionada Subcomisión realizó una sistemática labor para conocer el estado de situación de la ciberseguridad de las Instituciones Universitarias Públicas.

Que como resultado del trabajo colectivo la Subcomisión de Ciberseguridad ha producido un documento denominado “Políticas de Seguridad de la Información” en las instituciones universitarias nacionales y una guía de instrucciones del documento.

Que el Comité Ejecutivo del Consejo Interuniversitario Nacional (CIN) aprobó por Resolución CE 1669/2022 el documento denominado “Políticas de Seguridad de la Información”.

Que en estrecha vinculación con lo anteriormente expuesto, la Resolución del CONSEJO SUPERIOR N° 202/2019 establece que la SECRETARÍA DE INFORMÁTICA E INNOVACIÓN TECNOLÓGICA coordina las acciones de planificación de



infraestructura de redes, comunicaciones, y de seguridad de la información, a través de las cuales implementa medidas y controles con la finalidad de asegurar la integridad, confidencialidad y disponibilidad de los sistemas, incluyendo software, hardware, información que se está procesando, está almacenada o se está transmitiendo.

Que en concordancia con la Resolución CE 1669/2022 mencionada ut supra es necesario encomendar a la SECRETARÍA DE INFORMÁTICA E INNOVACIÓN TECNOLÓGICA de esta UNIVERSIDAD a que inicie, de manera paulatina y en forma progresiva, las acciones necesarias tendientes a dar cumplimiento con lo establecido en dicha normativa, que como anexo I se acompaña a la presente.

Que la SECRETARIA GENERAL y la SECRETARÍA DE INFORMÁTICA E INNOVACIÓN TECNOLÓGICA han tomado debida intervención.

Que la DIRECCIÓN DE ASUNTOS JURÍDICOS de la SECRETARÍA LEGAL Y TÉCNICA ha tomado la intervención de su competencia.

Que la presente medida se adopta en ejercicio de las atribuciones conferidas por el artículo 63 inciso x) del Estatuto de la UNIVERSIDAD, aprobado por Resolución del MINISTERIO DE EDUCACIÓN N° 584/15.

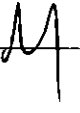
Por ello,

**EL CONSEJO SUPERIOR DE LA
UNIVERSIDAD NACIONAL DE JOSÉ CLEMENTE PAZ**

RESUELVE:

ARTÍCULO 1º.- Adherir a la Resolución CE 1669/2022 del Comité Ejecutivo del Consejo Interuniversitario Nacional (CIN) que como Anexo I se acompaña a la presente.


ARTÍCULO 2º.- Instrúyase a la SECRETARÍA DE INFORMÁTICA E INNOVACIÓN TECNOLÓGICA en articulación con las demás áreas de esta UNIVERSIDAD, a que

UNPAZ


inicie, de manera paulatina y en forma progresiva, las acciones necesarias tendientes a dar cumplimiento con lo establecido en la normativa citada en el artículo precedente.

ARTÍCULO 3º.- Regístrese, comuníquese y publíquese en el Boletín Oficial de esta UNIVERSIDAD. Cumplido, archívese.


LIC. SANTIAGO MONACO
SECRETARIO
CONSEJO SUPERIOR
Universidad Nacional de
José Clemente Paz


ABOG. DARIO KUSINSKY
PRESIDENTE
CONSEJO SUPERIOR
Universidad Nacional de
José Clemente Paz

RESOLUCION C. S. N° 132

UNPAZ

**Comisión de Conectividad y Sistemas de Información
POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. Documento****Resolución CE N° 1669/22
Buenos Aires, 8 de febrero de 2022****VISTO:**

la Decisión Administrativa N° 641/2021 de la Jefatura de Gabinete de Ministros de la Nación;

el documento e instructivo sobre requisitos mínimos de seguridad de la información elaborados por la Subcomisión de Ciberseguridad (Resol. CE N° 1620/21) que funciona en el ámbito de la Comisión de Conectividad y Sistemas de Información; y

CONSIDERANDO:

que la norma citada en el visto refiere a los requisitos mínimos de seguridad de la información para los organismos del sector público nacional;

que en línea con esa decisión, la Comisión de Conectividad y Sistemas de Información de este Consejo creó la Subcomisión de Ciberseguridad (Resol. CE N° 1620/21);

que la subcomisión realizó una sistemática labor a través de encuestas para conocer el estado de situación de la ciberseguridad en las instituciones universitarias públicas;

que los temas relevados refieren a los recursos humanos del área, políticas institucionales de ciberseguridad, gestión aplicada a esas políticas y estructuras con que cuenta el sistema, entre otros tópicos;

que fruto de ese trabajo colectivo ha producido un documento denominado Políticas de seguridad de la Información en las instituciones universitarias nacionales y una guía de instrucciones del documento;

que esa herramienta puede contribuir al desarrollo de la seguridad informática para el conjunto de universidades nucleadas en este Consejo;

que la Comisión de Conectividad y Sistemas de Información recomienda la aprobación del documento;

que este cuerpo considera que debe proveerse de conformidad a lo recomendado.

Por ello,

**EL COMITÉ EJECUTIVO DEL
CONSEJO INTERUNIVERSITARIO NACIONAL
RESUELVE:**



Consejo
Interuniversitario
Nacional

Artículo 1º: Aprobar el documento denominado "Políticas de Seguridad de la Información" y su guía de instrucciones que como anexos I y II se agregan a la presente.

Artículo 2º: Regístrese, dese a conocer y archívese.



MARIO MIGUEL F. GIMELLI
Secretario Ejecutivo



RODOLFO A. TECCHI
Presidente

Política de seguridad de la información de las Instituciones Universitarias Públicas

Introducción

El conocimiento es el activo más importante de las Instituciones Universitarias Públicas. Estos conocimientos se adquieren gracias al análisis y el proceso de los datos e información que se generan en archivos digitales o papeles, con el fin de dar cumplimiento a la misión estratégica. En el contexto de transformación digital en el que se encuentra avanzando las Instituciones Universitarias Públicas, se hace indispensable para su organización tener un control sobre sus archivos, manteniendo y asegurando su integridad, confidencialidad y disponibilidad de la información.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. También se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por fallos técnicos o, porque no, por catástrofes naturales.

Es por ello que esta política establece un marco organizativo y operacional para fortalecer la seguridad de los sistemas, los datos y los servicios prestados por las Instituciones Universitarias Públicas, alineada a la DA 641/21 de la Jefatura de Gabinete de Ministros "Requisitos mínimos de Seguridad de la Información para Organismos".

Las Instituciones Universitarias Públicas debe estar preparada para prevenir, detectar, responder y recuperarse de incidentes.

Prevención

Las Instituciones Universitarias Públicas debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, se deben implementar las medidas mínimas de seguridad propuestas para los organismos nacionales así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estas medidas, los roles y las responsabilidades de seguridad de la información de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de esta Política, las Instituciones Universitarias Públicas debe:

- Establecer los mecanismos para autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.
- Realizar continuas campañas de concientización a los miembros de la comunidad universitaria.

Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, se debe monitorizar la operación de manera continuada para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

La monitorización es especialmente relevante cuando se establecen líneas de defensa. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

Respuesta

Las Instituciones Universitarias Públicas debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en áreas de la entidad o en otros organismos relacionados con las Instituciones Universitarias Públicas.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias Informáticas o CERT (Computer Emergency Response Team) reconocidos a nivel nacional e internacional.

Recuperación

Para garantizar la disponibilidad de los servicios críticos, las Instituciones Universitarias Públicas debe desarrollar planes de continuidad de los sistemas como parte de su plan general de continuidad de negocio y actividades de recuperación.

A partir de lo expuesto hasta aquí se propone el siguiente modelo de Política de Seguridad de la Información para las universidades, que puede ser tomado como base y adaptado por cada institución.

ÍNDICE

Introducción	1
ÍNDICE	3
1. Misión	4
2. Alcance	4
3. Marco Normativo	4
Leyes relacionadas a la ciberseguridad	4
Normativas vinculadas a las funciones de la Dirección Nacional de Ciberseguridad	4
Otras normativas relacionadas a la ciberseguridad	5
4. Organización de la seguridad de la información	5
4.1 Roles, funciones y responsabilidades de seguridad	5
Propietario de la Información	5
Responsables de los servicios	6
Responsable de Seguridad de la Información	6
Responsables de los sistemas	7
Responsable del Área de Recursos Humanos	8
Responsable del Área Informática	8
Responsable del Área Legal o Jurídica	8
Toda la comunidad	9
4.2 Conformación del Comité de Seguridad	9
Funciones y Responsabilidades	9
Coordinador del comité de seguridad de la información	10
5. Gestión de riesgos	10
6. Obligaciones de la comunidad universitaria	11
7. Terceras partes	11
8. Normativas de seguridad	12

1. Misión

Cada Institución Universitaria Pública debe incluir la misión definida en el estatuto.

2. Alcance

La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de las Instituciones Universitarias Públicas.

Debe ser conocida y cumplida por todos los miembros de la Institución, tanto se trate de personal como de estudiantes, desde funcionarios políticos hasta técnicos, y sea cual fuere su nivel jerárquico y su situación de revista; y terceros vinculados a la misma.

3. Marco Normativo

Son de aplicación las leyes y normativas nacionales, provinciales y municipales en relación a seguridad de la información, protección de datos personales, propiedad intelectual y uso de herramientas de comunicaciones informáticas¹.

Leyes relacionadas a la ciberseguridad

- Ley 26.388 de Delito informático
- Ley 25.326 de Protección de Datos Personales
- Decreto Reglamentario N° 1558/2001
- Ley 25.506 de Firma Digital
- Decreto Reglamentario N° 2628/2002
- Ley 26.904 de Grooming

Normativas vinculadas a las funciones de la Dirección Nacional de Ciberseguridad

¹ <https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad/normativa>

- Decisión Administrativa 641/2021. Establece los requisitos mínimos de seguridad de la información para organismos públicos
- Disposición 6/2021. Creación del Comité Asesor para el Desarrollo e Implementación de aplicaciones seguras.
- Disposición 1/2021. Centro Nacional de Respuestas a Incidentes Informáticos (CERT.ar) en el ámbito de la Dirección Nacional de Ciberseguridad.
- Resolución 580/2011. Creación del Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad.
- Disposición ONTI 3/2013. Aprobación de la Política Modelo de Seguridad de la Información.
- Resolución 1523/2019. Definición de Infraestructuras Críticas.

Otras normativas relacionadas a la ciberseguridad

- Decreto 577/2017. Creación del Comité de Ciberseguridad.
- Decreto 480/2019. Modificación del Decreto 577/2017.
- Resolución 829/2019. Aprobación de la Estrategia Nacional de Ciberseguridad.
- Resolución 141/2019. Presidencia del Comité de Ciberseguridad.
- Disposición 8/2021 Guía introductoria para la Seguridad para el Desarrollo de Aplicaciones WEB

4. Organización de la seguridad de la información

Para administrar la seguridad de la información dentro de las Instituciones Universitarias Públicas y establecer un marco gerencial para iniciar y controlar su implementación, se requiere definir roles y distribuir funciones y responsabilidades.

4.1 Roles, funciones y responsabilidades de seguridad

Propietario de la Información

El Propietario de la Información de las Instituciones Universitarias Públicas tendrá las siguientes funciones:

- Clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma,
- Documentar y mantener actualizada la clasificación efectuada

- Establecer los requisitos de la información en materia de seguridad.
- Trabajar en colaboración con el Responsable de Seguridad de la Información y el Responsable del Sistema en el mantenimiento del mismo.
- Decidir los niveles de riesgo residual aceptables que afecten a la información y promover la aplicación de las medidas de seguridad correspondientes.

Responsables de los servicios

El responsable de cada servicio tendrá las siguientes funciones:

- Establecer los requisitos del servicio TIC en materia de seguridad.
- Trabajar en colaboración con el Responsable de Seguridad de la Información y el Responsable de Sistema en el mantenimiento de los sistemas.
- Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes (relacionados con el servicio) y por su cumplimiento.
- Decidir los niveles de riesgo residual aceptables que afecten al servicio y promover la aplicación de las medidas de seguridad correspondientes.

Responsable de Seguridad de la Información

El Responsable de Seguridad de la Información tendrá las siguientes funciones:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas en su ámbito de responsabilidad.
- Realizar y/o promover revisiones periódicas que permitan verificar el cumplimiento de las obligaciones de las Instituciones Universitarias Públicas en materia de seguridad.
- Promover la formación y concientización del personal de las Instituciones Universitarias Públicas en materia de seguridad de la información.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Analizar, completar y aprobar toda la documentación relacionada con la seguridad de los sistemas.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de control implementados en los sistemas.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar el informe periódico de seguridad para el propietario de los sistemas y a las autoridades de las Instituciones Universitarias Públicas, incluyendo los incidentes más relevantes del periodo.

- Aprobar los procedimientos de seguridad elaborados por el Responsable del Sistema.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en los sistemas.
- Elaborar la normativa de seguridad de la información de las Instituciones Universitarias Públicas.
- Promover la capacitación y concientización en el uso de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
- Ser el referente con la autoridad competente en materia de seguridad de la información.
- Convocar a una reunión con el comité de seguridad en caso excepcional ante la ocurrencia de un incidente.

Responsables de los sistemas

El responsable de cada sistema tendrá, dentro de sus áreas de actuación, las siguientes funciones:

- Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, incluyendo las especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y los procedimientos de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Colaborar en el proceso de análisis y gestión de riesgos en el Sistema.
- Elaborar la documentación de seguridad del Sistema.
- Delimitar las responsabilidades de cada área o entidad involucrada en el mantenimiento, explotación, implantación y supervisión del sistema.

- Velar por el cumplimiento de las obligaciones de los administradores de los sistemas de información para que las medidas de seguridad que les afecten en el ámbito de sus competencias sean implementadas.
- Promover la investigación de los incidentes de seguridad que afecten al sistema y comunicar al Responsable de Seguridad de la Información o a quién éste determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Acordar, de ser necesaria, la suspensión del servicio con los propietarios de la información y el responsable del servicio afectado, y el responsable de seguridad de la información.
- Elaborar los procedimientos de seguridad necesarios para la operativa en el sistema.

Responsable del Área de Recursos Humanos

- 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.
- Comunicar la presente Política a todo el personal, 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.
- Promover las campañas de concientización en seguridad de la información.

Responsable del Área Informática

- Cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de las Instituciones Universitarias Públicas.

Responsable del Área Legal o Jurídica

- Verificar el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de las Instituciones Universitarias Públicas con el personal y, en caso de existir, con los terceros. Asimismo, asesorará en materia legal a las Instituciones Universitarias Públicas, en lo que se refiere a la seguridad de la información.

Toda la comunidad

- 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, en los aspectos que correspondan.
- Asistir a las actividades relacionadas con las campañas de concientización y capacitación en seguridad de la información.

4.2 Conformación del Comité de Seguridad

La conformación aquí establecida incluye los roles que son necesarios mínimamente. Cada organización también podrá incluir otros roles que lo conformarán de acuerdo a sus características y funcionamiento.

1. Responsable de seguridad de la información.
2. Responsable(s) de TI (del área central).
3. Responsable del área RRHH.
4. Responsable del área legal.
5. Responsable del área económica.
6. Vicerrector y/o secretario general o a quienes estos deleguen.

El Comité podrá incorporar a sus reuniones a las personas que considere oportuno en función de los temas a tratar.

El Comité propondrá la designación del Coordinador que será aprobado por las autoridades de las Instituciones Universitarias Públicas.

Funciones y Responsabilidades

- Revisar y proponer al Consejo Superior para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información.
- Controlar cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.

- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área².
- Acordar y aprobar metodologías y procesos relativos a seguridad de la información.
- Garantizar que la seguridad sea parte del proceso de planificación de la información; evaluará y coordinará la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Resolver los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad.

Coordinador del comité de seguridad de la información

- Coordinar las acciones del Comité de Seguridad de la Información; y de
- Impulsar la implementación y cumplimiento de la Política de seguridad de la información y de toda la normativa que se desprenda de ella.

5. Gestión de riesgos

La Institución evaluará sus riesgos identificándolos, cuantificándolos y priorizándolos en función de los criterios de aceptación de riesgos y de los objetivos de control relevantes para el mismo. Los resultados guiarán y determinarán la apropiada acción de la dirección y las prioridades para gestionar los riesgos de seguridad de la información y para la implementación de controles seleccionados para protegerse contra estos riesgos.

Se debe repetir la evaluación:

- Regularmente, con la frecuencia que el Comité de Seguridad de la Información defina.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados, o cuando haya un cambio significativo en la plataforma tecnológica.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

² Se refiere a dar curso a las propuestas presentadas por parte de las áreas de acuerdo a sus competencias, elevándolas a la máxima autoridad, a través del Comité de Seguridad, con relación a la seguridad de la información del Organismo. Dichas iniciativas deben ser aprobadas luego por la máxima autoridad del Organismo.

6. Obligaciones de la comunidad universitaria

Todos los miembros de las Instituciones Universitarias Públicas tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa de seguridad desarrollada a partir de ella, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados definidos en el alcance de la presente política.

Se debe establecer un programa de concientización continua para atender a todos los miembros de la comunidad universitaria, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas de información recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

7. Terceras partes

Cuando las Instituciones Universitarias Públicas preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la respuesta ante incidentes de seguridad.

Cuando las Instituciones Universitarias Públicas utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la normativa de seguridad que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la referida normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concientizado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se refiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los propietarios de la Información y de los responsables de los servicios afectados antes de seguir adelante.

8. Normativas de seguridad

La política se desarrollará en normativas específicas que permitan la implementación de la presente política.

Se proponen las siguientes temáticas:

- Gestión de la Política de Seguridad;
- Gestión de la Organización;
- Recursos Humanos;
- Gestión de Activos;
- Gestión de Accesos;
- Criptografía;
- Seguridad Física y Ambiental;
- Seguridad de las Operaciones;
- Seguridad de las Comunicaciones;
- Adquisición, Desarrollo y Mantenimiento de Sistemas;
- Relaciones con Proveedores;
- Gestión de Incidentes de seguridad de la información;
- Gestión de la Continuidad;
- Cumplimiento.

Las normativas a desarrollarse deben incluir las temáticas anteriormente listadas pero no limitarse a las mismas.

Guía para desarrollo e implementación de las normativas de seguridad de la información

Índice

1	Introducción	11
1.1	Alcance	11
1.2	¿Qué es seguridad de la información?	11
1.3	¿Por qué es necesario?	11
1.4	Requerimientos de seguridad	12
1.5	Evaluación de los riesgos de seguridad	13
1.6	Selección de controles	13
1.7	¿Cómo empezar?	13
1.8	Factores críticos de éxito	14
2.	Términos y Definiciones	15
2.0	Terminología	15
2.1	Seguridad de la Información	16
2.2	Evaluación de Riesgos	17
2.2	Tratamiento de Riesgos	17
2.3	Gestión de Riesgos	18
2.4	Comité de Seguridad de la Información	18
2.5	Responsable de Seguridad de la Información	18
2.6	Incidente de Seguridad	18
2.7	Riesgo	18
2.8	Amenaza	19
2.9	Vulnerabilidad	19
2.10	Control	19
3.	Estructura de la guía	19
4.	Evaluación y tratamiento de riesgos	20
	Objetivo	20
4.1	Evaluación de los riesgos de seguridad	20

4.2 Tratamiento de riesgos de seguridad	21
5. Cláusula: Política de Seguridad de la Información	22
Objetivo	22
5.1 Categoría: Política de Seguridad de la información	22
Objetivo	22
5.1.1 Control: Documento de la política de seguridad de la información	23
Organización de la Seguridad	23
Gestión de Activos	23
Recursos Humanos	23
Física y Ambiental	23
Gestión de las Comunicaciones y las Operaciones	23
Gestión de Accesos	24
Adquisición, Desarrollo y Mantenimiento de los Sistemas	24
Gestión de Incidentes de seguridad	24
Gestión de Continuidad	24
Cumplimiento	24
5.1.2 Control: Revisión de la política de seguridad de la información	25
6. Cláusula: Organización	25
Objetivo	25
6.1 Categoría: Organización interna	25
Objetivo	25
6.1.1 Control: Compromiso de la dirección con la seguridad de la información	26
6.1.2 Control: Coordinación de la seguridad de la información	27
6.1.3 Control: Asignación de responsabilidades de la seguridad de la información	28
6.1.4 Control: Autorización para Instalaciones de Procesamiento de Información	28
6.1.5 Control: Acuerdos de confidencialidad	29
6.1.6 Control: Contacto con otros organismos	29
6.1.7 Control: Contacto con grupos de interés especial	30
6.1.8 Control: Revisión independiente de la seguridad de la información	30
6.2 Categoría: Dispositivos móviles y trabajo remoto	30
Objetivo	30
6.2.1 Control: Dispositivos Móviles	31
6.2.2 Control: Trabajo Remoto	32

7. Cláusula: Recursos Humanos	33
Objetivo	33
7.1 Categoría: Antes del empleo	34
Objetivo	34
7.1.1 Control: Funciones y responsabilidades	34
7.1.2 Control: Investigación de antecedentes	34
7.1.3 Control: Términos y condiciones de contratación	34
7.2 Categoría: Durante el empleo	35
Objetivo	35
7.2.1 Control: Responsabilidad de la dirección	36
7.2.2 Control: Concientización, formación y capacitación en seguridad de la información	36
7.2.3 Control: Proceso disciplinario	37
7.3 Categoría: Cese del empleo o cambio de puesto de trabajo	37
Objetivo	37
7.3.1 Control: Responsabilidad del cese o cambio	37
7.3.2 Control: Devolución de activos	38
7.3.3 Control: Retiro de los derechos de acceso	38
8. Cláusula: Gestión de Activos	39
Objetivo	39
8.1 Categoría: Responsabilidad sobre los activos	39
Objetivo	39
8.1.1 Control: Inventario de activos	39
8.1.2 Control: Propiedad de los activos	40
8.1.3 Control: Uso aceptable de los activos	40
8.2 Categoría: Clasificación de la información	41
Objetivo	41
8.2.1 Control: Directrices de clasificación	41
8.2.2 Control: Etiquetado y manipulado de la información	43
8.3 Categoría: Gestión de medios físicos	44
Objetivo	44
8.3.1 Control: Administración de Medios Informáticos Removibles	44
8.3.2 Control: Eliminación de Medios de Información	45
8.3.3 Control: Seguridad de los Medios en Tránsito	45
9. Cláusula: Gestión de Accesos	46

Objetivo	46
9.1 Categoría: Requerimientos para la Gestión de Acceso	46
Objetivo	46
9.1.1 Control: Política de Gestión de Accesos	46
9.1.2 Control: Reglas de Gestión de Acceso	47
9.2 Categoría: Administración de Gestión de Usuarios	47
Objetivo	47
9.2.1 Control: Registración de Usuarios	48
9.2.2 Control: Gestión de Privilegios	49
9.2.3 Control: Gestión de Contraseñas de Usuario	49
9.2.4 Control: Administración de Contraseñas Críticas	50
9.2.5 Control: Revisión de Derechos de Acceso de Usuarios	51
9.3 Categoría: Responsabilidades del Usuario	51
Objetivo	51
9.3.1 Control: Uso de Contraseñas	52
9.4 Categoría: Control de Acceso a Sistemas y Aplicaciones	52
Objetivo	52
9.4.1 Control: Política de Utilización de los Servicios de Red	53
9.4.2 Control: Camino Forzado	53
9.4.3 Control: Autenticación de Usuarios para Conexiones Externas	54
9.4.4 Control: Autenticación de Nodos	54
9.4.5 Control: Protección de los Puertos (Ports) de Diagnóstico Remoto	55
9.4.6 Control: Subdivisión de Redes	55
9.4.7 Control: Acceso a Internet	55
9.4.8 Control: Conexión a la Red	56
9.4.9 Control: Ruteo de Red	56
9.4.10 Control: Seguridad de los Servicios de Red	56
9.5 Categoría: Control de Acceso al Sistema Operativo	57
Objetivo	57
9.5.1 Control: Identificación Automática de Terminales	57
9.5.2 Control: Procedimientos de Conexión de Terminales.	58
9.5.3 Control: Identificación y Autenticación de los Usuarios	58
9.5.4 Control: Sistema de Administración de Contraseñas	59
10. Cláusula: Criptografía	60
Objetivos	60

10.1 Categoría: Cumplimiento de Requisitos Legales	60
Objetivo	60
10.1.1 Control: Política de Utilización de Controles Criptográficos	60
10.1.2 Control: Cifrado	61
10.1.3 Control: Firma Digital	61
10.1.4 Control: Servicios de No Repudio	62
10.1.5 Control: Protección de claves criptográficas	62
10.1.6 Control: Protección de Claves criptográficas: Normas y procedimientos	63
11. Cláusula: Física y Ambiental	64
Objetivo	64
11.1 Categoría: Áreas Seguras	64
Objetivo	64
11.1.1 Control: Perímetro de seguridad física	65
11.1.2 Control: Controles físicos de entrada	66
11.1.3 Control: Seguridad de oficinas, despachos, instalaciones	67
11.1.4	68
11.1.5 Control: Trabajo en áreas seguras	68
11.1.6 Control: Áreas de acceso público, de carga y descarga	69
11.2 Categoría: Seguridad de los equipos	69
Objetivo	69
11.2.1 Control: emplazamiento y protección de equipos	70
11.2.2 Control: Instalaciones de suministro	70
11.2.3 Control: Seguridad del cableado	71
11.2.4 Control: Mantenimiento de los equipos	72
11.2.5 Control: Seguridad de los equipos fuera de las instalaciones	73
11.2.6 Control: Reutilización o retiro seguro de equipos	73
11.2.7 Control: Retirada de materiales propiedad de las Instituciones Universitarias Públicas	73
11.2.8 Control: Políticas de Pantallas Limpias	74
11.2.9 Control: Políticas de Escritorios Limpios	74
12. Cláusula: Seguridad en las Operaciones	75
Objetivo	75
12.1 Categoría: Procedimientos y Responsabilidades operativas	75
Objetivo	75

12.1.1 Control: Documentación de los Procedimientos Operativos	76
12.1.2 Control: Cambios en las Operaciones	77
12.1.3 Control: Planificación de la Capacidad	77
12.1.4 Control: Separación de entornos de desarrollo, pruebas y operacionales	78
12.2 Categoría: Protección contra el malware (código malicioso)	78
Objetivo	78
12.2.1 Control: Control contra el malware (código malicioso)	79
12.2.2 Control: Código Móvil	79
12.3 Categoría: Resguardo (backup)	80
Objetivo	80
12.3.1 Control: Resguardo de la Información	80
12.4 Categoría: Registro y Monitoreo	81
Objetivo	81
12.4.1 Control: Registro de eventos	82
12.4.2 Control: Protección del registro de información	82
12.4.3 Control: Registro del Administrador y del Operador	82
12.4.4 Control: Sincronización de Relojes	83
12.5 Categoría: Control de Software Operacional	83
Objetivo	83
12.5.1 Control: Instalación de software en sistemas operacionales	83
12.6 Categoría: Administración de vulnerabilidades técnicas	84
Objetivo	84
12.6.1 Control: Administración de vulnerabilidades técnicas	84
12.6.2 Control: Restricciones en la instalación de software	85
12.7 Categoría: Consideraciones sobre la auditoría de los sistemas de información	86
Objetivo	86
12.7.1 Control: Controles de auditoría de los sistemas de información	86
13. Cláusula: Gestión de Comunicaciones	87
Objetivo	87
13.1 Categoría: Gestión de la Red	87
Objetivo	87
13.1.1 Control: Redes	87
13.1.2 Control: Seguridad de Servicio de red	88
13.2 Categoría: Transferencia de información	88

Objetivo	88
13.2.1 Control: Procedimientos y controles de intercambio de la información	89
13.2.2 Control: Acuerdos de Intercambio de Información	89
13.2.3 Control: Seguridad de la Mensajería	90
13.2.4 Control: Acuerdos de confidencialidad.	90
14. Cláusula: Adquisición, desarrollo y mantenimiento de sistemas	91
Objetivo	91
14.1 Categoría: Requerimientos de Seguridad de los Sistemas	91
Objetivo	91
14.1.1 Control: Análisis y Especificaciones de los Requerimientos de seguridad	91
14.1.2 Control: Seguridad de servicios aplicativos en redes públicas	92
14.1.3 Control: Protección de servicios de aplicativos	93
14.2 Categoría: Seguridad en los Sistemas de Aplicación	93
Objetivo	93
14.2.1 Control: Validación de Datos de Entrada	94
14.2.2 Control: Controles de Procesamiento Interno	94
14.2.3 Control: Autenticación de Mensajes	95
14.2.4 Control: Validación de Datos de Salidas	95
14.3 Categoría: Seguridad de los Archivos del Sistema	96
Objetivo	96
14.3.1 Control: Software Operativo	96
14.3.2 Control: Protección de los Datos de Prueba del Sistema	97
14.3.3 Control: Cambios a Datos Operativos	97
14.3.4 Control: Acceso a las Bibliotecas de Programas fuentes	98
14.4 Categoría: Seguridad de los Procesos de Desarrollo y Soporte	99
Objetivo	99
14.4.1 Control: Procedimiento de Control de Cambios	99
14.4.2 Control: Revisión Técnica de los Cambios en el sistema Operativo	100
14.4.3 Control: Restricción del Cambio de Paquetes de Software	101
14.4.4 Control: Canales Ocultos y Código Malicioso	101
14.4.5 Control: Desarrollo Externo de Software	101
14.5 Categoría: Gestión de vulnerabilidades técnicas	102
Objetivo	102

14.5.1 Control: Vulnerabilidades técnicas	102
15. Cláusula: Relaciones con Proveedores	103
Objetivo	103
15.1 Categoría: Seguridad de la información en las relaciones con el proveedor	103
Objetivo	103
15.1.1 Control: Política de seguridad de la información para las relaciones con el proveedor	103
15.1.2 Control: Abordar la seguridad dentro de los acuerdos del proveedor	105
15.1.3 Control: Cadena de suministro de tecnologías de la información y comunicaciones	106
15.2 Categoría: Administración de prestación de servicios de proveedores	107
Objetivo	107
15.2.1 Control: Supervisión y Revisión de los servicios del proveedor	107
15.2.2 Control: Gestión de cambios a los servicios del proveedor	108
16. Cláusula: Gestión de Incidentes de Seguridad	108
Objetivo	108
16.1 Categoría: Informe de los eventos y debilidades de la seguridad de la información	108
Objetivo	108
16.1.1 Control: Reporte de los eventos de la seguridad de información	109
16.1.2 Control: Reporte de las debilidades de la seguridad	109
16.1.3 Control: Comunicación de Anomalías del Software	110
16.2 Categoría: Gestión de los Incidentes y mejoras de la seguridad de la información	110
Objetivo	110
16.2.1 Control: Responsabilidades y procedimientos	110
16.2.2 Control: Aprendiendo a partir de los incidentes de la seguridad de la información	111
16.2.3 Control: Procesos Disciplinarios	112
17. Cláusula: Gestión de la Continuidad	112
Objetivo	112
17.1 Categoría: Gestión de continuidad de las Instituciones Universitarias Públicas	112
Objetivo	112
17.1.1 Control: Proceso de Administración de la continuidad de las Instituciones Universitarias Públicas	113

17.1.2 Control: Continuidad de las Actividades y Análisis de los impactos	113
17.1.3 Control: Elaboración e implementación de los planes de continuidad de las Actividades de las Instituciones Universitarias Públicas	114
17.1.4 Control: Marco para la Planificación de la Continuidad de las Actividades de las Instituciones Universitarias Públicas	115
17.1.5 Control: Ensayo, Mantenimiento y Reevaluación de los Planes de continuidad de las Instituciones Universitarias Públicas	116
17.2 Categoría: Redundancias	118
Objetivo	118
17.2.1 Control: Disponibilidad de las instalaciones de procesamiento de la información	118
18. Cláusula: Cumplimiento	119
Objetivos	119
18.1 Categoría: Cumplimiento de Requisitos Legales	119
Objetivo	119
18.1.1 Control: Identificación de la Legislación Aplicable	120
18.1.2 Control: Derechos de Propiedad Intelectual	120
18.1.3 Control: Protección de los Registros de las Instituciones Universitarias Públicas	121
18.1.4 Control: Protección de Datos y Privacidad de la Información Personal	123
18.1.5 Control: Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información	125
18.1.6 Control: Regulación de Controles para el Uso de Criptografía	126
18.1.7 Control: Recolección de Evidencia	126
18.1.8 Control: Delitos Informáticos	127
18.2 Categoría: Revisiones de la Política de Seguridad y la Compatibilidad Técnica	127
Objetivo	127
18.2.1 Control: Cumplimiento de la Política de Seguridad	128
18.2.2 Control: Verificación de la Compatibilidad Técnica	128
18.3 Categoría: Consideraciones de Auditorías de Sistemas	129
Objetivo	129
18.3.1 Controles de Auditoría de Sistemas	129
18.3.2 Control: Protección de los Elementos Utilizados por la Auditoría de Sistemas	130
18.3.3 Control: Sanciones Previstas por Incumplimiento	130
Anexo - Conformación del comité de seguridad de la información.	132

Anexo - Procesos de Seguridad y sus responsables	133
Anexo - Informaciones	134
Anexo - Dispositivos móviles	135
Anexo - Materiales de capacitación	136
Anexo - Política de contraseñas	137
Anexo - Asignación de funciones en controles criptográficos	138
Anexo - Algoritmos de cifrado.	139
Anexo - Métodos de control de acceso físico	140
Anexo - Áreas protegidas y lugares seguros.	141
Anexo - Métodos de detección de intrusos	142
Anexo - Herramientas de auditoría.	143
Anexo - Segregación de ambientes	144
Anexo - Administradores de los planes de contingencia	146
Anexo - Revisión de los planes de contingencia.	147
Anexo - Partidas presupuestarias	148
Anexo - Modelo acuerdo de confidencialidad o no divulgación	149
Modelo 1 - contrato de locación de obra	149
Modelo 2 - Contrato de locación de servicios.	151
Anexo - Activos de información	155
Anexo - Sistemas Sensibles y Críticos	156

1 Introducción

1.1 Alcance

El presente documento es una guía para el desarrollo e implementación de las normativas de seguridad de la información, con el objeto de gestionarla adecuadamente en las Instituciones Universitarias Públicas.

Debe ser tenida en cuenta como marco de referencia para el desarrollo e implementación de políticas y normativas de seguridad de la información en todas las Universidades.

1.2 ¿Qué es seguridad de la información?

La información es un activo que, como otros activos importantes, es esencial y en consecuencia necesita ser protegido adecuadamente.

La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida.

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo de la operación y la operación normal de las Instituciones Universitarias Públicas.

La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión de las Instituciones Universitarias Públicas.

1.3 ¿Por qué es necesario?

La información y los procesos, sistemas y redes de apoyo son activos importantes. Definir, lograr, mantener y mejorar la seguridad de la información puede ser esencial para mantener una eficacia en la operación de las actividades de las Instituciones Universitarias Públicas, observancia legal e imagen.

Las organizaciones y sus sistemas y redes de información enfrentan amenazas de seguridad de un amplio rango de fuentes; incluyendo fraude por computadora, espionaje, sabotaje, vandalismo, fuego o inundación. Las causas de daño como código malicioso, pirateo computarizado o ataques de denegación de servicio se hacen cada vez más comunes, más ambiciosas y cada vez más sofisticadas.

La seguridad de la información es importante tanto para negocios del sector público como privado, y para proteger las infraestructuras críticas. En ambos sectores, la seguridad de la información funcionará como un facilitador; por ejemplo para lograr el e-gobierno para evitar o reducir los riesgos relevantes. La interconexión de redes públicas y privadas y el intercambio de fuentes de información incrementan la dificultad de lograr un control del acceso. La tendencia a la computación distribuida también ha debilitado la efectividad de un control central y especializado.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que se puede lograr a través de medios técnicos es limitada, y debiera ser apoyada por la gestión y los procedimientos adecuados. Identificar qué controles establecer requiere de un planeamiento cuidadoso y prestar atención a los detalles. La gestión de la seguridad de la información requiere, como mínimo, la participación de los diferentes grupos de interés, proveedores, terceros, clientes u otros grupos externos. También se puede requerir asesoría especializada de organizaciones externas.

1.4 Requerimientos de seguridad

Todo comienza con identificar los requerimientos de seguridad. Existen tres fuentes principales de requerimientos de seguridad. Una fuente se deriva de evaluar los riesgos para las Instituciones Universitarias Públicas, tomando en cuenta la estrategia general y los objetivos de las Instituciones Universitarias Públicas.

A través de la evaluación del riesgo, se identifican las amenazas para los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se calcula el impacto potencial.

Otra fuente son los requerimientos legales, reguladores, estatutarios y contractuales que tienen que satisfacer una organización, sus socios comerciales, contratistas y proveedores de servicio; y su ambiente sociocultural.

Otra fuente es el conjunto particular de principios, objetivos y requerimientos funcionales para el procesamiento de la información que una organización ha desarrollado para sostener sus operaciones.

1.5 Evaluación de los riesgos de seguridad

Los requerimientos de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. El gasto en controles debiera ser equilibrado con el daño operacional probable resultado de fallas en la seguridad.

Los resultados de la evaluación del riesgo ayudarán a guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de seguridad de la información, e implementar los controles seleccionados para protegerse contra esos riesgos.

La evaluación del riesgo se debería repetir periódicamente para tratar cualquier cambio que podría influir en los resultados de la evaluación del riesgo.

Se puede encontrar más información de la evaluación de los riesgos de seguridad en la cláusula 4.1 "Evaluando los riesgos de la seguridad".

1.6 Selección de controles

Una vez que se han identificado los requerimientos y los riesgos de seguridad y se han tomado las decisiones para el tratamiento de los riesgos, se deberían seleccionar los controles apropiados y se deberían implementar para asegurar que los riesgos se reduzcan a un nivel aceptable.

La selección de los controles de seguridad depende de las decisiones organizacionales basadas en el criterio de aceptación del riesgo, opciones de tratamiento del riesgo y el enfoque general para la gestión del riesgo aplicado a las Instituciones Universitarias Públicas, y también debieran estar sujetas a todas las regulaciones y legislación nacionales e internacionales aplicables.

1.7 ¿Cómo empezar?

Se pueden considerar un número de controles como un buen punto de inicio para la implementación de la seguridad de la información. Estos se basan en requerimientos legales esenciales o pueden ser considerados como una práctica común para la seguridad de la información.

Los controles considerados como esenciales para una organización desde el punto de vista legislativo incluyen, dependiendo de la legislación aplicable:

- a) protección de datos y privacidad de la información personal,
- b) protección de los registros organizacionales,

c) derechos de propiedad intelectual.

Los controles considerados, práctica común para la seguridad de la información, incluyen:

- a) documento de la política de seguridad de la información;
- b) asignación de responsabilidades de la seguridad de la información;
- c) conocimiento, educación y capacitación en seguridad de la información;
- d) procesamiento correcto en las aplicaciones;
- e) gestión de la vulnerabilidad técnica;
- f) gestión de la continuidad operacional;
- g) gestión de los incidentes y mejoras de la seguridad de la información.

Estos controles se aplican a la mayoría de las organizaciones y en la mayoría de los escenarios.

Se debiera notar que aunque los controles en esta guía son importantes y debieran ser considerados, se debiera determinar la relevancia de cualquier control a la luz de los riesgos específicos que enfrenta las Instituciones Universitarias Públicas. Por lo tanto, aunque el enfoque arriba mencionado es considerado como un buen punto de inicio, no reemplaza la selección de controles basada en la evaluación del riesgo.

1.8 Factores críticos de éxito

La experiencia ha demostrado que los siguientes factores con frecuencia son críticos para una exitosa implementación de la seguridad de la información dentro de una organización:

- a) política, objetivos y actividades de seguridad de información que reflejan los objetivos de las Instituciones Universitarias Públicas;
- b) un enfoque y marco referencial para implementar, mantener, monitorear y mejorar la seguridad de la información que sea consistente con la cultura organizacional;
- c) soporte visible y compromiso de todos los niveles de gestión;
- d) un buen entendimiento de los requerimientos de seguridad de la información, evaluación del riesgo y gestión del riesgo;
- e) comunicación efectiva de la seguridad de la información con todos los directores, empleados y otras partes para lograr conciencia sobre el tema;
- f) distribución de lineamientos sobre la política y los estándares de seguridad de la información para todos los directores, empleados y otras partes involucradas;

- g) provisión para el financiamiento de las actividades de gestión de la seguridad de la información;
- h) proveer el conocimiento, capacitación y educación apropiados;
- i) establecer un proceso de gestión de incidentes de seguridad de la información;
- j) implementación de un sistema de medición que se utiliza para evaluar el desempeño en la gestión de la seguridad de la información y retroalimentación de sugerencias para el mejoramiento.

2. Términos y Definiciones

2.0 Terminología

Área de Seguridad Informática:

Comunidad Universitaria: Se refiere a todas las personas relacionadas con las Instituciones Universitarias Públicas ya sean autoridades, personal o estudiantes en cualquiera de los niveles.

Personal: En esta política el término personal se utilizará para designar a personas con relación laboral con las Instituciones Universitarias Públicas, como así también a contratados, becarios, pasantes y a cualquier persona que realice tareas dentro de las Instituciones Universitarias Públicas, cualquiera sea su forma de vinculación.

Propietario de la información: Toda la información listada en el Anexo - Informaciones es propiedad de las Instituciones Universitarias Públicas. No obstante para la aplicación de la presente política el término Propietario de la Información se refiere al responsable de la Unidad Organizativa que tiene la custodia de la información. El mismo deberá ser un funcionario electo o designado por una autoridad superior, como por ejemplo Decanos o secretarios de rectorado o de facultad. Para ejercer sus funciones deberá ser explícitamente designado por el Comité de Seguridad de la Información y estar incluido en el "Anexo - Informaciones".

Propietario de un activo: Todos los activos listados en el Anexo - Activos de información son propiedad de las Instituciones Universitarias Públicas. No obstante para la aplicación de la presente política el término Propietario de un Activo se refiere al responsable de la Unidad Organizativa que tiene la custodia de la información. El mismo deberá ser un funcionario electo o designado por una autoridad superior, como por ejemplo Decanos o secretarios de rectorado o de facultad. Para ejercer sus funciones deberá ser explícitamente designado por el Comité de Seguridad de la Información y estar incluido en el "Anexo - Activos de información".

Responsable del Área Administrativa: Se refiere al Responsable del Área con capacidad para realizar contratos con terceras partes dentro de cada Unidad organizativa.

Responsable del Área Informática: El o los encargados de las áreas de tecnologías.

Responsable del Área Legal o Jurídica: Director de asuntos jurídicos o función similar.

Responsable del Área de Recursos Humanos: Director de personal o cargo similar.

Responsable de la Seguridad Física:

Unidad Académica: Estructura de la universidad con capacidad de... Como por ejemplo Facultad, Departamento, Secretaría, etc.

Unidad Organizativa: Se usa como sinónimo de Unidad Académica.

2.1 Seguridad de la Información

La seguridad de la información se entiende como la preservación de las siguientes características:

Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deben considerarse los conceptos de:

Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto las Instituciones Universitarias Públicas.

Confiable de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología de la Información: Se refiere al hardware y software operados por las Instituciones Universitarias Públicas o por un tercero que procese información en su nombre, para llevar a cabo una función propia de las Instituciones Universitarias Públicas, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

2.2 Evaluación de Riesgos

Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria de las Instituciones Universitarias Públicas.

2.2 Tratamiento de Riesgos

Proceso de selección e implementación de medidas para modificar el riesgo.

2.3 Gestión de Riesgos

Actividades coordinadas para dirigir y controlar una organización en lo que concierne al riesgo.

NOTA. La gestión de riesgos usualmente incluye la evaluación de riesgos, el tratamiento de riesgos, la aceptación de riesgos y la comunicación de riesgos.

2.4 Comité de Seguridad de la Información

El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de las áreas sustantivas de las Instituciones Universitarias Públicas, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

2.5 Responsable de Seguridad de la Información

Es la persona que cumple la función de impulsar y supervisar el cumplimiento de la presente Política, proponer normativas, políticas complementarias y controles de seguridad y de asesorar en materia de seguridad de la información a los integrantes de las Instituciones Universitarias Públicas que así lo requieran.

2.6 Incidente de Seguridad

Un incidente de seguridad es un evento adverso en un sistema de información, que puede comprometer o comprometer la confidencialidad, integridad y/o disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

2.7 Riesgo

Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impacto.

2.8 Amenaza

Una causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización.

2.9 Vulnerabilidad

Una debilidad de un activo o grupo de activos que puede ser aprovechada por una amenaza.

2.10 Control

Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales, las cuales pueden ser de naturaleza administrativa, técnica, de gestión, o legal. Control es también utilizado como sinónimo de salvaguarda o de contramedida.

3. Estructura de la guía

Este modelo que se divide en dos partes, y guarda la siguiente estructura:

- Cuatro capítulos introductorios, con los términos generales y el establecimiento de la Evaluación y el Tratamiento de los riesgos,
- Catorce cláusulas que abarcan los diferentes aspectos o dominios de la seguridad de la información. Se presentan de manera sistemática y consistente.

Cada cláusula contiene un número de categorías o grupos de controles de seguridad principales. Las catorce cláusulas (acompañadas por el número de categorías de seguridad principales incluidas dentro de cada cláusula) son:

- Política de Seguridad (1);
- Organización (2);
- Recursos Humanos (3);
- Gestión de Activos (3);

- Gestión de Accesos (5);
- Criptografía (1);
- Seguridad Física y Ambiental (2);
- Seguridad de las Operaciones (7);
- Seguridad de las Comunicaciones (2);
- Adquisición, Desarrollo y Mantenimiento de Sistemas (5);
- Relaciones con Proveedores (3);
- Gestión de Incidentes de seguridad de la información (2);
- Gestión de la Continuidad (2);
- Cumplimiento (3).

Por último, por cada categoría, se establece un objetivo y contiene uno o más controles a realizar.

A modo de síntesis se enuncia a continuación la estructura de cada cláusula

- Cláusula o dominio
 1. Objetivos
 2. Normativa
- Categorías
 - Objetivo
- Controles

4. Evaluación y tratamiento de riesgos

Objetivo

Conocer los riesgos a los que se expone las Instituciones Universitarias Públicas en materia de seguridad de la información.

Generar información de utilidad para la toma de decisiones en materia de controles de seguridad.

4.1 Evaluación de los riesgos de seguridad

Las Instituciones Universitarias Públicas evaluará sus riesgos identificándolos, cuantificándolos y priorizándolos en función de los criterios de aceptación de riesgos y de los objetivos de control relevantes para el mismo. Los resultados guiarán y determinarán la

apropiada acción de la dirección y las prioridades para gestionar los riesgos de seguridad de la información y para la implementación de controles seleccionados para protegerse contra estos riesgos.

Se debe efectuar la evaluación de riesgos periódicamente, para tratar con los cambios en los requerimientos de seguridad y en las situaciones de riesgo, por ejemplo: cambios producidos en activos, amenazas, vulnerabilidades, impactos, valoración de riesgos. Asimismo, se debe efectuar la evaluación cada vez que ocurran cambios significativos. Es conveniente que estas evaluaciones de riesgos se lleven a cabo de una manera metódica capaz de producir resultados comparables y reproducibles.

El alcance de una evaluación de riesgos puede incluir a todo las Instituciones Universitarias Públicas, una parte, un sistema de información particular, componentes específicos de un sistema, o servicios. Resulta recomendable seguir una metodología de evaluación de riesgos para llevar a cabo el proceso.

4.2 Tratamiento de riesgos de seguridad

Antes de considerar el tratamiento de un riesgo, las Instituciones Universitarias Públicas debe decidir los criterios para determinar si los riesgos pueden, o no, ser aceptados. Los riesgos pueden ser aceptados si por ejemplo: se evaluó que el riesgo es bajo o que el costo del tratamiento no es económicamente viable para las Instituciones Universitarias Públicas. Tales decisiones deben ser tomadas por las autoridades y debidamente documentadas.

Para cada uno de los riesgos identificados durante la evaluación de riesgos, se necesita tomar una decisión para su tratamiento. Las posibles opciones para el tratamiento de riesgos incluyen:

- a) Mitigar los riesgos mediante la aplicación de controles apropiados para reducir los riesgos;
- b) Aceptar los riesgos de manera objetiva y consciente, siempre y cuando éstos satisfagan claramente la política y los criterios de aceptación de riesgos de las Instituciones Universitarias Públicas;
- c) Evitar los riesgos, eliminando las acciones que dan origen a la ocurrencia de estos;
- d) Transferir los riesgos asociados a otras partes interesadas, por ejemplo: compañías de seguro o proveedores.

Para aquellos riesgos donde la decisión ha sido la mitigación, se buscará reducir los riesgos a un nivel aceptable mediante la implementación de controles, teniendo en cuenta lo siguiente:

- a) requerimientos y restricciones de legislaciones y regulaciones nacionales e internacionales;
- b) objetivos organizacionales;
- c) requerimientos y restricciones operativos;
- d) costo de implementación y operación en relación directa a los riesgos reducidos, y proporcionales a los requerimientos y restricciones de las Instituciones Universitarias Públicas;
- e) la necesidad de equilibrar las inversiones en la implementación y operación de los controles contra el daño que podría resultar de las fallas de seguridad.

Los controles a implementar pueden ser seleccionados del contenido de las cláusulas de esta política, o se pueden establecer nuevos controles para satisfacer necesidades específicas de las Instituciones Universitarias Públicas. Es necesario reconocer que algunos controles pueden no ser aplicables a todo sistema de información o a su ambiente, y podrían no ser aplicables en todos los Organismos.

Se debe recordar que ningún conjunto de controles puede alcanzar la seguridad absoluta. Los controles implementados deben ser evaluados permanentemente para que puedan ser mejorados en eficiencia y efectividad.

5. Cláusula: Política de Seguridad de la Información

Objetivo

Proteger los recursos de información de las Instituciones Universitarias Públicas y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales,

Mantener la Política de Seguridad de las Instituciones Universitarias Públicas actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

5.1 Categoría: Política de Seguridad de la información

Objetivo

Proporcionar a los órganos de gobierno la dirección y soporte para la seguridad de la información en concordancia con los requerimientos, las leyes y regulaciones relevantes. El mismo debe establecer claramente la dirección de la política en línea con los objetivos.

5.1.1 Control: Documento de la política de seguridad de la información

El documento de la política debe ser aprobado por el Consejo Superior de las Instituciones Universitarias Públicas, publicado y comunicado a todo el personal y las partes externas relevantes.

La Política y las normas derivadas se conforman de una serie de pautas sobre aspectos específicos de la Seguridad de la información, que incluyen los siguientes tópicos:

Organización de la Seguridad

Orientado a administrar la seguridad de la información dentro de las Instituciones Universitarias Públicas y establecer un marco gerencial para controlar su implementación.

Gestión de Activos

Destinado a mantener una adecuada protección de los activos de las Instituciones Universitarias Públicas.

Recursos Humanos

Orientado a reducir los riesgos de error humano, comisión de ilícitos contra las Instituciones Universitarias Públicas o uso inadecuado de instalaciones.

Física y Ambiental

Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información de las Instituciones Universitarias Públicas.

Gestión de las Comunicaciones y las Operaciones

Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.

Gestión de Accesos

Orientado a controlar el acceso lógico a la información.

Adquisición, Desarrollo y Mantenimiento de los Sistemas

Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su adquisición, desarrollo y/o implementación y durante su mantenimiento.

Gestión de Incidentes de seguridad

Orientado a administrar todos los eventos que atenten contra la confidencialidad, integridad y disponibilidad de la información y los activos tecnológicos

Gestión de Continuidad

Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.

Cumplimiento

Destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

A fin de asegurar la implementación de las medidas de seguridad comprendidas en esta Política, las Instituciones Universitarias Públicas identificará los recursos necesarios e indicará formalmente las partidas presupuestarias correspondientes, como anexo a la presente Política. Lo expresado anteriormente no implicará necesariamente la asignación de partidas presupuestarias adicionales. (Ver "Anexo - Partidas presupuestarias").

El Consejo Superior de las Instituciones Universitarias Públicas aprobará formalmente la Política y la comunicará a todos el personal, mediante el Responsable del Área de Recursos Humanos y terceras partes relevantes.

5.1.2 Control: Revisión de la política de seguridad de la información

La política de seguridad de la información debe tener un dueño, responsable de las actividades de desarrollo, evaluación y revisión de la política.

La actividad de revisión debe incluir las oportunidades de mejoras, en respuesta a los cambios, entre otros: organizacionales, normativos, legales, de terceros, tecnológicos.

Las mejoras tenidas en cuenta deben quedar registradas y tener las aprobaciones de los responsables.

El Comité de Seguridad de la Información debe revisarla a intervalos planeados y prever el tratamiento de caso de los cambios no planeados, a efectos de mantener actualizada la política.

Asimismo efectuará toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como ser, cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, etc.

6. Cláusula: Organización

Objetivo

Administrar la seguridad de la información dentro de las Instituciones Universitarias Públicas y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

Fomentar la consulta y cooperación con Organismos especializados para la obtención de asesoría en materia de seguridad de la información.

Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información de las Instituciones Universitarias Públicas.

6.1 Categoría: Organización interna

Objetivo

Manejar la seguridad de la información dentro de las Instituciones Universitarias Públicas.

Se debe establecer un marco referencial gerencial o política, para iniciar y controlar la implementación de la seguridad de la información dentro de las

Instituciones Universitarias Públicas.

El Consejo Superior de las Instituciones Universitarias Públicas debe aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implementación de la seguridad en todo las Instituciones Universitarias Públicas.

6.1.1 Control: Compromiso de la dirección con la seguridad de la información

El rector de las Instituciones Universitarias Públicas debe apoyar la seguridad de la información a través de una dirección clara, mostrando compromiso, asignando roles y reconociendo responsabilidades explícitas.

Debe aprobar la política de seguridad de la información, como asimismo revisar los beneficios de la implementación de la misma.

La seguridad de la información es una responsabilidad de las Instituciones Universitarias Públicas compartida por todas las Autoridades políticas del mismo, por lo cual se crea el Comité de Seguridad de la Información. Su integración se indica en el "Anexo - Conformación del comité de seguridad de la información". El Comité estará destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad de la información. El mismo contará con un Coordinador, quien cumplirá la función de impulsar la implementación de la presente Política.

El Comité de Seguridad de la Información estará conformado por los responsables de la Unidades Organizativas y los roles que se indican en el "Anexo - Conformación del comité de seguridad de la información". Este anexo podrá ser modificado con la aprobación del Consejo Superior de las Instituciones Universitarias Públicas.

Este Comité tendrá entre sus funciones:

- a) Revisar y proponer al Consejo Superior de las Instituciones Universitarias Públicas para su aprobación, la Política y las funciones generales en materia de seguridad de la información.
- b) Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- c) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.

- d) Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área¹.
- e) Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
- f) Garantizar que la seguridad sea parte del proceso de planificación informática de las Instituciones Universitarias Públicas.
- g) Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- h) Promover la difusión y apoyo a la seguridad de la información dentro de las Instituciones Universitarias Públicas.
- i) Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información de las Instituciones Universitarias Públicas frente a interrupciones imprevistas.

El Comité de Seguridad de la Información propondrá la designación del Coordinador al rector de las Instituciones Universitarias Públicas, quien deberá aprobar la propuesta.

6.1.2 Control: Coordinación de la seguridad de la información

Tipicamente, la coordinación de la seguridad de la información debiera involucrar la cooperación y colaboración de los Responsables de las Unidades Organizativas, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad, y capacidades especializadas en áreas como seguros, temas legales, recursos humanos, TI o gestión del riesgo. Estas actividades son:

- a) asegurar que las actividades de seguridad sean ejecutadas en conformidad con la política de seguridad de la información;
- b) identificar cómo manejar las no-conformidades;
- c) aprobar las metodologías y procesos para la seguridad de la información; por ejemplo, la evaluación del riesgo y la clasificación de la información;
- d) identificar cambios significativos en las amenazas y la exposición de la información y los medios de procesamiento de la información ante amenazas;
- e) evaluar la idoneidad y coordinar la implementación de los controles de la seguridad de información;
- f) promover de manera efectiva la educación, capacitación y conocimiento de la seguridad de la información a través de toda las Instituciones Universitarias Públicas;

¹ Se refiere a dar curso a las propuestas presentadas por parte de las áreas de acuerdo a sus competencias, elevándolas al Consejo Superior, a través del Comité de Seguridad, con relación a la seguridad de la información de las Instituciones Universitarias Públicas. Dichas iniciativas deben ser aprobadas luego por el Consejo Superior de las Instituciones Universitarias Públicas.

- g) evaluar la información recibida del monitoreo y revisar los incidentes de seguridad de la información, y recomendar las acciones apropiadas en respuesta a los incidentes de seguridad de información identificados.

6.1.3 Control: Asignación de responsabilidades de la seguridad de la información

La asignación de responsabilidades de la seguridad de la información debe ejecutarse en forma alineada a la política de seguridad de la información (ver cláusula 5 política de seguridad de la información).

Las Instituciones Universitarias Públicas deberá contar con un “Responsable de Seguridad de la Información”, quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información de las Instituciones Universitarias Públicas, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática tratados en la presente Política.

El Comité de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación la definición y asignación de las responsabilidades que surjan del presente Modelo.

En el “Anexo - Procesos de Seguridad y sus responsables” se detallan los procesos de seguridad, indicándose en cada caso el/los responsable/s del cumplimiento de los aspectos de esta Política aplicables. Este anexo podrá ser modificado a propuesta del Coordinador del Comité de Seguridad de la Información y con la aprobación del Comité de Seguridad de la Información.

De igual forma, en el “Anexo - Informaciones” se detallan los propietarios de la información que se encuentran en el alcance de la presente política, quienes serán los Responsables de las Unidades Organizativas a cargo del manejo de la misma.

Cabe aclarar que, si bien los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservarán la responsabilidad del cumplimiento de las mismas. La delegación de la administración por parte de los propietarios de la información será documentada por los mismos y proporcionada al Responsable de Seguridad de la Información.

6.1.4 Control: Autorización para Instalaciones de Procesamiento de Información

Los nuevos recursos de procesamiento de información serán autorizados por los Responsables de las Unidades Organizativas involucradas, considerando su propósito y uso, conjuntamente con el Responsable de Seguridad de la Información,

a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad pertinentes.

Las siguientes guías deben ser consideradas para el proceso de autorización:

- a) Cumplir con los niveles de aprobación vigentes en las Instituciones Universitarias Públicas, incluso el responsable del ambiente de seguridad de la información, asegurando el cumplimiento de las políticas y requerimientos.
- b) Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas de las Instituciones Universitarias Públicas.
- c) El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso será evaluado en cada caso por el Responsable de Seguridad de la Información y debe ser autorizado por el Responsable del Área Informática y por el responsable de la Unidad Organizativa a la que se destinen los recursos.

6.1.5 Control: Acuerdos de confidencialidad

Se definirán, implementarán y revisarán regularmente los acuerdos de confidencialidad o de no divulgación para la protección de la información de las Instituciones Universitarias Públicas. Dichos acuerdos deben responder a los requerimientos de confidencialidad o no divulgación de las Instituciones Universitarias Públicas, los cuales serán revisados periódicamente. Asimismo, deben cumplir con toda legislación o normativa que alcance a las Instituciones Universitarias Públicas en materia de confidencialidad de la información.

Dichos acuerdos deben celebrarse tanto con el personal de las Instituciones Universitarias Públicas como con aquellos terceros que se relacionen de alguna manera con su información.

El modelo de acuerdo de confidencialidad o no divulgación se encuentra en el "Anexo - Modelo acuerdo de confidencialidad o no divulgación".

6.1.6 Control: Contacto con otros organismos

A efectos de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad, se mantendrán contactos con Organismos especializados en temas relativos a la seguridad informática existentes, tanto nacionales como internacionales.

El intercambio de información confidencial para fines de asesoramiento o de transmisión de experiencias, sólo se permite cuando se haya firmado un Acuerdo de Confidencialidad previo o con aquellas Organizaciones especializadas en temas

relativos a la seguridad de la Información cuyo personal está obligado a mantener la confidencialidad de los temas que trata.

6.1.7 Control: Contacto con grupos de interés especial

El Responsable de Seguridad de la información será el encargado de coordinar los conocimientos y las experiencias disponibles en las Instituciones Universitarias Públicas a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Éste podrá obtener asesoramiento de otros Organismos. Con el objeto de optimizar su gestión, se habilitará al Responsable de Seguridad de la Información el contacto con las Unidades Organizativas de todas las Áreas de las Instituciones Universitarias Públicas.

Debe considerar ser miembro de grupos de interés especial para:

- a) Adquirir nuevos conocimientos acerca de las mejores prácticas y estar actualizado;
- b) Asegurar que la concientización acerca de la seguridad de la información esté actualizada y completa;
- c) Recibir alertas tempranas, avisos y recomendaciones ante ataques y vulnerabilidades;
- d) Proporcionar vínculos adecuados durante el tratamiento de los incidentes de seguridad de la información.

6.1.8 Control: Revisión independiente de la seguridad de la información

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la información realizará revisiones independientes sobre la vigencia, implementación y gestión de la Política de Seguridad de la Información, a efectos de garantizar que las prácticas de las Instituciones Universitarias Públicas reflejan adecuadamente sus disposiciones.

Estas revisiones deben incluir las oportunidades de evaluación de mejoras y las necesidades de cambios de enfoque en la seguridad, incluyendo políticas y objetivos de control.

Se deben registrar y reportar todas estas actividades.

6.2 Categoría: Dispositivos móviles y trabajo remoto

Objetivo

Asegurar la seguridad de la información cuando se utilizan medios de computación y teletrabajo móviles.

La protección requerida se debe conmensurar con los riesgos que causan estas maneras de trabajo específicas. Cuando se utiliza computación móvil, se deben considerar los riesgos de trabajar en un ambiente desprotegido y se debería aplicar la protección apropiada. En el caso del teletrabajo, las Instituciones Universitarias Públicas debe aplicar protección a la conexión que se utilizará entre el lugar del teletrabajo y las Instituciones Universitarias Públicas.

6.2.1 Control: Dispositivos Móviles

Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información ni la infraestructura de las Instituciones Universitarias Públicas.

Se debe tener en cuenta en este sentido, todos los dispositivos incluidos en el "Anexo - Dispositivos móviles". Este anexo será actualizado con una periodicidad no mayor a 6 (seis) meses por el Responsable de Seguridad de la Información.

Se desarrollarán procedimientos adecuados para estos dispositivos, que abarquen los siguientes conceptos:

- a) La protección física necesaria.
- b) El acceso seguro a los dispositivos.
- c) La utilización segura de los dispositivos en lugares públicos.
- d) El acceso a los sistemas de información y servicios de las Instituciones Universitarias Públicas a través de dichos dispositivos.
- e) Las técnicas criptográficas a utilizar para la transmisión de información clasificada.
- f) Los mecanismos de resguardo de la información contenida en los dispositivos.
- g) La protección contra software malicioso.

La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de pérdida, robo o hurto. En consecuencia debe entrenarse especialmente al personal que los utilice. Se desarrollarán normas y procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles, que contemplarán las siguientes recomendaciones:

- a) Permanecer siempre cerca del dispositivo.
- b) No dejar desatendidos los equipos.
- c) No llamar la atención acerca de portar un equipo valioso.
- d) No poner identificaciones de las Instituciones Universitarias Públicas en el dispositivo, salvo los estrictamente necesarios.
- e) No poner datos de contacto técnico en el dispositivo.

- f) Mantener cifrada la información clasificada.

Por otra parte, se confeccionarán procedimientos que permitan al poseedor del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información de las Instituciones Universitarias Públicas, los que incluirán:

- a) Revocación de las credenciales afectadas
- b) Notificación a grupos de trabajo donde potencialmente se pudieran haber comprometido recursos.

6.2.2 Control: Trabajo Remoto

El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo a las Instituciones Universitarias Públicas.

Para ello, el personal autorizado a realizar trabajo remoto se comprometerá, mediante declaración jurada, a cumplir las normas y procedimientos que se establecerán considerando los siguientes aspectos:

- a) Deberá adecuarse a las condiciones mínimas recomendadas para el lugar físico donde desarrolla sus actividades remotas
- b) Los requerimientos de seguridad de comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de las Instituciones Universitarias Públicas, la sensibilidad de la información a la que se accederá y que pasará a través del vínculo de comunicación y la sensibilidad del sistema interno.
- c) La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo, familia y amigos.
- d) Evitar la instalación / desinstalación de software no autorizado por las Instituciones Universitarias Públicas.

Los controles y disposiciones comprenden:

- a) Proveer de mobiliario para almacenamiento y equipamiento adecuado para las actividades de trabajo remoto en caso de ser necesario.
- b) Definir el trabajo permitido, el horario de trabajo, la clasificación de la información que se puede almacenar en el equipo remoto desde el cual se accede a la red de las Instituciones Universitarias Públicas y los sistemas internos y servicio a los cuales el trabajador remoto está autorizado a acceder.
- c) Proveer de un adecuado equipo de comunicación, con inclusión de métodos para asegurar el acceso remoto.

- d) Incluir seguridad física.
- e) Definir reglas y orientación respecto del acceso de terceros al equipamiento e información.
- f) Proveer el hardware y el soporte y mantenimiento del software.
- g) Definir los procedimientos de respaldos y de continuidad de las operaciones.
- h) Efectuar auditoría y monitoreo de la seguridad.
- i) Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.
- j) Asegurar el reintegro del equipamiento en las mismas condiciones en que fue entregado, en el caso en que cese la necesidad de trabajar en forma remota.

Se implementarán procesos de auditoría específicos para los casos de accesos remotos, que serán revisados regularmente. Se llevará un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.

7. Cláusula: Recursos Humanos

Objetivo

Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos de confidencialidad a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de las Instituciones Universitarias Públicas en el transcurso de sus tareas normales.

Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.

Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

7.1 Categoría: Antes del empleo

Objetivo

Asegurar que el personal, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios.

Las responsabilidades de seguridad deben ser tratadas antes del empleo en las definiciones de trabajo adecuadas y en los términos y condiciones del empleo.

7.1.1 Control: Funciones y responsabilidades

Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo.

Éstas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

Se definirán y comunicarán claramente los roles y responsabilidades de seguridad a los candidatos para el puesto de trabajo durante el proceso de preselección.

7.1.2 Control: Investigación de antecedentes

Se llevarán a cabo controles de verificación del personal en el momento en que se solicita el puesto. Estos controles incluirán todos los aspectos que indiquen las normas que a tal efecto alcanzan a las Instituciones Universitarias Públicas.

Se recomiendan algunos aspectos, no limitantes, de verificación a modo de ejemplo:

- a) Disponibilidad de referencias de carácter satisfactorias
- b) Chequeo del curriculum vitae del postulante
- c) Confirmación de títulos académicos y profesionales mencionados por el postulante
- d) Acreditación de su identidad

7.1.3 Control: Términos y condiciones de contratación

Como parte de sus términos y condiciones iniciales de empleo, el personal, cualquiera sea su situación de revista, firmará un Compromiso de Confidencialidad o

no divulgación, en lo que respecta al tratamiento de la información de las Instituciones Universitarias Públicas. La copia firmada del compromiso debe ser retenida en forma segura por el Área de Recursos Humanos u otra competente.

Asimismo, mediante el Compromiso de Confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

Se desarrollará un procedimiento para la suscripción del Compromiso de Confidencialidad donde se incluirán aspectos sobre:

- Suscripción inicial del Compromiso por parte de la totalidad del personal. Revisión del contenido del Compromiso anualmente.
- Método de re-suscripción en caso de modificación del texto del Compromiso.
- Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información.

Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede de las Instituciones Universitarias Públicas y del horario normal de trabajo.

Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de empleo.

7.2 Categoría: Durante el empleo

Objetivo

Asegurar que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.

Se deben definir las responsabilidades de la gerencia para asegurar que se aplique la seguridad a lo largo de todo el tiempo del empleo de la persona dentro de las Instituciones Universitarias Públicas.

7.2.1 Control: Responsabilidad de la dirección

La dirección solicitará al personal, contratistas y usuarios de terceras partes que apliquen la seguridad en concordancia con las políticas y procedimientos establecidos por las Instituciones Universitarias Públicas, cumpliendo con lo siguiente:

- a) estar adecuadamente informados de sus roles y responsabilidades de seguridad de la información antes de que se les otorgue el acceso a información sensible o a los sistemas de información;
- b) ser provistos de guías para establecer las expectativas de seguridad de su rol dentro de las Instituciones Universitarias Públicas;
- c) ser motivados para cumplir con las políticas de seguridad de las Instituciones Universitarias Públicas;
- d) alcancen un nivel de conciencia sobre la seguridad acorde con sus roles y responsabilidades dentro de las Instituciones Universitarias Públicas;
- e) cumplir con las condiciones y términos del empleo, los cuales incluyen las políticas de seguridad de la información de las Instituciones Universitarias Públicas y métodos adecuados de trabajo;
- f) mantenerse con las habilidades y calificaciones adecuadas.

Si el personal, contratistas y usuarios no son conscientes de sus responsabilidades de seguridad, pueden causar daños considerables a las Instituciones Universitarias Públicas. Un personal motivado tiene más probabilidades de ser más confiable y causar menos incidentes de seguridad de la información.

7.2.2 Control: Concientización, formación y capacitación en seguridad de la información

Todo el personal de las Instituciones Universitarias Públicas y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en las Instituciones Universitarias Públicas, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de las Instituciones Universitarias Públicas. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

El Responsable del Área de Recursos Humanos será el encargado de coordinar las acciones de capacitación que surjan de la presente Política.

Cada año se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento.

Las Áreas Responsables del Material de Capacitación se encuentran en el "Anexo - Materiales de capacitación". El Responsable del Área de Recursos Humanos será el responsable de mantenerlo actualizado.

El personal que ingrese a las Instituciones Universitarias Públicas recibirá el material, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

Por otra parte, se arbitrarán los medios técnicos necesarios para comunicar a toda la comunidad, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.

7.2.3 Control: Proceso disciplinario

Se seguirá el proceso disciplinario formal contemplado en las normas estatutarias, escalafonarias y convencionales que rigen al personal de las Instituciones Universitarias Públicas, para el personal que violen la Política, Normas y Procedimientos de Seguridad de las Instituciones Universitarias Públicas.

El proceso disciplinario también se puede utilizar como un elemento disuasivo para evitar que el personal, contratistas y terceros que violen las políticas y procedimientos de la seguridad de las Instituciones Universitarias Públicas y cualquier otro incumplimiento de la seguridad.

7.3 Categoría: Cese del empleo o cambio de puesto de trabajo

Objetivo

Asegurar que los usuarios, empleados, contratistas y terceras personas salgan de las Instituciones Universitarias Públicas o cambien de empleo de una manera ordenada.

Se deben establecer las responsabilidades para asegurar que la salida de las Instituciones Universitarias Públicas del usuario empleado, contratista o tercera persona sea manejada y se complete la devolución de todo el equipo y se eliminen todos los derechos de acceso.

7.3.1 Control: Responsabilidad del cese o cambio

Las responsabilidades para realizar la desvinculación o cambio de puesto deben ser claramente definidas y asignadas, incluyendo requerimientos de seguridad y responsabilidades legales a posteriori y, cuando sea apropiado, las

responsabilidades contenidas dentro de cualquier acuerdo de confidencialidad, y los términos y condiciones de empleo con continuidad por un período definido de tiempo luego de la finalización del trabajo del empleado, contratista o usuario de tercera parte.

Puede ser necesario informar al personal, contratistas y terceros de los cambios en el personal y los acuerdos de operación.

7.3.2 Control: Devolución de activos

Todo el personal, contratistas y usuarios de terceras partes deben devolver todos los activos de las Instituciones Universitarias Públicas en su poder (software, documentos corporativos, equipamiento, dispositivos de computación móviles, tarjetas de crédito, tarjetas de ingreso, etc.) tras la terminación de su empleo, contrato, o acuerdo.

En los casos donde el empleado, contratista y usuarios tengan conocimiento que es importante para las operaciones actuales, esa información debe ser documentada y transferida a las Instituciones Universitarias Públicas.

7.3.3 Control: Retiro de los derechos de acceso

Se revisarán los derechos de acceso de un individuo a los activos asociados con los sistemas y servicios de información tras la desvinculación. Esto determinará si es necesario remover los derechos de acceso.

Con el cambio de un empleo deben removerse todos los derechos de acceso que no fueron aprobados para el nuevo empleo, comprendiendo esto accesos lógicos y físicos, llaves, tarjetas de identificación, instalaciones de procesamiento de la información, suscripciones, y remoción de cualquier documentación que lo identifique como un miembro corriente de las Instituciones Universitarias Públicas.

Si un empleado, contratista o usuario de tercera parte que se está desvinculando tiene conocimiento de contraseñas para cuentas que permanecen activas, éstas deben ser cambiadas tras la finalización o cambio de empleo, contrato o acuerdo.

Se evaluará la reducción o eliminación de los derechos de acceso a los activos de la información y a las instalaciones de procesamiento de la información antes de que el empleo termine o cambie, dependiendo de factores de riesgos, tales como:

- a) si la terminación o cambio es iniciado por el empleado, contratista o usuario de tercera parte, o por la gestión y la razón de la finalización;

- b) las responsabilidades actuales del empleado, contratista o cualquier otro usuario;
- c) el valor de los activos accesibles actualmente.

8. Cláusula: Gestión de Activos

Objetivo

- Garantizar que los activos de información reciban un apropiado nivel de protección.
- Clasificar la información para señalar su sensibilidad y criticidad.
- Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

8.1 Categoría: Responsabilidad sobre los activos

Objetivo

Todos los activos deben ser inventariados y contar con un propietario nombrado.

Los propietarios deben identificar todos los activos y se debiera asignar la responsabilidad por el mantenimiento de los controles apropiados. La implementación de controles específicos puede ser delegada por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección apropiada de los activos.

8.1.1 Control: Inventario de activos

Se identificarán los activos de información de las Instituciones Universitarias Públicas. Existen muchos tipos de activos, que incluyen pero no se limitan a:

- a) información: bases de datos, archivos de datos, documentación, contratos, acuerdos;
- b) activos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo, y utilitarios;
- c) activos físicos: equipamiento de computación, equipamiento de comunicaciones, medios removibles y otros equipamientos;

- d) instalaciones: edificios, ubicaciones físicas, tendido eléctrico, red de agua y gas, etc.;
- e) servicios: servicios de cómputo y de comunicaciones, servicios generales, por ejemplo: calefacción, iluminación, energía, y aire acondicionado;
- f) personas, y sus calificaciones, habilidades y experiencia;
- g) activos intangibles, tales como la reputación y la imagen de las Instituciones Universitarias Públicas.

El inventario será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad de no mayor a 6 meses.

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

8.1.2 Control: Propiedad de los activos

Toda la información y los activos junto a sus medios de procesamiento de información deben ser propiedad de un responsable designado en las Instituciones Universitarias Públicas.

Se designarán los Propietarios de los activos identificados, quienes deben cumplir sus funciones de propietario, esto es:

- a) informar sobre cualquier cambio que afecte el inventario de activos;
- b) clasificar los activos en función a su valor;
- c) definir los requisitos de seguridad de los activos;
- d) velar por la implementación y el mantenimiento de los controles de seguridad requeridos en los activos.

Cabe aclarar que, si bien los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservarán la responsabilidad del cumplimiento de las mismas. La delegación de la administración por parte de los propietarios de los activos será documentada por los mismos y proporcionada al Responsable de Seguridad de la Información.

8.1.3 Control: Uso aceptable de los activos

Se identificarán, documentarán e implementarán reglas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de la información.

Todo el personal, contratistas y usuarios de terceras partes deben seguir las reglas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de la misma, incluyendo pero sin limitarse a:

- a) sistemas de mensajería (como por ejemplo correo electrónico o servicios de mensajería instantánea),
- b) sistemas de gestión,
- c) estaciones de trabajo,
- d) dispositivos móviles,
- e) herramientas y equipamiento de publicación de contenidos.

8.2 Categoría: Clasificación de la información

Objetivo

Asegurar que la información reciba un nivel de protección apropiado.

La información debe ser clasificada para indicar la necesidad, prioridades y grado de protección esperado cuando se maneja la información.

La información tiene diversos grados de confidencialidad e importancia. Algunos ítems pueden requerir un nivel de protección adicional o manejo especial. Se debe utilizar un esquema de clasificación de información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de uso especiales.

8.2.1 Control: Directrices de clasificación

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.

A continuación se establece la metodología de clasificación de la información propuesta en función a cada una de las mencionadas características:

Confidencialidad:

0. Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de las Instituciones Universitarias Públicas o no. PÚBLICO

1. Información que puede ser conocida y utilizada por todo el personal de las Instituciones Universitarias Públicas y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para las Instituciones Universitarias Públicas, el Sector Público

Nacional o terceros. RESERVADA - USO INTERNO

2. 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 las Instituciones Universitarias Públicas, al Sector Público Nacional o a terceros. RESERVADA - CONFIDENCIAL

3. Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de las Instituciones Universitarias Públicas, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros. RESERVADA SECRETA

Integridad:

0. Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria de las Instituciones Universitarias Públicas.

1. Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para las Instituciones Universitarias Públicas, el Sector Público Nacional o terceros.

2. Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para las Instituciones Universitarias Públicas, el Sector Público Nacional o terceros.

3. Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves a las Instituciones Universitarias Públicas, al Sector Público Nacional o a terceros.

Disponibilidad:

0. Información cuya inaccesibilidad no afecta la operatoria de las Instituciones Universitarias Públicas.

1. Información cuya inaccesibilidad permanente durante un plazo no menor a una semana podría ocasionar pérdidas significativas para las Instituciones Universitarias Públicas, el Sector Público Nacional o terceros.

2. Información cuya inaccesibilidad permanente durante un plazo no menor a un día podría ocasionar pérdidas significativas a las Instituciones Universitarias Públicas, al Sector Público Nacional o a terceros.

3. Información cuya inaccesibilidad permanente durante un plazo no menor a una hora podría ocasionar pérdidas significativas a las Instituciones Universitarias Públicas, al Sector Público Nacional o a terceros.

Al referirse a pérdidas, se contemplan aquellas mensurables (materiales) y no mensurables (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 deben tener acceso a la misma.

En adelante se mencionará como "información clasificada" (o "datos clasificados") a aquella que se encuadre en los niveles 1, 2 o 3 de Confidencialidad.

8.2.2 Control: Etiquetado y manipulado 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.).

- Transmisión a través de mecanismos de intercambio de archivos (FTP, almacenamiento masivo remoto, etc.).

Para cada uno de los niveles de clasificación, se deben definir los procedimientos de manejo seguros, incluyendo las actividades de procesamiento, almacenaje, transmisión, de-clasificación y destrucción.

8.3 Categoría: Gestión de medios físicos

Objetivo

Evitar la divulgación no-autorizada; modificación, eliminación o destrucción de activos; y la interrupción de las actividades. Los medios se deberían controlar y proteger físicamente.

Se deben establecer los procedimientos de operación apropiados para proteger los documentos, medios de cómputo (por ejemplo, cintas y discos), entrada/salida de datos (input/output) y documentación del sistema de una divulgación no-autorizada, modificación, eliminación y destrucción.

8.3.1 Control: Administración de Medios Informáticos Removibles

El Responsable del Área Informática, con la asistencia del Responsable de Seguridad de la Información, implementará procedimientos para la administración de medios informáticos removibles, como cintas, discos, pendrives e informes impresos. El cumplimiento de los procedimientos se hará de acuerdo a la cláusula "9.1 Categoría: Requerimientos para el Control de Acceso".

Se deben considerar las siguientes acciones para la implementación de los procedimientos:

- a) Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por las Instituciones Universitarias Públicas.
- b) Requerir autorización para retirar cualquier medio de las Instituciones Universitarias Públicas y realizar un control de todos los retiros a fin de mantener un registro de auditoría.
- c) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores y la criticidad de la información almacenada.

8.3.2 Control: Eliminación de Medios de Información

El Responsable del Área Informática, junto con el Responsable de Seguridad de la Información definirá procedimientos para la eliminación segura de los medios de soporte de información respetando la normativa vigente.

Los procedimientos deben considerar que los siguientes elementos requerirán almacenamiento y eliminación segura:

- a) Documentos en papel.
- b) Voces u otras grabaciones.
- c) Papel carbónico.
- d) Informes de salida.
- e) Cintas de impresora de un solo uso.
- f) Cintas magnéticas.
- g) Discos u otros dispositivos removibles.
- h) Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor).
- i) Listados de programas.
- j) Datos de prueba.
- k) Documentación del sistema.

La evaluación del mecanismo de eliminación debe contemplar el tipo de dispositivo y la criticidad de la información contenida.

8.3.3 Control: Seguridad de los Medios en Tránsito

Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deben contemplar:

- a) La utilización de medios de transporte o servicios de mensajería confiables. El Propietario de la Información a transportar determinará qué servicio de mensajería se utilizará conforme la criticidad de la información a transmitir.
- b) Suficiente embalaje para envío de medios a través de servicios postales o de mensajería, siguiendo las especificaciones de los fabricantes o proveedores.
- c) La adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas. Entre los ejemplos se incluyen:
 - 1) Uso de recipientes cerrados.
 - 2) Entrega en mano.
 - 3) Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso).

- 4) En casos excepcionales, división de la mercadería a enviar en más de una entrega y envío por diferentes rutas.

9. Cláusula: Gestión de Accesos

Objetivo

Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información. Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

Controlar la seguridad en la conexión entre la red de las Instituciones Universitarias Públicas y otras redes públicas o privadas. Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

9.1 Categoría: Requerimientos para la Gestión de Acceso

Objetivo

Controlar el acceso a la información. Se debe controlar el acceso a la información, medios de procesamiento de la información y procesos sobre la base de los requerimientos de las Instituciones Universitarias Públicas y de seguridad. Las reglas de control del acceso deben tomar en cuenta las políticas para la divulgación y autorización de la información.

9.1.1 Control: Política de Gestión de Accesos

En la aplicación de gestión de acceso, se contemplarán los siguientes aspectos:

- 1) Identificar los requerimientos de seguridad de cada una de las aplicaciones.
- 2) Identificar toda la información gestionada por las aplicaciones.

- 3) Establecer criterios coherentes entre esta Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas y redes (Ver "cláusula 8 Gestión de Activos").
- 4) Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
- 5) Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
- 6) Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones y dispositivos disponibles.

9.1.2 Control: Reglas de Gestión de Acceso

Las reglas de control de acceso especificadas, deben:

- 1) Indicar expresamente si las reglas son obligatorias u optativas.
- 2) 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".
- 3) 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 (Ver cláusula 8 Gestión de Activos).
- 4) Controlar los cambios en los permisos de usuario.
- 5) 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.

9.2 Categoría: Administración de Gestión de Usuarios

Objetivo

Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

Los procedimientos debieran abarcar todas las etapas en el ciclo de vida del acceso del usuario, desde el registro inicial de usuarios nuevos hasta la baja final de los usuarios que ya no requieren acceso a los sistemas y servicios de información.

9.2.1 Control: Registración de Usuarios

El Responsable de Seguridad de la Información 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:

- a) 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.
- b) Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.
- c) 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 las Instituciones Universitarias Públicas, por ejemplo que no compromete la segregación de funciones.
- d) Entregar a los usuarios un detalle escrito de sus derechos de acceso.
- e) Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.
- f) Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
- g) Mantener un registro formal de todas las personas registradas para utilizar el servicio.
- h) 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 las Instituciones Universitarias Públicas o sufrieron la pérdida/robo de sus credenciales de acceso.
- i) Efectuar revisiones periódicas con el objeto de:
 - i) cancelar identificadores y cuentas de usuario redundantes
 - ii) inhabilitar cuentas inactivas pasado un periodo de gracia, por ejemplo 60 días
 - iii) eliminar cuentas inactivas pasado un período de gracia, por ejemplo 120 días

En el caso de existir excepciones, deben ser debidamente justificadas y aprobadas.
- j) Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.
- k) 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 en caso de corresponder.

9.2.2 Control: Gestión 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:

- 1) 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.
- 2) 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.
- 3) 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.
- 4) 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.
- 5) 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 de la Información.

9.2.3 Control: Gestión 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:

- 1) 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.
- 2) 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 acreditada la identidad del usuario.

- 3) 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 formal cuando la reciban.
- 4) Almacenar las contraseñas sólo en sistemas informáticos protegidos.
- 5) Utilizar otras tecnologías de autenticación y autorización de usuarios, como ser la biométrica (por ejemplo verificación de huellas dactilares), verificación de firma, uso de autenticadores de hardware (como las tarjetas de circuito integrado), etc. El uso de esas herramientas se dispondrá cuando la evaluación de riesgos realizada por el Responsable de Seguridad de la Información conjuntamente con el Responsable del Área de Informática y el Propietario de la Información lo determine necesario (o lo justifique).
- 6) Configurar los sistemas de tal manera que se cumplan, cuando correspondiere, según el "Anexo - Política de contraseñas", el cual deberá contener como mínimo los siguiente el "Anexo - Política de contraseñas", el cual deberá contener como mínimo los siguiente aspectos:
 - a) Periodos de validez para las contraseñas;
 - b) Posibilidad de reutilización de contraseñas ya usadas;
 - c) Formato de la contraseña:
 - i) longitud mínima;
 - ii) tipos de caracteres que deben incluir;
 - iii) cumplimiento de reglas semánticas.
 - d) Posibilidad de elección y modificación de la contraseña por parte del usuario;
 - e) Almacenamiento de las claves;
 - f) Tamaño del histórico de claves a almacenar para cada usuario;
 - g) Método de encriptación de las claves.
 - h) número de intentos de autenticación permitidos

9.2.4 Control: Administración de Contraseñas Críticas

En los diferentes ambientes de procesamiento existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual. El Responsable de Seguridad de

la Información definirá procedimientos para la administración de dichas contraseñas críticas que contemplen lo siguiente:

- 1) Se definirán las causas que justificarán el uso de contraseñas críticas así como el nivel de autorización requerido.
- 2) Las contraseñas seleccionadas serán seguras, y su definición será efectuada como mínimo por dos personas, de manera que ninguna de ellas conozca la contraseña completa.
- 3) Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente.
- 4) La utilización de las contraseñas críticas será registrada, documentando las causas que determinaron su uso, así como el responsable de las actividades que se efectúen con la misma.
- 5) Cada contraseña crítica se renovará una vez utilizada y se definirá un período luego del cual la misma será renovada en caso de que no se la haya utilizado.
- 6) Se registrarán todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas. Dicho registro será revisado posteriormente por el Responsable de Seguridad de la Información.

9.2.5 Control: Revisión de Derechos de Acceso de Usuarios

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información de que se trate llevará a cabo semestralmente un proceso formal, a fin de revisar los derechos de acceso de los usuarios. Se deben contemplar los siguientes controles:

- 1) Revisar los derechos de acceso de los usuarios a lo sumo semestralmente.
- 2) Revisar las autorizaciones de privilegios especiales de derechos de acceso con una periodicidad no menor a los 3 meses.
- 3) Revisar las asignaciones de privilegios a lo sumo semestralmente a fin de garantizar que no se obtengan privilegios no autorizados.

9.3 Categoría: Responsabilidades del Usuario

Objetivo

Evitar el acceso de usuarios no-autorizados, evitar poner en peligro la información y evitar el robo de información y los medios de procesamiento de la información.

La cooperación de los usuarios autorizados es esencial para una seguridad efectiva.

Los usuarios deben estar al tanto de sus responsabilidades para mantener controles de acceso efectivos, particularmente con relación al uso de claves secretas y la seguridad del equipo del usuario.

Se debe implementar una política de escritorio y pantalla limpios para reducir el riesgo de acceso no autorizado o daño a los papeles, medios y medios de procesamiento de la información.

9.3.1 Control: Uso de Contraseñas

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 directivas indicadas en el "Anexo - Política de contraseñas".

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas y en tránsito.

9.4 Categoría: Control de Acceso a Sistemas y Aplicaciones

Objetivo

Evitar el acceso no autorizado a los servicios de la red.

Se debe controlar el acceso a los servicios de redes internas y externas.

El acceso del usuario a las redes y servicios de las redes no deben comprometer la seguridad de los servicios de la red asegurando:

- 1) que existan las interfaces apropiadas entre la red de las Instituciones Universitarias Públicas y las redes de otras organizaciones, y redes públicas;
- 2) se apliquen los mecanismos de autenticación apropiados para los usuarios y el equipo;
- 3) el control del acceso del usuario a la información sea obligatorio.

9.4.1 Control: Política de Utilización de los Servicios de Red

Las conexiones no seguras a los servicios de red pueden afectar a todo las Instituciones Universitarias Públicas, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

El Responsable del Área Informática tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del titular de una Unidad Organizativa que lo solicite para personal de su incumbencia.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la administración y del control de seguridad de las Instituciones Universitarias Públicas.

Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

- 1) Identificar las redes y servicios de red a los cuales se permite el acceso.
- 2) Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.
- 3) Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

Esta Política será coherente con la Política de Gestión de Accesos de las Instituciones Universitarias Públicas.

9.4.2 Control: Camino Forzado

Las redes están diseñadas para permitir el máximo alcance de distribución de recursos y flexibilidad en la elección de la ruta a utilizar. Estas características también pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones de las Instituciones Universitarias Públicas, o para el uso no autorizado de servicios de información. Por esto, el camino de las comunicaciones será controlado.

Se limitarán las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales el mismo se encuentra autorizado a acceder, mediante la implementación de controles en diferentes puntos de la misma.

Los requerimientos relativos a caminos forzados se basarán en la Política de Control de Accesos de las Instituciones Universitarias Públicas. El Responsable de Seguridad de la Información, conjuntamente con el Propietario de la Información de que se trate, realizará una evaluación de riesgos a fin de determinar los mecanismos de control que corresponda en cada caso.

9.4.3 Control: Autenticación de Usuarios para Conexiones Externas

Las conexiones externas son de gran potencial para accesos no autorizados a la información de las Instituciones Universitarias Públicas. Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación. Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros. El Responsable de Seguridad de la Información, conjuntamente con el Propietario de la Información de que se trate, realizará una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

La autenticación de usuarios remotos puede llevarse a cabo utilizando:

- 1) Un método de autenticación físico (por ejemplo tokens de hardware), para lo que debe implementarse un procedimiento que incluya:
 - a) Asignación de la herramienta de autenticación.
 - b) Registro de los poseedores de autenticadores.
 - c) Mecanismo de rescate al momento de la desvinculación del personal al que se le otorgó.
 - d) Método de revocación de acceso del autenticador, en caso de compromiso de seguridad.
- 2) Un protocolo de autenticación (por ejemplo desafío/respuesta), para lo que debe implementarse un procedimiento que incluya:
 - a) Establecimiento de las reglas con el usuario.
 - b) Establecimiento de un ciclo de vida de las reglas para su renovación.
- 3) También puede utilizarse una herramienta de verificación de la dirección del usuario de red, a fin de constatar el origen de la conexión.

En caso de utilizarse sistemas de Voz sobre IP, deben ajustarse los controles a fin de que no sean utilizados para efectuar comunicaciones no autorizadas (ej.: bloqueo de puertos).

9.4.4 Control: Autenticación de Nodos

Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación de las Instituciones Universitarias Públicas. Por consiguiente, las conexiones a sistemas informáticos remotos serán

autenticadas. Esto es particularmente importante si la conexión utiliza una red que está fuera de control de la gestión de seguridad de las Instituciones Universitarias Públicas. En el punto anterior se mencionan algunos ejemplos de autenticación y de cómo puede lograrse. La autenticación de nodos puede servir como un medio alternativo de autenticación de grupos de usuarios remotos, cuando éstos están conectados a un servicio informático seguro y compartido.

9.4.5 Control: Protección de los Puertos (Ports) de Diagnóstico Remoto

Muchas computadoras y sistemas de comunicación son instalados y administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado, con las mismas características del punto "9.4.3 Control: Autenticación de Usuarios para Conexiones Externas". También para este caso debe tenerse en cuenta el punto "9.4.2 Control: Camino Forzado".

9.4.6 Control: Subdivisión de Redes

Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados. Para esto se definirán y documentarán los perímetros de seguridad que sean convenientes para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado de acuerdo a la Política de Control de Accesos.

La subdivisión en dominios de la red tomará en cuenta criterios como los requerimientos de seguridad comunes de grupos de integrantes de la red, la mayor exposición de un grupo a peligros externos, separación física, u otros criterios de aglutinamiento o segregación preexistentes.

Basándose en la Política de Gestión de Accesos y los requerimientos de acceso (9.1 Categoría: Requerimientos para la Gestión de Accesos), el Responsable del Área Informática evaluará el costo relativo y el impacto en el desempeño que ocasione la implementación de equipamiento o desarrollo específico adecuado para subdividir la red. Luego decidirá, junto con el Responsable de Seguridad de la Información, el esquema más apropiado a implementar.

9.4.7 Control: 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 de la Información 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 la Cláusula 6.1.5 Control: Acuerdos de confidencialidad. Para ello, el Responsable de Seguridad de la Información junto con el Responsable del Área de Informática analizarán las medidas a ser implementadas para efectivizar dicho control, como ser la instalación de "firewalls", "proxies", "clases dhcp", etc.

9.4.8 Control: Conexión a la Red

Sobre la base de lo definido en el punto "9.1 Categoría: Requerimientos para la gestión de accesos", se implementarán controles para limitar la capacidad de conexión de los usuarios. Dichos controles se podrán implementar en los dispositivos de interconexión que separen los diferentes dominios de la red.

Algunos ejemplos de los entornos a las que deben implementarse restricciones son:

- 1) Correo electrónico.
- 2) Transferencia de archivos.
- 3) Acceso interactivo.
- 4) Acceso a la red fuera del horario laboral.

9.4.9 Control: Ruteo de Red

En las redes compartidas, especialmente aquellas que se extienden fuera de los límites de las Instituciones Universitarias Públicas, se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos. Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino. Adicionalmente, para este objetivo pueden utilizarse diversos métodos incluyendo entre otros autenticación de protocolos de ruteo, ruteo estático, traducción de direcciones y listas de control de acceso.

9.4.10 Control: Seguridad de los Servicios de Red

El Responsable de Seguridad de la Información junto con el Responsable del Área informática definirán las pautas para garantizar la seguridad de los servicios de red de las Instituciones Universitarias Públicas, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.
- Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentarse.
- Instalar periódicamente las actualizaciones de seguridad.
- Implementar sitios seguros utilizando certificados digitales.

Dicha configuración será revisada periódicamente por el Responsable de Seguridad de la Información.

9.5 Categoría: Control de Acceso al Sistema Operativo

Objetivo

Evitar el acceso no autorizado a los sistemas operativos.

Se deben utilizar medios de seguridad para restringir el acceso a los sistemas operativos a los usuarios no autorizados. Los medios deben tener la capacidad para:

- 1) autenticar a los usuarios autorizados, en concordancia con una política de control de acceso definida;
- 2) registrar los intentos exitosos y fallidos de autenticación del sistema;
- 3) registrar el uso de los privilegios especiales del sistema;
- 4) emitir alarmas cuando se violen las políticas de seguridad del sistema;
- 5) proporcionar los medios de autenticación apropiados;
- 6) cuando sea apropiado, restringir el tiempo de conexión de los usuarios

9.5.1 Control: Identificación Automática de Terminales

El Responsable de Seguridad de la Información junto con el Responsable del Área Informática realizará una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

Si del análisis realizado surgiera la necesidad de proveer un método de identificación de terminales, se redactará un procedimiento que indique:

- 1) El método de identificación automática de terminales utilizado.
- 2) El detalle de transacciones permitidas por terminal o dispositivo.

9.5.2 Control: Procedimientos de Conexión de Terminales.

El acceso a los servicios de información sólo será posible a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema informático será diseñado para minimizar la oportunidad de acceso no autorizado.

Este procedimiento, por lo tanto, debe divulgar la mínima información posible acerca del sistema, a fin de evitar proveer de asistencia innecesaria a un usuario no autorizado.

El procedimiento de identificación debe:

- 1) Mantener en secreto los identificadores de sistemas o aplicaciones hasta tanto se haya llevado a cabo exitosamente el proceso de conexión.
- 2) Desplegar un aviso general advirtiendo que sólo los usuarios autorizados pueden acceder a la computadora.
- 3) Evitar dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión.
- 4) Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta.
- 5) Limitar el número de intentos de conexión no exitosos permitidos y:
 - a) Registrar los intentos no exitosos.
 - b) Impedir otros intentos de identificación, una vez superado el límite permitido.
 - c) Desconectar conexiones de comunicaciones de datos.
- 6) Limitar el tiempo máximo permitido para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión.
- 7) Desplegar la siguiente información, al completarse una conexión exitosa:
 - a) Fecha y hora de la conexión exitosa anterior.
 - b) Detalles de los intentos de conexión no exitosos desde la última conexión exitosa.

9.5.3 Control: Identificación y Autenticación de los Usuarios

Todos los usuarios (incluido el personal de soporte técnico, como 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, a fin de garantizar la trazabilidad de las transacciones. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

En circunstancias excepcionales, cuando existe un claro beneficio para las Instituciones Universitarias Públicas, 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.

Si se utilizara un método de autenticación físico (por ejemplo autenticadores de hardware), debe implementarse un procedimiento que incluya:

- 1) Asignar la herramienta de autenticación.
- 2) Registrar los poseedores de autenticadores.
- 3) Rescatar el autenticador al momento de la desvinculación del personal al que se le otorgó.
- 4) Revocar el acceso del autenticador, en caso de compromiso de seguridad.

Si se utilizara un método de autenticación externo (por ejemplo autenticadores por software), debe implementarse un procedimiento que incluya:

- 1) Registrar los poseedores de autenticadores.
- 2) Revocar el acceso del autenticador, en caso de compromiso de seguridad.

Se recomienda la utilización de más de un factor de autenticación para los usuarios, principalmente para los sistemas críticos.

9.5.4 Control: 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:

- 1) Imponer el uso de contraseñas individuales para determinar responsabilidades.
- 2) 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.

- 3) Imponer una selección de contraseñas de calidad según lo señalado en el punto "9.3.1 Control: Uso de Contraseñas".
- 4) Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas.
- 5) Obligar a los usuarios a cambiar las contraseñas provisionales en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
- 6) A los efectos de evitar la reutilización de las contraseñas utilizadas por el usuario, de acuerdo al "Anexo- Política de contraseñas", se deberá mantener un registro histórico de las mismas.
- 7) Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.

10. Cláusula: Criptografía

Objetivos

Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, no-repudio, la autenticidad y/o la integridad de la información.

10.1 Categoría: Cumplimiento de Requisitos Legales

Objetivo

Se utilizarán sistemas y técnicas criptográficas para la protección de la información en base a un análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad. Se debe desarrollar una política sobre el uso de controles criptográficos. Se debe establecer una gestión clave para sostener el uso de técnicas criptográficas.

10.1.1 Control: Política de Utilización de Controles Criptográficos

Las Instituciones Universitarias Públicas establece la presente Política de uso de controles criptográficos, a fin de determinar su correcto uso. Para ello se indica que:

- a) Se utilizarán controles criptográficos en los siguientes casos:
 - 1) Para la protección de claves de acceso a sistemas, datos y servicios.
 - 2) Para la transmisión de información clasificada
 - 3) Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el Responsable de Seguridad de la Información.
- b) Se desarrollarán procedimientos respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.
- c) La asignación de funciones en el control criptográfico se encuentran en el "Anexo - Asignación de funciones en controles criptográficos." El responsable de Seguridad de la Información será el encargado de completarlo y mantenerlo actualizado, deberá revisarlo a lo sumo semestralmente.
- d) Los algoritmos de cifrado y tamaños de clave que se pueden utilizar se encuentran en el "Anexo - Algoritmos de cifrado." El Responsable del Área Informática será el encargado de completarlo y mantenerlo actualizado, deberá revisarlo a lo sumo semestralmente.

10.1.2 Control: Cifrado

Mediante la evaluación de riesgos que llevará a cabo el Propietario de la Información y el Responsable de Seguridad de la Información, se identificará el nivel requerido de protección, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.

Al implementar la Política de las Instituciones Universitarias Públicas en materia criptográfica, se considerarán los controles aplicables a la exportación e importación de tecnología criptográfica. Ver Cláusula 18.1.6 Control: Regulación de Controles para el Uso de Criptografía

10.1.3 Control: Firma Digital

Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos. Pueden aplicarse a cualquier tipo de documento que se procese electrónicamente. Se implementan mediante el uso de una técnica criptográfica sobre la base de dos claves relacionadas de manera única, donde una clave, denominada privada, se utiliza para crear una firma y la otra, denominada pública, para verificarla.

Se tomarán recaudos para proteger la confidencialidad de las claves privadas.

Asimismo, es importante garantizar la vinculación entre el poseedor del par de claves y su clave pública. La misma se provee mediante el uso de un certificado de clave pública.

Los algoritmos de firma utilizados, como así también la longitud de clave a emplear, son los descriptos en el "Anexo - Algoritmos de cifrado".

Se recomienda que las claves criptográficas utilizadas para firmar digitalmente no sean empleadas en procedimientos de cifrado de información. Dichas claves deben ser resguardadas bajo el control exclusivo de su titular.

Al utilizar firmas y certificados digitales, se considerará la legislación vigente que describa las condiciones bajo las cuales una firma digital es legalmente válida. Ver "Cláusula 18.1.6 Control: Regulación de Controles para el Uso de Criptografía".

En algunos casos podría ser necesario establecer acuerdos especiales para respaldar el uso de las firmas digitales. A tal fin se debe obtener asesoramiento legal con respecto al marco normativo aplicable y la modalidad del acuerdo a implementar. (Ver Cláusula 10.1.1 Control: Política de utilización de controles criptográficos).

10.1.4 Control: Servicios de No Repudio

Estos servicios se utilizarán cuando sea necesario resolver disputas acerca de la ocurrencia de un evento o acción. Su objetivo es proporcionar herramientas para evitar que aquél que haya originado una transacción electrónica niegue haberla efectuado.

10.1.5 Control: Protección de claves criptográficas

Se implementará un sistema de administración de claves criptográficas para respaldar la utilización por parte de las Instituciones Universitarias Públicas de los dos tipos de técnicas criptográficas, a saber:

- a) Técnicas de clave secreta (criptografía simétrica), cuando dos o más actores comparten la misma clave y ésta se utiliza tanto para cifrar información como para descifrarla.
- b) Técnicas de clave pública (criptografía asimétrica), cuando cada usuario tiene un par de claves: una clave pública (que puede ser revelada a cualquier persona) utilizada para cifrar y una clave privada (que debe mantenerse en secreto) utilizada para descifrar. Las claves asimétricas utilizadas para cifrado no deben ser las mismas que se utilizan para firmar digitalmente.

Todas las claves serán protegidas contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada.

Se aplicarán con este propósito los algoritmos criptográficos enumerados en el punto "10.1.1 Control: Política de Utilización de Controles Criptográficos."

Se proporcionará una protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.

10.1.6 Control: Protección de Claves criptográficas: Normas y procedimientos

Se redactarán las normas y procedimientos necesarios para:

- a) Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.
- b) Generar u obtener certificados de clave pública de manera segura.
- c) Distribuir claves de forma segura a los usuarios que corresponda, incluyendo información sobre cómo deben activarse cuando se reciban.
- d) Almacenar claves, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados.
- e) Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.
- f) Revocar claves, incluyendo cómo deben retirarse o desactivarse las mismas, por ejemplo cuando las claves están comprometidas o cuando un usuario se desvincula de las Instituciones Universitarias Públicas (en cuyo caso las claves también deben archivarse).
- g) Recuperar claves perdidas o alteradas como parte de la administración de la continuidad de las actividades de las Instituciones Universitarias Públicas, por ejemplo para la recuperación de la información cifrada.
- h) Archivar claves, por ejemplo, para la información archivada o resguardada.
- i) Destruir claves.
- j) Registrar y auditar las actividades relativas a la administración de claves.

A fin de reducir la probabilidad de compromiso, las claves tendrán fechas de inicio y caducidad de vigencia, definidas de manera que sólo puedan ser utilizadas por un lapso no mayor a 12 meses.

Es importante que el proceso de administración de los certificados de clave pública sea absolutamente confiable. Este proceso deberá ser llevado a cabo por una entidad denominada Autoridad de Certificación (AC) o Certificador.

11. Cláusula: Física y Ambiental

Objetivo

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información de las Instituciones Universitarias Públicas.

Proteger el equipamiento de procesamiento de información crítica de las Instituciones Universitarias Públicas ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información de las Instituciones Universitarias Públicas.

Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

Proporcionar protección proporcional a los riesgos identificados.

11.1 Categoría: Áreas Seguras

Objetivo

Evitar el acceso físico no autorizado, daño e interferencia con la información y los espacios físicos de las Instituciones Universitarias Públicas.

Los medios de procesamiento de información crítica o confidencial deben ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Deben estar físicamente protegidos del acceso no autorizado, daño e interferencia.

11.1.1 Control: Perímetro de seguridad física

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las sedes de las Instituciones Universitarias Públicas y de las instalaciones de procesamiento de información.

Las Instituciones Universitarias Públicas deberá utilizar perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía

eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera estarán definidas por el Responsable del Área Informática con el asesoramiento del Responsable de Seguridad de la Información, de acuerdo a la evaluación de riesgos efectuada.

Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda:

- a) Definir y documentar claramente el perímetro de seguridad.
- b) Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo mediante mecanismos de control, vallas, alarmas, cerraduras, etc.
- c) Verificar la existencia de un área de recepción atendida por personal. Si esto no fuera posible se implementarán alguno de los medios alternativos de control de acceso indicados en el "Anexo - Métodos de control de acceso físico", al área o edificio que corresponda. El acceso a dichas áreas y edificios estará restringido exclusivamente al personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa. El Responsable de Seguridad de la Información y el Responsable de la Seguridad Física serán los encargados de completarlo y mantenerlo actualizado, deberán revisar dicho anexo a lo sumo semestralmente.
- d) Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo por incendio, humedad e inundación.
- e) Identificar claramente todas las puertas de incendio de un perímetro de seguridad.

Un área segura puede ser una oficina con llave, o varias oficinas rodeadas

por una barrera de seguridad física interna continua. Pueden ser necesarios barreras y perímetros adicionales para controlar el acceso físico entre las áreas con diferentes requerimientos de seguridad, dentro del mismo perímetro de seguridad

El Responsable de Seguridad de la Información llevará un registro actualizado de los sitios protegidos, indicando:

- a) Identificación del Edificio y Área.
- b) Principales elementos a proteger.
- c) Medidas de protección física.

11.1.2 Control: Controles físicos de entrada

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Responsable de Seguridad de la Información 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:

- a) 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 instruyendo al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.
- b) Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se utilizarán los controles de autenticación para autorizar y validar todos los accesos indicados en el "Anexo - Métodos de control de acceso físico". Se mantendrá un registro protegido para poder auditar todos los accesos.
- c) Implementar el uso de una identificación unívoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.
- d) Revisar y actualizar semestralmente los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el Responsable de la Unidad Organizativa de la que dependa.
- e) Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

11.1.3 Control: Seguridad de oficinas, despachos, 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.

A los efectos de este control las áreas protegidas y los lugares seguros son los indicados en el "Anexo - Áreas protegidas". El responsable de Seguridad de la Información será el encargado de completarlo y mantenerlo actualizado, deberá revisarlo a lo sumo semestralmente.

Se establecen las siguientes medidas de protección para áreas protegidas:

- a) Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.
- b) Establecer que los edificios o sitios donde se realicen actividades de procesamiento de Información serán discretos y ofrecerán un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.
- c) Ubicar las funciones y el equipamiento de soporte, por ejemplo: impresoras, fotocopiadoras, máquinas de fax, adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.
- d) 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.
- e) Implementar los mecanismos de control para la detección de intrusos detallados en el "Anexo - Métodos de detección de intrusos". Los mismos serán instalados según estándares profesionales y probados periódicamente. Estos mecanismos de control comprenderán todas las puertas exteriores y ventanas accesibles. El Responsable de Seguridad de la Información y el Responsable de la Seguridad Física serán los encargados de completarlo y mantenerlo actualizado, deberán revisarlo a lo sumo semestralmente.
- f) Separar las instalaciones de procesamiento de información administradas por las Instituciones Universitarias Públicas de aquellas administradas por terceros.
- g) 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.
- h) Almacenar los materiales peligrosos o combustibles en lugares seguros a una distancia prudencial de las áreas protegidas de las Instituciones Universitarias Públicas. Los suministros, como los útiles de escritorio, no serán trasladados al área protegida hasta que sean requeridos.
- i) Almacenar los equipos redundantes y la información de resguardo (backup)

en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal.

11.1.4 Control: Protección contra amenazas externas y de origen ambiental

Se debe asignar y aplicar protección física contra daños por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre.

Se debe prestar consideración a cualquier amenaza contra la seguridad presentada por locales vecinos; por ejemplo, un fuego en un edificio vecino, escape de agua en el techo o pisos en sótano o una explosión en la calle.

Se debe considerar los siguientes lineamientos para evitar el daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre:

- a) Los materiales peligrosos o combustibles deben ser almacenados a una distancia segura del área asegurada. Los suministros a granel como papelería no deben almacenarse en el área asegurada;
- b) el equipo de reemplazo y los medios de respaldo debieran ubicarse a una distancia segura para evitar el daño de un desastre que afecte el local principal;
- c) se debe proporcionar equipo contra-incendios ubicado adecuadamente.

11.1.5 Control: Trabajo en áreas seguras

Para incrementar la seguridad de las áreas protegidas, se establecen los siguientes controles y lineamientos adicionales. Esto incluye controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí:

- a) Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.
- b) Evitar la ejecución de trabajos por parte de terceros sin supervisión.
- c) Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas.
- d) Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que requiera acceder al área protegida, será otorgado solamente cuando sea necesario y se encuentre autorizado y monitoreado. Se mantendrá un registro de todos los accesos de personas ajenas.

- e) Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.
- f) Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que hayan sido formalmente autorizadas por el Responsable de dicho área o el Responsable del Área Informática y el Responsable de Seguridad de la Información.
- g) Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

11.1.6 Control: Áreas de acceso público, de carga y descarga

Se controlarán las áreas de Recepción y Distribución, las cuales estarán aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados.

Para ello se establecerán controles físicos que considerarán los siguientes lineamientos:

- a) Limitar el acceso a las áreas de depósito, desde el exterior de la sede de las Instituciones Universitarias Públicas, sólo al personal previamente identificado y autorizado.
- b) Diseñar el área de depósito de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.
- c) Proteger todas las puertas exteriores del depósito cuando se abre la puerta interna.
- d) Inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.
- e) Registrar el material entrante al ingresar al silio pertinente.
- f) Cuando fuese posible, el material entrante debe estar segregado o separado en sus diferentes partes que lo constituyan.

11.2 Categoría: Seguridad de los equipos

Objetivo

Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de las Instituciones Universitarias Públicas.

Se debe proteger el equipo de amenazas físicas y ambientales.

11.2.1 Control: emplazamiento y protección de equipos

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:

- a) Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.
- b) Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.
- c) Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.
- d) Adoptar controles adecuados para minimizar el riesgo de amenazas potenciales, por:
 - 1) Inundaciones
 - 2) Incendios
 - 3) Terremotos
 - 4) Vandalismo.

Se deben establecer lineamientos sobre las actividades de comer, beber y fumar en la proximidad de los medios de procesamiento de la información.

Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información. Esta revisión se realizará semestralmente.

Se deben aplicar protección contra rayos a todos los edificios y se deben adaptar filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones.

Considerar asimismo el impacto de las amenazas citadas en el punto d) que tengan lugar en zonas próximas a la sede de las Instituciones Universitarias Públicas.

11.2.2 Control: Instalaciones de suministro

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

- a) Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.
- b) Contar con un suministro de energía ininterrumpible (UPS) para asegurar el

apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de las Instituciones Universitarias Públicas. La determinación de dichas operaciones críticas, será el resultado del análisis de impacto realizado por el Responsable de Seguridad de la Información conjuntamente con los Propietarios de la Información con incumbencia. Los planes de contingencia contemplarán las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.

- c) Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Debe realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir qué componentes será necesario abastecer de energía alternativa. Dicho análisis será realizado por el Responsable de Seguridad de la Información conjuntamente con los Propietarios de la Información. Se dispondrá de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado. Cuando el encendido de los generadores no sea automático, se asegurará que el tiempo de funcionamiento de la UPS permita el encendido manual de los mismos. Los generadores serán inspeccionados y probados periódicamente para asegurar que funcionen según lo previsto.

Asimismo, se procurará que los interruptores de emergencia se ubiquen cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica. Se proveerá de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía.

Se implementará protección contra descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo a las normativas vigentes.

Las opciones para lograr la continuidad de los suministros de energía incluyen múltiples alimentaciones para evitar que una falla en el suministro de energía.

11.2.3 Control: Seguridad del cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra interceptación o daño, mediante las siguientes acciones:

- a) Cumplir con los requisitos técnicos vigentes.
- b) Utilizar pisoducto, cielorraso desmontable o cableado embutido en la pared,

siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información.

- c) Proteger el cableado de red contra interceptación no autorizada o daño mediante como por ejemplo usando conductos o evitando trayectos que atraviesen áreas públicas.
- d) Separar los cables de energía de los cables de comunicaciones para evitar interferencias.
- e) Proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos blindados.

Para los sistemas sensibles o críticos indicados en el "Anexo - Sistemas Sensibles y Críticos" se implementarán los siguientes controles adicionales:

- a) Instalar conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.
- b) Utilizar rutas o medios de transmisión alternativos.

El Comité de seguridad de la información será el responsable de revisar, con una periodicidad no mayor a seis meses, y mantener actualizado el "Anexo - Sistemas Sensibles y Críticos".

11.2.4 Control: Mantenimiento de los equipos

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

- a) 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 del Responsables del Área Informática. El Área de Informática mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.
- b) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
- c) Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
- d) Registrar el retiro de equipamiento de la sede de las Instituciones Universitarias Públicas para su mantenimiento.
- e) Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

11.2.5 Control: Seguridad de los equipos fuera de las instalaciones

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de las Instituciones Universitarias Públicas, será autorizado por el responsable patrimonial. En el caso de que en el mismo se almacene información clasificada, debe ser aprobado además por el Propietario de la misma. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de las Instituciones Universitarias Públicas para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento. Asimismo, se mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito de las Instituciones Universitarias Públicas, cuando sea conveniente.

Los riesgos de seguridad, por ejemplo: daño, robo o interceptación; puede variar considerablemente entre los edificios y se debe tomarlo en cuenta para evaluar los controles apropiados.

11.2.6 Control: Reutilización o retiro seguro de equipos

La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento. Los medios de almacenamiento conteniendo material sensible, por ejemplo discos rígidos no removibles, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda.

Los dispositivos que contengan información confidencial deben requerir una evaluación de riesgo para determinar si los ítems debieran ser físicamente destruidos en lugar de enviarlos a reparar o descartar.

11.2.7 Control: Retirada de materiales propiedad de las Instituciones Universitarias Públicas

El equipamiento y la información (no clasificada como pública) serán retirados de la sede de las Instituciones Universitarias Públicas solo con autorización formal.

Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de las Instituciones Universitarias Públicas, las que serán llevadas a cabo por el Área de Auditoría Interna. El personal será puesto en conocimiento de la posibilidad de realización de dichas comprobaciones.

Los empleados deben saber que se llevan a cabo chequeos inesperados, y los chequeos se deben realizar con la debida autorización de los requerimientos legales y reguladores.

11.2.8 Control: Políticas de Pantallas Limpias

Los usuarios deben 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 de la Información 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:

- a) 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.
- b) Proteger equipos informáticos contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

11.2.9 Control: Políticas de Escritorios Limpios

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles 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:

- a) 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.
- b) Guardar bajo llave la información sensible o crítica de las Instituciones Universitarias Públicas (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.
- c) 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.

- d) Proteger los puntos de recepción y envío de correo postal y las máquinas de fax no atendidas.
- e) Bloquear las fotocopiadoras (o protegerlas de alguna manera del uso no autorizado) fuera del horario normal de trabajo.
- f) Retirar inmediatamente la información sensible o confidencial, una vez impresa.

12. Cláusula: Seguridad en las Operaciones

Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.

Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones:

12.1 Categoría: Procedimientos y Responsabilidades operativas

Objetivo

Asegurar la operación correcta y segura de los medios de procesamiento de la información.

Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información. Esto incluye el desarrollo de los procedimientos de operación apropiados

12.1.1 Control: 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 Seguridad de la Información.

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

- a) Procesamiento y manejo de la información.
- b) Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.
- c) Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
- d) Restricciones en el uso de utilitarios del sistema.
- e) Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.
- f) 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.
- g) 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:

- a) Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.
- b) Instalación y mantenimiento de las plataformas de procesamiento.
- c) Monitoreo del procesamiento y las comunicaciones.
- d) Inicio y finalización de la ejecución de los sistemas.
- e) Programación y ejecución de procesos.
- f) Gestión de servicios.
- g) Resguardo de información.
- h) Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.
- i) Reemplazo o cambio de componentes del ambiente de procesamiento y comunicaciones.
- j) Uso del correo electrónico.

12.1.2 Control: Cambios en las Operaciones

Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio debe ser evaluado previamente en aspectos técnicos y de seguridad.

El Responsable de Seguridad de la Información controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. El Responsable del Área Informática evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

Se retendrá un registro de auditoría que contenga toda la información relevante de cada cambio implementado.

Los procedimientos de control de cambios contemplarán los siguientes puntos:

- a) Identificación y registro de cambios significativos.
- b) Evaluación del posible impacto de dichos cambios.
- c) Aprobación formal de los cambios propuestos.
- d) Planificación del proceso de cambio.
- e) Prueba del nuevo escenario.
- f) Comunicación de detalles de cambios a todas las personas pertinentes.
- g) Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

12.1.3 Control: Planificación de la Capacidad

El Responsable del Área Informática, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados. Para ello tomará en cuenta además los nuevos requerimientos de los sistemas así como las tendencias actuales y proyectadas en el procesamiento de la información de las Instituciones Universitarias Públicas para el período estipulado de vida útil de cada componente. Asimismo, informará las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva.

12.1.4 Control: Separación de entornos de desarrollo, pruebas y operacionales

Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado productivo.

Para ello, se tendrán en cuenta los siguientes controles:

- a) Ejecutar el software de desarrollo y de producción, en diferentes ambientes de operaciones, equipos, o directorios.
- b) Separar las actividades de desarrollo y prueba, en entornos diferentes.
- c) Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente de producción, cuando no sean indispensables para el funcionamiento del mismo.
- d) Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.
- e) Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes.
- f) El personal de desarrollo no tendrá acceso al ambiente productivo. De ser extrema dicha necesidad, se establecerá un procedimiento de emergencia para la autorización, documentación y registro de dichos accesos.

12.2 Categoría: Protección contra el malware (código malicioso)

Objetivo

Proteger la integridad del software y la integración. Se requiere tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados. El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos; como ser, entre otros, virus Troyanos, bombas lógicas, etc. Se deberá concientizar a todos los miembros de la comunidad respecto a los peligros de los códigos maliciosos.

12.2.1 Control: Control contra el malware (código malicioso)

El Responsable de Seguridad de la Información definirá controles de detección y prevención para la protección contra software malicioso. El Responsable del Área Informática, o el personal designado por éste, implementará dichos controles.

El Responsable de Seguridad de la Información desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios. Estos controles deben considerar establecer políticas y procedimientos formales que contemplen las siguientes acciones:

- a) Prohibir la instalación y uso de software no autorizado por las Instituciones Universitarias Públicas (Ver "18.1.2 Control: Derecho de Propiedad Intelectual").
- b) Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio (ej: dispositivos portátiles), señalando las medidas de protección a tomar.
- c) Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, como medida precautoria y rutinaria.
- d) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).
- e) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de las Instituciones Universitarias Públicas, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
- f) Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
- g) Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.
- h) Concientizar al personal acerca del problema de los falsos antivirus (rogues) y las cadenas falsas (hoax) y de cómo proceder frente a los mismos.
- i) Redactar normas de protección y habilitación de puertos de conexión de dispositivos móviles y sus derechos de acceso.

12.2.2 Control: Código Móvil

En caso que el código móvil sea autorizado, se debe garantizar que la configuración asegure que el código móvil autorizado opere de acuerdo a una configuración de seguridad claramente definida, previniendo que el código móvil no autorizado sea ejecutado.

Asimismo, se implementarán acciones para la protección contra acciones maliciosas resultantes de la ejecución no autorizada de código móvil, como ser:

- a) ejecución del código móvil en un ambiente lógicamente aislado;
- b) bloqueo del uso de código móvil;
- c) bloqueo de la recepción de código móvil;
- d) activación de medidas técnicas como sea disponible en un sistema específico para asegurar que el código móvil es gestionado;
- e) control de los recursos disponibles para el acceso del código móvil;
- f) implementación de controles criptográficos para autenticar de forma unívoca el código móvil.

12.3 Categoría: Resguardo (backup)

Objetivo

Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.

Se deben establecer los procedimientos de rutina para implementar la política de respaldo acordada y la estrategia (ver también Cláusula 17.1 Categoría: Gestión de Continuidad de las Instituciones Universitarias Públicas) para tomar copias de respaldo de los datos y practicar su restauración oportuna.

12.3.1 Control: Resguardo de la Información

El Responsable del Área Informática, de Seguridad de la Información y los Propietarios de Información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información.

El Responsable del Área Informática dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración e integridad. Para esto se debe contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico de las Instituciones Universitarias Públicas. Los sistemas de resguardo deben probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades de las Instituciones Universitarias Públicas, según el punto (ver también "Cláusula

17.1 Categoría: Gestión de Continuidad de las Instituciones Universitarias Públicas”).

Se definirán procedimientos para el resguardo de la información, que deben considerar los siguientes puntos:

- a) Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.
- b) Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor, y asegurando la destrucción de los medios desechados.
- c) Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deben retener al menos tres generaciones o ciclos de información de resguardo para la información y el software esenciales para las Instituciones Universitarias Públicas. Para la definición de información mínima a ser resguardada en el sitio remoto, se debe tener en cuenta el nivel de clasificación otorgado a la misma, en términos de disponibilidad y requisitos legales a los que se encuentre sujeta.
- d) Asignar a la información de resguardo un nivel de protección física y ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.
- e) Probar periódicamente los medios de resguardo.
- f) Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

12.4 Categoría: Registro y Monitoreo

Objetivo

Detectar las actividades de procesamiento de información no autorizadas.

Se deben monitorear los sistemas y se deben reportar los eventos de seguridad de la información. Se deben utilizar bitácoras de operador y se deben registrar las fallas para asegurar que se identifiquen los problemas en los sistemas de información. Las Instituciones Universitarias Públicas debe cumplir con todos los requerimientos legales relevantes aplicables a sus actividades de monitoreo y registro.

Se debe utilizar el monitoreo del sistema para chequear la efectividad de los controles adoptados y para verificar la conformidad con un modelo de política de acceso.

12.4.1 Control: Registro de eventos

Se producirán y mantendrán registros de auditoría en los cuales se registren las actividades, excepciones, y eventos de seguridad de la información de los usuarios, por un período acordado para permitir la detección e investigación de incidentes.

Se debe evaluar la registración, en los mencionados registros, de la siguiente información:

- a) identificación de los usuarios;
- b) fechas, tiempos, y detalles de los eventos principales, por ejemplo, inicio y cierre de sesión;
- c) identidad del equipo o la ubicación si es posible;
- d) registros de intentos de acceso al sistema exitosos y fallidos;
- e) registros de intentos de acceso a los datos u otro recurso, exitosos y rechazados;
- f) cambios a la configuración del sistema;
- g) uso de privilegios;
- h) uso de utilitarios y aplicaciones de sistemas;
- i) archivos accedidos y el tipo de acceso;
- j) direcciones de redes y protocolos;
- k) alarmas que son ejecutadas por el sistema de control de accesos;
- l) activación y desactivación de los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusos.

12.4.2 Control: Protección del registro de información

Se implementarán controles para la protección de los registros de auditoría contra cambios no autorizados y problemas operacionales, incluyendo:

- a) alteraciones de los tipos de mensajes que son grabados;
- b) edición o eliminación de archivos de registro;
- c) pérdida de registro de eventos debido a la saturación de la capacidad de almacenamiento.

12.4.3 Control: Registro del Administrador y del Operador

Se registrarán y revisarán periódicamente en particular las actividades de los

administradores y operadores de sistema incluyendo:

- a) cuenta de administración u operación involucrada;
- b) fecha y hora del evento (éxito o falla);
- c) información acerca del evento (por ejemplo, los archivos manipulados) o las fallas (por ejemplo, los errores ocurridos y las acciones correctivas tomadas);
- d) procesos involucrados.

12.4.4 Control: Sincronización de Relojes

A fin de garantizar la exactitud de los registros de auditoría, al menos los equipos que realicen estos registros, deben tener una correcta configuración de sus relojes.

Para ello, se dispondrá de un procedimiento de ajuste de relojes, el cual indicará también la verificación de los relojes contra una fuente externa del dato y la modalidad de corrección ante cualquier variación significativa.

12.5 Categoría: Control de Software Operacional

Objetivo

Garantizar la seguridad de los archivos del sistema.

Se debe controlar el acceso a los archivos del sistema y el código fuente del programa, y los proyectos TI. Asimismo, las actividades de soporte se debieran realizar de una manera segura.

12.5.1 Control: Instalación de software en sistemas operacionales

Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.

- Toda aplicación, desarrollada por las Instituciones Universitarias Públicas o por un tercero tendrá un único Responsable designado formalmente por el Responsable del Área Informática.
- Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.
- El Responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de la función de "implementador" al personal de su área que considere adecuado, quien

tendrá como funciones principales:

- a) Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.
- b) Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.
- c) Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del sector encargado del testeo y del usuario final.
- d) Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

Otros controles a realizar son:

- a) Guardar sólo los ejecutables en el ambiente de producción.
- b) Llevar un registro de auditoría de las actualizaciones realizadas.
- c) Retener las versiones previas del sistema, como medida de contingencia.
- d) Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y conformidades pertinentes, las pruebas previas a realizarse, etc.
- e) Denegar, cuando correspondiere, permisos de modificación al implementador sobre los programas fuentes bajo su custodia.

Evitar, que la función de implementador sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.

12.6 Categoría: Administración de vulnerabilidades técnicas

Objetivo

Se implementará la gestión de las vulnerabilidades técnicas de forma efectiva, sistemática y repetible, con mediciones que confirmen su efectividad. Dichas consideraciones incluirán los sistemas operativos, y cualquier otra aplicación en uso.

12.6.1 Control: Administración de vulnerabilidades técnicas

Se obtendrá información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, la exposición de las Instituciones

Universitarias Públicas a tales vulnerabilidades evaluadas, y se tomarán las medidas necesarias para tratar los riesgos asociados.

Para ello se contará con un inventario de software donde se detalle información de versiones del mismo así como datos del proveedor y responsable interno.

El proceso de gestión de las vulnerabilidades técnicas debe comprender:

- a) Definición de roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas;
- b) Procedimientos de identificación de vulnerabilidades técnicas potenciales;
- c) Definición de una línea de tiempo para reaccionar ante las notificaciones de las vulnerabilidades técnicas potencialmente relevantes;
- d) Definición de prioridades para la atención de necesidades relacionadas con actualizaciones de seguridad;
- e) Identificación de los riesgos asociados y las acciones a llevar a cabo ante vulnerabilidades identificadas;
- f) Identificación de los riesgos asociados a la instalación de parches;
- g) Aprobación y evaluación de los parches antes de que sean instalados para garantizar que son efectivos y que no resultan en efectos secundarios que no puedan ser tolerados;
- h) Consideración de controles alternativos en caso de inexistencia de parches;
- i) Generación y mantenimiento de un registro de auditoría para todos los procedimientos emprendidos;
- j) Seguimiento y evaluación regular del proceso de gestión de las vulnerabilidades técnicas para garantizar su efectividad y eficiencia;

12.6.2 Control: Restricciones en la instalación de software

Se deben establecer e implementar:

- las reglas que rigen la instalación de software por parte de los usuarios y poner en vigencia una política estricta sobre qué tipo de software pueden instalar los usuarios.

La instalación no controlada de software en dispositivos computacionales puede dar pie a la introducción de vulnerabilidades y a la fuga de información, a la falta de integridad u otros incidentes de seguridad de información o bien a la transgresión de derechos de propiedad intelectual.

12.7 Categoría: Consideraciones sobre la auditoría de los sistemas de información

Objetivo

Asegurar el cumplimiento de minimizar el impacto de las actividades de auditoría en los sistemas operacionales.

12.7.1 Control: Controles de auditoría de los sistemas de información

Cuando se realicen actividades de auditoría que involucren verificaciones de los sistemas en producción, se tomarán recaudos en la planificación de los requerimientos y tareas, y se acordará con las áreas involucradas a efectos de minimizar el riesgo de interrupciones en las operaciones.

Se contemplarán los siguientes puntos:

- a) Acordar con el Área que corresponda los requerimientos de auditoría.
- b) Controlar el alcance de las verificaciones. Esta función será realizada por el responsable de auditoría.
- c) Limitar las verificaciones a un acceso de sólo lectura del software y datos de producción. Caso contrario, se tomarán los resguardos necesarios a efectos de aislar y contrarrestar los efectos de las modificaciones realizadas, una vez finalizada la auditoría. Por ejemplo:
 - Eliminar archivos transitorios.
 - Eliminar entidades ficticias y datos incorporados en archivos maestros.
 - Revertir transacciones.
 - Revocar privilegios otorgados.
- d) Identificar claramente los recursos de tecnologías de información (TI) para llevar a cabo las verificaciones, los cuales serán puestos a disposición de los auditores. A tal efecto, la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información completará el formulario incluido en el "Anexo - Herramientas de auditoría", el cual debe ser puesto en conocimiento de las áreas involucradas.
- e) Identificar y acordar los requerimientos de procesamiento especial o adicional.
- f) Monitorear y registrar todos los accesos, a fin de generar una pista de referencia. Los datos a resguardar deben incluir como mínimo:
 - Fecha y hora.
 - Puesto de trabajo.
 - Usuario.
 - Tipo de acceso.
 - Identificación de los datos accedidos.
 - Estado previo y posterior.
 - Programa y/o función utilizada.

- g) Documentar todos los procedimientos de auditoría, requerimientos y responsabilidades.

13. Cláusula: Gestión de Comunicaciones

Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

13.1 Categoría: Gestión de la Red

Objetivo

Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicancias legales, monitoreo y protección.

También se pueden requerir controles adicionales para proteger la información confidencial que pasa a través de redes públicas.

13.1.1 Control: Redes

El Responsable de Seguridad de la Información definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes de las Instituciones Universitarias Públicas, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

- a) Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias, la que será llevada a cabo por el responsable establecido en el punto "6.1.3 Control: Asignación de responsabilidad de la seguridad de la información".
- b) Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados. Implementar controles

especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.

- c) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

El Responsable del Área Informática implementará dichos controles.

13.1.2 Control: Seguridad de Servicio de red

El Responsable de Seguridad de la Información junto con el Responsable del Área Informática definirán las pautas para garantizar la seguridad de los servicios de red de las Instituciones Universitarias Públicas, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.
- Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.
- Instalar periódicamente las actualizaciones de seguridad.
- Dicha configuración será revisada periódicamente por el Responsable de Seguridad de la Información.

13.2 Categoría: Transferencia de información

Objetivo

Mantener la seguridad en el intercambio de información dentro de las Instituciones Universitarias Públicas y con cualquier otra entidad externa.

Los intercambios de información dentro de las organizaciones se deben basar en una política formal de intercambio, seguida en línea con los acuerdos de intercambio, y debiera cumplir con cualquier legislación relevante (ver 18 Cláusula: Cumplimiento).

Se deben establecer los procedimientos y estándares para proteger la información y los medios físicos que contiene la información en tránsito.

13.2.1 Control: Procedimientos y controles de intercambio de la información

Se establecerán procedimientos y controles formales para proteger el intercambio de información a través del uso de todos los tipos de instalaciones de comunicación, considerando lo siguiente:

- a) Protección de la información intercambiada de la interceptación, copiado, modificación, de que sea mal dirigida, y de su destrucción.
- b) Detección de y la protección contra el código malicioso que puede ser transmitido a través del uso de comunicaciones electrónicas.
- c) Definición del uso aceptable de las instalaciones de comunicación electrónicas.
- d) Uso seguro de comunicaciones inalámbricas.
- e) Responsabilidades del empleado, contratista y cualquier otro usuario de no comprometer a las Instituciones Universitarias Públicas, por ejemplo, a través de la difamación, hostigamiento, personificación, reenvío de cadenas de comunicación epistolar, compras no autorizadas y cualquier otro medio (ej.: redes sociales).
- f) Uso de técnicas criptográficas para proteger la confidencialidad, integridad y la autenticidad de la información.
- g) Directrices de retención y eliminación para toda la correspondencia en concordancia con las leyes y regulaciones relevantes, locales y nacionales.
- h) Instrucción del personal sobre las precauciones que deben tomar a la hora de transmitir información de las Instituciones Universitarias Públicas.

13.2.2 Control: Acuerdos de Intercambio de Información

Cuando se realicen acuerdos entre organizaciones para el intercambio de información y software, se especificarán el grado de sensibilidad de la información de las Instituciones Universitarias Públicas involucrada y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos:

- a) Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.
- b) Procedimientos de notificación de emisión, transmisión, envío y recepción.
- c) Normas técnicas para el empaquetado y la transmisión.
- d) Pautas para la identificación del prestador del servicio de correo.
- e) Responsabilidades y obligaciones en caso de pérdida, exposición o divulgación no autorizada de datos.
- f) Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida.

- g) Términos y condiciones de la licencia bajo la cual se suministra el software.
- h) Información sobre la propiedad de la información suministrada y las condiciones de su uso.
- i) Normas técnicas para la grabación y lectura de la información y del software.
- j) Controles especiales que puedan requerirse para proteger ítems sensibles, (claves criptográficas, etc.).

13.2.3 Control: Seguridad de la Mensajería

La mensajería electrónica como el correo electrónico, el intercambio de datos electrónicos, la mensajería instantánea y las redes sociales juegan un papel muy importante en las comunicaciones organizacionales. La mensajería electrónica tiene diferentes riesgos que las comunicaciones basadas en papel.

Se considerarán las siguientes medidas de seguridad en los mensajes electrónicos:

- protección de mensajes por el acceso no autorizado, modificaciones o denegación de servicio;
- correcta asignación de la dirección y el transporte del mensaje;
- confiabilidad y disponibilidad general del servicio;
- consideraciones legales, por ejemplo, requerimientos para firmas electrónicas;
- obtención de aprobación previa al uso de los servicios públicos externos tales como mensajería instantánea o el compartir archivos;
- niveles altos de controles de autenticación para los accesos desde las redes públicamente accesibles.

13.2.4 Control: Acuerdos de confidencialidad.

Se definirán, implementarán y revisarán regularmente los acuerdos de confidencialidad o de no divulgación para la protección de la información de las Instituciones Universitarias Públicas. Dichos acuerdos deben responder a los requerimientos de confidencialidad o no divulgación de las Instituciones Universitarias Públicas, los cuales serán revisados periódicamente. Asimismo, deben cumplir con toda legislación o normativa que alcance a las Instituciones Universitarias Públicas en materia de confidencialidad de la información.

Dichos acuerdos deben celebrarse tanto con el personal de las Instituciones Universitarias Públicas como con aquellos terceros que se relacionen de alguna manera con su información.

14. Cláusula: Adquisición, desarrollo y mantenimiento de sistemas

Objetivo

Asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información.

Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

Definir los métodos de protección de la información crítica o sensible.

14.1 Categoría: Requerimientos de Seguridad de los Sistemas

Objetivo

Garantizar que la seguridad sea una parte integral de los sistemas de información.

Los sistemas de información incluyen sistemas de operación, infraestructura, aplicaciones operativas, productos de venta masiva, servicios y aplicaciones desarrolladas por el usuario. El diseño e implementación del sistema de información que soporta el proceso operativo puede ser crucial para la seguridad. Se deben identificar y acordar los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información.

14.1.1 Control: Análisis y Especificaciones de los Requerimientos de seguridad

Esta Política se implementa para incorporar seguridad a los sistemas de información (propios o de terceros) y a las mejoras o actualizaciones que se les incorporen.

Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles manuales de apoyo.

Se deben tener en cuenta las siguientes consideraciones:

- a) Definir un procedimiento para que durante las etapas de análisis y diseño del sistema, se incorporen a los requerimientos, los correspondientes controles de seguridad. Este procedimiento debe incluir una etapa de evaluación de riesgos previa al diseño, para definir los requerimientos de seguridad e identificar los controles apropiados. En esta tarea deben participar las áreas usuarias, de sistemas, de seguridad informática y auditoría, especificando y aprobando los controles automáticos a incorporar al sistema y las necesidades de controles manuales complementarios. Las áreas involucradas podrán solicitar certificaciones y evaluaciones independientes para los productos a utilizar.
- b) Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar la materialización de amenazas en las actividades realizadas.
- c) Considerar que los controles introducidos en la etapa de diseño, son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.

14.1.2 Control: Seguridad de servicios aplicativos en redes públicas

Se controlarán los mecanismos de distribución y difusión tales como documentos, computadoras, dispositivos de computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general (analógica o digital), multimedia, servicios o instalaciones postales, equipos de fax, etc.

Al interconectar dichos medios, se considerarán las implicancias en lo que respecta a la seguridad y a las actividades propias de las Instituciones Universitarias Públicas, incluyendo:

- a) Vulnerabilidades de la información en los sistemas de oficina, por ejemplo la grabación de llamadas telefónicas o teleconferencias, la confidencialidad de las llamadas, el almacenamiento de faxes, la apertura o distribución del correo.
- b) Procedimientos y controles apropiados para administrar la distribución de información, por ejemplo el uso de boletines electrónicos institucionales.
- c) Exclusión de categorías de información sensible de las Instituciones Universitarias Públicas, si el sistema no brinda un adecuado nivel de protección.
- d) Restricción del acceso a la información de las actividades que desarrollan determinadas personas, por ejemplo aquellas que trabajan en proyectos sensibles.
- e) La aptitud del sistema para dar soporte a las aplicaciones de las Instituciones Universitarias Públicas, como la comunicación de órdenes o autorizaciones.
- f) Categorías de personal y contratistas o terceros a los que se permite el uso

del sistema y las ubicaciones desde las cuales se puede acceder al mismo.

- g) Restricción de acceso a determinadas instalaciones a específicas categorías de usuarios.
- h) Identificación de la posición o categoría de los usuarios, por ejemplo empleados de las Instituciones Universitarias Públicas o contratistas, en directorios accesibles por otros usuarios.
- i) Retención y resguardo de la información almacenada en el sistema.
- j) Requerimientos y disposiciones relativos a sistemas de soporte de reposición de información previa.

14.1.3 Control: Protección de servicios de aplicativos

Se tomarán recaudos para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada que podría, por ejemplo, dañar la reputación de las Instituciones Universitarias Públicas que emite la publicación. Es posible que la información de un sistema de acceso público, por ejemplo la información en un servidor Web accesible por Internet, deba cumplir con ciertas normas de la jurisdicción en la cual se localiza el sistema o en la cual tiene lugar la transacción electrónica. Se implementará un proceso de autorización formal antes de que la información se ponga a disposición del público, estableciéndose en todos los casos los encargados de dicha aprobación.

Todos los sistemas de acceso público deben prever que:

- a) La información se obtenga, procese, proporcione y/o publique de acuerdo a la normativa vigente, en especial la Ley 25.326 de Protección de Datos Personales.
- b) La información que se ingresa al sistema de publicación, o aquella que procesa el mismo, sea procesada en forma completa, exacta y oportuna.
- c) La información sensible o confidencial sea protegida durante el proceso de recolección y su almacenamiento, así como también al momento de su cesión o transferencia.
- d) El acceso al sistema de publicación no permita el acceso accidental a las redes a las cuales se conecta el mismo.
- e) El responsable de la publicación de información en sistemas de acceso público sea claramente identificado.
- f) Se garantice la validez y vigencia de la información publicada.

14.2 Categoría: Seguridad en los Sistemas de Aplicación

Objetivo

Para evitar la pérdida, modificación o uso inadecuado de los datos pertenecientes a los sistemas de información, se establecerán controles y registros de auditoría, verificando:

- a) La validación efectiva de datos de entrada.
- b) El procesamiento interno.
- c) La autenticación de mensajes (interfaces entre sistemas)
- d) La validación de datos de salida.

14.2.1 Control: Validación de Datos de Entrada

Se definirá un procedimiento que durante la etapa de diseño, especifique controles que aseguren la validez de los datos ingresados, tan cerca del punto de origen como sea posible, controlando también datos permanentes y tablas de parámetros.

Este procedimiento considerará los siguientes controles:

- a) Control de secuencia.
- b) Control de monto límite por operación y tipo de usuario.
- c) Control del rango de valores posibles y de su validez, de acuerdo a criterios predeterminados.
- d) Control de paridad.
- e) Control contra valores cargados en las tablas de datos.
- f) Controles por oposición, de forma tal que quien ingrese un dato no pueda autorizarlo y viceversa.

Por otra parte, se llevarán a cabo las siguientes acciones:

- a) Se definirá un procedimiento para realizar revisiones periódicas de contenidos de campos claves o archivos de datos, definiendo quién lo realizará, en qué forma, con qué método, quiénes deben ser informados del resultado, etc.
- b) Se definirá un procedimiento que explicita las alternativas a seguir para responder a errores de validación en un aplicativo.
- c) Se definirá un procedimiento que permita determinar las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

14.2.2 Control: Controles de Procesamiento Interno

Se definirá un procedimiento para que durante la etapa de diseño, se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.

Para ello se implementarán:

- a) Procedimientos que permitan identificar el uso y localización en los aplicativos, de funciones de incorporación y eliminación que realizan cambios en los datos.
- b) Procedimientos que establezcan los controles y verificaciones necesarios para prevenir la ejecución de programas fuera de secuencia o cuando falle el procesamiento previo.
- c) Procedimientos que establezcan la revisión periódica de los registros de auditoría o alertas de forma de detectar cualquier anomalía en la ejecución de las transacciones.
- d) Procedimientos que realicen la validación de los datos generados por el sistema.
- e) Procedimientos que verifiquen la integridad de los datos y del software cargado o descargado entre computadoras.
- f) Procedimientos que controlen la integridad de registros y archivos.
- g) Procedimientos que verifiquen la ejecución de los aplicativos en el momento adecuado.
- h) Procedimientos que aseguren el orden correcto de ejecución de los aplicativos, la finalización programada en caso de falla, y la detención de las actividades de procesamiento hasta que el problema sea resuelto.

14.2.3 Control: Autenticación de Mensajes

Cuando una aplicación tenga previsto el envío de mensajes que contengan información clasificada, se implementarán los controles criptográficos determinados en el punto 10.1.1 Control: Política de Utilización de Controles Criptográficos.

14.2.4 Control: Validación de Datos de Salidas

Se establecerán procedimientos para validar la salida de los datos de las aplicaciones, incluyendo:

- a) Comprobaciones de la razonabilidad para probar si los datos de salida son plausibles.
- b) Control de conciliación de cuentas para asegurar el procesamiento de todos los datos.

- c) Provisión de información suficiente, para que el lector o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información.
- d) Procedimientos para proceder en función de los resultados de las pruebas de validación de salidas.
- e) Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

14.3 Categoría: Seguridad de los Archivos del Sistema

Objetivo

Se garantizará que los desarrollos y actividades de soporte a los sistemas se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo.

14.3.1 Control: Software Operativo

Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.

- Toda aplicación, desarrollada por las Instituciones Universitarias Públicas o por un tercero tendrá un único Responsable designado formalmente por el Responsable del Área Informática.
- Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.
- El Responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de la función de "implementador" al personal de su área que considere adecuado, quien tendrá como funciones principales:
 - a) Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.
 - b) Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.
 - c) Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del sector encargado del testeo y del usuario final.
 - d) Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

Otros controles a realizar son:

- e) Guardar sólo los ejecutables en el ambiente de producción.
- f) Llevar un registro de auditoría de las actualizaciones realizadas.
- g) Retener las versiones previas del sistema, como medida de contingencia.
- h) Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y conformes pertinentes, las pruebas previas a realizarse, etc.
- i) Denegar permisos de modificación al implementador sobre los programas fuentes bajo su custodia.
- j) Evitar, que la función de implementador sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.

14.3.2 Control: Protección de los Datos de Prueba del Sistema

Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo. Para proteger los datos de prueba se establecerán normas y procedimientos que contemplen lo siguiente:

Prohibir el uso de bases de datos operativas. En caso contrario se deben despersonalizar los datos antes de su uso. Aplicar idénticos procedimientos de control de acceso que en la base de producción. Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización.

Eliminar inmediatamente, una vez completadas las pruebas, la información operativa utilizada.

14.3.3 Control: Cambios a Datos Operativos

La modificación, actualización o eliminación de los datos operativos serán realizados a través de los sistemas que procesan dichos datos y de acuerdo al esquema de control de accesos implementado en los mismos. Una modificación por fuera de los sistemas a un dato, almacenado ya sea en un archivo o base de datos, podría poner en riesgo la integridad de la información.

Los casos en los que no fuera posible la aplicación de la precedente política, se considerarán como excepciones. El Responsable de Seguridad de la Información definirá procedimientos para la gestión de dichas excepciones que contemplarán lo siguiente:

- a) Se generará una solicitud formal para la realización de la modificación, actualización o eliminación del dato.

- b) El Propietario de la Información afectada y el Responsable de Seguridad de la Información aprobarán la ejecución del cambio evaluando las razones por las cuales se solicita.
- c) Se generarán cuentas de usuario de emergencia para ser utilizadas en la ejecución de excepciones. Las mismas serán protegidas mediante contraseñas, sujetas al procedimiento de administración de contraseñas críticas y habilitadas sólo ante un requerimiento de emergencia y por el lapso que ésta dure.
- d) Se designará un encargado de implementar los cambios, el cual no será personal del área de Desarrollo. En el caso de que esta función no pueda ser segregada, se aplicarán controles adicionales de acuerdo a lo establecido en la Cláusula 7 Recursos Humanos.
- e) Se registrarán todas las actividades realizadas con las cuentas de emergencia. Dicho registro será revisado posteriormente por el Responsable de Seguridad de la Información.

14.3.4 Control: Acceso a las Bibliotecas de Programas fuentes

Para reducir la probabilidad de alteración de programas fuentes, se aplicarán los siguientes controles:

- a) El Responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda la función de "administrador de programas fuentes" al personal de su área que considere adecuado, quien tendrá en custodia los programas fuentes y debe:
 - Proveer al Área de Desarrollo los programas fuentes solicitados para su modificación, manteniendo en todo momento la correlación programa fuente / ejecutable.
 - Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, Analista Responsable que autorizó, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).
 - Verificar que el Analista Responsable que autoriza la solicitud de un programa fuente sea el designado para la aplicación, rechazando el pedido en caso contrario. Registrar cada solicitud aprobada.
 - Administrar las distintas versiones de una aplicación.
 - Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador.
- b) Denegar al "administrador de programas fuentes" permisos de modificación sobre los programas fuentes bajo su custodia.
- c) Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.

- d) Establecer que el implementador de producción efectuará la generación del programa objeto o ejecutable que estará en producción (compilación), a fin de garantizar tal correspondencia.
- e) Desarrollar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática.
- f) Evitar que la función de “administrador de programas fuentes” sea ejercida por personal que pertenezca al sector de desarrollo y/o mantenimiento.
- g) Prohibir la guarda de programas fuentes históricos (que no sean los correspondientes a los programas operativos) en el ambiente de producción.
- h) Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.
- i) Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos por las Instituciones Universitarias Públicas en los procedimientos que surgen de la presente política.

14.4 Categoría: Seguridad de los Procesos de Desarrollo y Soporte

Objetivo

Esta Política provee seguridad al software y a la información del sistema de aplicación, por lo tanto se controlarán los entornos y el soporte dado a los mismos.

14.4.1 Control: 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:

- a) Verificar que los cambios sean propuestos por usuarios autorizados y respete los términos y condiciones que surjan de la licencia de uso.
- b) Mantener un registro de los niveles de autorización acordados.

- c) Solicitar la autorización del Propietario de la Información, en caso de tratarse de cambios a sistemas de procesamiento de la misma.
- d) Efectuar un análisis de riesgos del cambio.
- e) Determinar los requisitos de seguridad para el cambio.
- f) Analizar el impacto de los cambios sobre los controles de seguridad existentes.
- g) Obtener aprobación formal por parte del Responsable del Área Informática para las tareas detalladas, antes que comiencen las tareas.
- h) Solicitar la revisión del Responsable de Seguridad de la Información para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.
- i) Efectuar las actividades relativas al cambio en el ambiente de desarrollo.
- j) Obtener la aprobación por parte del usuario autorizado y del área de pruebas mediante pruebas en el ambiente correspondiente.
- k) Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
- l) Mantener un control de versiones para todas las actualizaciones de software.
- m) Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.
- n) Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria.
- o) Garantizar que sea el implementador quien efectúe el pasaje de los objetos modificados al ambiente operativo, de acuerdo a lo establecido en "14.3.1 Control: Software Operativo".

En el Anexo - Segregación de ambientes se presenta un esquema modelo de segregación de ambientes de procesamiento.

14.4.2 Control: Revisión Técnica de los Cambios en el sistema Operativo

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

Para ello, se definirá un procedimiento que incluya:

- a) Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.
- b) Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación.
- c) Asegurar la actualización del Plan de Continuidad de las Actividades de las Instituciones Universitarias Públicas.

14.4.3 Control: Restricción del Cambio de Paquetes de Software

En caso de considerarlo necesario la modificación de paquetes de software suministrados por proveedores, y previa autorización del Responsable del Área Informática, se debe:

- a) Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
- b) Determinar la conveniencia de que la modificación sea efectuada por las Instituciones Universitarias Públicas, por el proveedor o por un tercero.
- c) Evaluar el impacto que se produciría si las Instituciones Universitarias Públicas se hace cargo del mantenimiento.
- d) Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

14.4.4 Control: Canales Ocultos y Código Malicioso

Un canal oculto puede exponer información utilizando algunos medios indirectos y desconocidos. El código malicioso está diseñado para afectar a un sistema en forma no autorizada y no requerida por el usuario.

En este sentido, se redactarán normas y procedimientos que incluyan:

- a) Adquirir programas a proveedores acreditados o productos ya evaluados.
- b) Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.
- c) Controlar el acceso y las modificaciones al código instalado.
- d) Utilizar herramientas para la protección contra la infección del software con código malicioso.
- e) Ejecutar controles y tests de evaluación de seguridad periódicamente y, en especial, previo a su puesta en producción.

14.4.5 Control: Desarrollo Externo de Software

Para el caso que se considere la tercerización del desarrollo de software, se establecerán normas y procedimientos que contemplen los siguientes puntos:

- a) Acuerdos de licencias, propiedad de código y derechos conferidos (Ver 18.1.2 Derechos de Propiedad Intelectual).

- b) Requerimientos contractuales con respecto a la calidad y seguridad del código y la existencia de garantías.
- c) Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.
- d) Verificación del cumplimiento de las condiciones de seguridad.
- e) Acuerdos de custodia de los fuentes del software (y cualquier otra información requerida) en caso de quiebra y/o inhabilidad de la tercera parte.

14.5 Categoría: Gestión de vulnerabilidades técnicas

Objetivo

Se implementará la gestión de las vulnerabilidades técnicas de forma efectiva, sistemática y repetible, con mediciones que confirmen su efectividad. Dichas consideraciones incluirán los sistemas operativos, y cualquier otra aplicación en uso.

14.5.1 Control: Vulnerabilidades técnicas

Se obtendrá información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, la exposición de las Instituciones Universitarias Públicas a tales vulnerabilidades evaluadas, y se tomarán las medidas necesarias para tratar los riesgos asociados.

Para ello se contará con un inventario de software donde se detalle información de versiones del mismo así como datos del proveedor y responsable interno.

El proceso de gestión de las vulnerabilidades técnicas debe comprender:

- a) Definición de roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas;
- b) Procedimientos de identificación de vulnerabilidades técnicas potenciales;
- c) Definición de una línea de tiempo para reaccionar ante las notificaciones de las vulnerabilidades técnicas potencialmente relevantes;
- d) Definición de prioridades para la atención de necesidades relacionadas con actualizaciones de seguridad;
- e) Identificación de los riesgos asociados y las acciones a llevar a cabo ante vulnerabilidades identificadas;

- f) Identificación de los riesgos asociados a la instalación de parches;
- g) Aprobación y evaluación de los parches antes de que sean instalados para garantizar que son efectivos y que no resultan en efectos secundarios que no puedan ser tolerados;
- h) Consideración de controles alternativos en caso de inexistencia de parches;
- i) Generación y mantenimiento de un registro de auditoría para todos los procedimientos emprendidos;
- j) Seguimiento y evaluación regular del proceso de gestión de las vulnerabilidades técnicas para garantizar su efectividad y eficiencia;

15. Cláusula: Relaciones con Proveedores

Objetivo

Establecer y mantener el nivel acordado de seguridad de información y prestación de servicios conforme a los acuerdos del proveedor.

15.1 Categoría: Seguridad de la información en las relaciones con el proveedor

Objetivo

Garantizar y asegurar la protección de la información de las Instituciones Universitarias Públicas que es accedida por los proveedores, cumpliendo con el nivel de seguridad establecido.

15.1.1 Control: Política de seguridad de la información para las relaciones con el proveedor

Se deben acordar los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso de los proveedores a los activos de las Instituciones Universitarias Públicas con el proveedor y se deben documentar debidamente.

Las Instituciones Universitarias Públicas debe identificar e imponer controles de seguridad de la información para abordar específicamente el acceso de los proveedores a la información de las Instituciones Universitarias Públicas en una política.

Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de equipamiento de trabajo de las Instituciones Universitarias Públicas, contemplarán los siguientes aspectos:

- a) la identificación y la documentación de los tipos de proveedores, es decir, los servicios de TI, las utilidades de logística, los servicios financieros, los componentes de la infraestructura de TI y a quiénes autorizará a las Instituciones Universitarias Públicas para acceder a su información;
- b) un proceso y ciclo de vida estandarizado para administrar las relaciones con los proveedores;
- c) la definición de los tipos de acceso a la información que se les permitirá a los distintos tipos de proveedores y el monitoreo y control del acceso;
- d) requisitos mínimos de seguridad de la información para cada tipo de información y tipo de acceso para servir de base para los acuerdos individuales con los proveedores en base a las necesidades de las Instituciones Universitarias Públicas y los requisitos y su perfil de riesgo;
- e) procesos y procedimientos para monitorear la adherencia a los requisitos de seguridad de información establecidos para cada tipo de proveedor y tipo de acceso, incluida la revisión de terceros y la validación de productos;
- f) controles de precisión y nivel de detalles para garantizar la integridad de la información o el procesamiento de información que entrega cualquiera de las partes;
- g) tipos de obligaciones aplicables a los proveedores para proteger la información;
- h) manejo de incidentes y contingencias asociadas con el acceso a los proveedores, incluidas las responsabilidades de las Instituciones Universitarias Públicas y los proveedores;
- i) resiliencia y, en caso de ser necesario, disposiciones de recuperación y contingencia para garantizar la disponibilidad de la información o el procesamiento de información proporcionado por cualquiera de las partes;
- j) capacitación de concientización para el personal de las Instituciones Universitarias Públicas involucrado en las adquisiciones sobre políticas, procesos y procedimientos correspondientes;
- k) capacitación de concientización para el personal de las Instituciones Universitarias Públicas que interactúa con el personal de los proveedores en cuanto a las reglas adecuadas sobre el compromiso y el comportamiento en base al tipo de proveedor y el nivel de acceso del proveedor a los sistemas y la información de las Instituciones Universitarias Públicas;
- l) que las condiciones sobre los controles y requisitos de seguridad de la información se documentarán en un acuerdo firmado por ambas partes;
- m) administración de las transiciones necesarias de información, instalaciones de procesamiento de información y cualquier otra cosa que se deba mover y, garantizando que se mantiene la seguridad de la información a través de todo el periodo de transición.

15.1.2 Control: Abordar la seguridad dentro de los acuerdos del proveedor

Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de las Instituciones Universitarias Públicas.

Se deben establecer y documentar acuerdos con los proveedores para garantizar que no existan malos entendidos entre las Instituciones Universitarias Públicas y el proveedor en cuanto a las obligaciones de ambas partes para cumplir con los requisitos de seguridad de la información pertinentes.

A continuación se definen los términos para incluir en los acuerdos a fin de y poder satisfacer los requisitos de seguridad de la información identificados:

- a) descripción de la información que se debe proporcionar o a la que se debe acceder y los métodos para proporcionar o acceder a la información;
- b) clasificación de la información de acuerdo al esquema de clasificación de las Instituciones Universitarias Públicas; y si es necesario también realizar el mapeo entre el esquema propio de las Instituciones Universitarias Públicas y el esquema de clasificación del proveedor;
- c) requisitos legales y normativos, incluida la protección de datos personales, los derechos de propiedad intelectual y una descripción de sobre cómo se garantizará si se cumplen;
- d) obligación de cada parte contractual de implementar un conjunto de controles acordados incluido el control de acceso, la revisión de desempeño, el monitoreo, los informes y la auditoría;
- e) reglas de uso aceptable de la información, incluido en uso inaceptable en caso de ser necesario;
- f) una lista explícita del personal autorizado para acceder a o recibir la información o los procedimientos o condiciones de las Instituciones Universitarias Públicas para su autorización y el retiro de la autorización, para el acceso a o la recepción de la información de las Instituciones Universitarias Públicas al personal del proveedor;
- g) políticas de seguridad de la información pertinentes al contrato específico;
- h) requisitos y procedimientos de la administración de incidentes (en especial la notificación y la colaboración durante la remediación de incidentes);
- i) requisitos de capacitación y concientización para procedimientos específicos y requisitos de seguridad de la información, es decir, para la respuesta ante incidentes y procedimientos de autorización;
- j) normativas pertinentes para la subcontratación, incluidos los controles que se deben implementar;
- k) socios de acuerdos pertinentes, incluida una persona de contacto para los asuntos de seguridad de la información;

- l) requisitos de selección, si existe alguno, para el personal del proveedor para realizar los procedimientos de selección y notificación si no se ha completado la selección o si los resultados dan pie a dudas o inquietudes;
- m) derecho a auditar los procesos y los controles del proveedor relacionados al acuerdo;
- n) procesos de resolución de defectos y resolución de conflictos;
- o) obligación del proveedor a entregar periódicamente un informe independiente sobre la efectividad de los controles y un acuerdo sobre la corrección oportuna de los asuntos pertinentes indicados en el informe;
- p) obligaciones del proveedor para cumplir con los requisitos de seguridad de las Instituciones Universitarias Públicas.

15.1.3 Control: Cadena de suministro de tecnologías de la información y comunicaciones

Se deben incluir en los acuerdos con los proveedores, los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.

Se deben incluir los siguientes temas en los acuerdos con el proveedor sobre la seguridad de la cadena de suministro:

- a) definir los requisitos de seguridad de la información que se aplicarán a la adquisición de tecnologías, productos o servicios de información y comunicación además de los requisitos de seguridad de la información para las relaciones con el proveedor;
- b) para los servicios de tecnología de información y comunicación, que requieren que los usuarios propaguen los requisitos de seguridad de las Instituciones Universitarias Públicas en toda la cadena de suministro si los proveedores realizan subcontrataciones para partes del servicio de tecnología de información y comunicación proporcionados a las Instituciones Universitarias Públicas;
- c) para los productos de tecnología de información y comunicación que requieren que los proveedores propaguen las prácticas de seguridad correspondientes a través de toda la cadena de suministro si estos productos incluyen componentes comprados a otros proveedores;
- d) implementación de un proceso de monitoreo y métodos aceptables para validar que los productos y servicios de tecnología de información y comunicación se adhieren a los requisitos de seguridad establecidos;
- e) implementación de un proceso para identificar los componentes de los productos o servicios que son fundamentales para mantener la funcionalidad y que, por lo tanto, requiere una mayor atención y escrutinio cuando se desarrollan fuera de las Instituciones Universitarias Públicas, especialmente

- si el proveedor del nivel superior externalice los aspectos de los componentes de productos o servicios a otros proveedores;
- f) obtención de una garantía de que los componentes críticos y su origen se pueden rastrear en toda la cadena de suministros;
 - g) obtener la garantía de que los productos de tecnología de información y comunicación entregados funcionan según lo esperado sin ninguna función inesperada o no deseada;
 - h) definición de las reglas para compartir la información en cuanto a la cadena de suministro y cualquier posible problema y compromiso entre las Instituciones Universitarias Públicas y los proveedores;
 - i) implementación de procesos específicos para administrar el ciclo de vida de los componentes de tecnología de información y comunicación junto con la disponibilidad y los riesgos de seguridad asociados. Esto incluye los riesgos de los componentes que ya no están disponibles debido a que los proveedores ya no están en el negocio o a que ya no proporcionan estos componentes debido a los avances de la tecnología.

15.2 Categoría: Administración de prestación de servicios de proveedores

Objetivo

Garantizar el mantenimiento del nivel acordado de seguridad de información y prestación de servicios conforme a los acuerdos del proveedor.

15.2.1 Control: Supervisión y Revisión de los servicios del proveedor

Se llevará a cabo el seguimiento, control y revisión de los servicios de las terceras partes asegurando que se encuentran adheridos a los términos de seguridad de la información y las condiciones definidas en los acuerdos, y que los incidentes de seguridad de la información y los problemas son manejados en forma apropiada.

Las Instituciones Universitarias Públicas mantendrá control suficiente y visión general de todos los aspectos de seguridad para la información sensible o crítica, o de las instalaciones de procesamiento de información accedidas, procesadas o gestionadas por una tercera parte. Se recomienda que las Instituciones Universitarias Públicas asegure que se mantenga la visibilidad de las actividades de seguridad como gestión de cambios, identificación de vulnerabilidades y reporte/respuesta de incidentes de seguridad de información a través de un proceso de reportes claro y definido, con formato y estructura.

15.2.2 Control: Gestión de cambios a los servicios del proveedor

Se gestionarán los cambios en la provisión de los servicios, incluyendo el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los sistemas y procesos del negocio involucrados y la reevaluación de los riesgos.

El proceso de gestión del cambio de un servicio de tercera parte necesita tener cuenta:

- Los cambios realizados por las Instituciones Universitarias Públicas para implementar:
 - mejoras a los servicios corrientes ofrecidos;
 - desarrollo de cualquier aplicaciones y sistemas nuevos;
 - modificaciones o actualizaciones de las políticas y procedimientos de las Instituciones Universitarias Públicas;
 - nuevos controles para resolver los incidentes de la seguridad de la información y para mejorar la seguridad;
- cambios en los servicios de las terceras partes para implementar:
 - cambios y mejoras de las redes;
 - uso de nuevas tecnologías;
 - adopción de nuevos productos o nuevas versiones/publicaciones;
 - nuevas herramientas de desarrollo y ambientes;
 - cambios de las ubicaciones físicas de las instalaciones de servicio;
 - cambio de proveedores.

16. Cláusula: Gestión de Incidentes de Seguridad

Objetivo

Garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.

16.1 Categoría: Informe de los eventos y debilidades de la seguridad de la información

Objetivo

Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que

permita que se realice una acción correctiva oportuna.

16.1.1 Control: Reporte de los eventos de la seguridad de información

Los incidentes relativos a la seguridad serán comunicados a través de las autoridades o canales apropiados tan pronto como sea posible.

Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes.

Dicho procedimiento debe contemplar que ante la detección de un supuesto incidente o violación de la seguridad, el Responsable de Seguridad de la Información sea informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo.

Asimismo, mantendrá al Comité de Seguridad al tanto de la ocurrencia de incidentes de seguridad.

Sin perjuicio de informar a otros Organismos de competencia, el Responsable de Seguridad de la Información, comunicará a los organismos nacionales de referencia en materia de ciberseguridad, todo incidente o violación de la seguridad, que involucre recursos informáticos.

Todos los miembros de las Instituciones Universitarias Públicas y contratistas deben conocer fehacientemente el procedimiento de comunicación de incidentes de seguridad, y deben informar formalmente los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

16.1.2 Control: Reporte de las debilidades de la seguridad

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 formalmente las mismas al Responsable de Seguridad de la Información.

Se prohíbe expresamente a los usuarios la realización de pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.

16.1.3 Control: Comunicación de Anomalías del Software

Se establecerán procedimientos para la comunicación de anomalías de software, los cuales deben contemplar:

- a) Registrar los síntomas del problema y los mensajes que aparecen en pantalla.
- b) Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.
- c) Alertar inmediatamente de modo formal al Responsable de Seguridad de la Información de forma directa o a través del responsable del activo en cuestión.

16.2 Categoría: Gestión de los Incidentes y mejoras de la seguridad de la información

Objetivo

Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes de seguridad de la información.

Se deben establecer las responsabilidades y procedimientos para manejar de manera efectiva los eventos y debilidades en la seguridad de la información una vez que han sido reportados. Se debe aplicar un proceso de mejora continua para la respuesta, monitoreo, evaluación y gestión general de los incidentes en la seguridad de la información.

16.2.1 Control: Responsabilidades y procedimientos

Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad. Se deben considerar los siguientes ítems:

- a) Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo como mínimo:
 - 1) Fallas operativas
 - 2) Código malicioso
 - 3) Intrusiones
 - 4) Fraude informático

- 5) Error humano
- 6) Catástrofes naturales
- b) Comunicar formalmente los incidentes a través de autoridades o canales apropiados tan pronto como sea posible.
- c) Contemplar los siguientes puntos en los procedimientos para los planes de contingencia (diseñados para recuperar sistemas y servicios tan pronto como sea posible):
 - 1) Definición de las primeras medidas a implementar.
 - 2) Análisis e identificación de la causa del incidente.
 - 3) Planificación e implementación de soluciones para evitar la repetición del mismo, si fuera necesario.
 - 4) Comunicación formal con las personas afectadas o involucradas con la recuperación del incidente.
 - 5) Notificación de la acción a la autoridad y/u Organismos pertinentes.
- d) Registrar pistas de auditoría y evidencia similar para:
 - 1) Análisis de problemas internos.
 - 2) Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial (Ver Cláusula 10.1. Categoría: Cumplimiento de Requisitos Legales).
- e) Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:
 - 1) Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
 - 2) Documentación de todas las acciones de emergencia emprendidas en forma detallada.
 - 3) Comunicación de las acciones de emergencia a los Responsables de las áreas afectadas por el incidente.
 - 4) Constatación de la integridad de los controles y sistemas de las Instituciones Universitarias Públicas en un plazo mínimo.

En los casos en los que se considere necesario, se solicitará la participación del Responsable del Área Jurídica de las Instituciones Universitarias Públicas en el tratamiento de incidentes de seguridad ocurridos.

16.2.2 Control: Aprendiendo a partir de los incidentes de la seguridad de la información

Se definirá un proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes o de alto impacto. Esto será

evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

16.2.3 Control: Procesos Disciplinarios

Se seguirá el proceso disciplinario formal contemplado en las normas estatutarias, escalafonarias y convencionales que rigen para los miembros de la comunidad que violen la Política, Normas y Procedimientos de Seguridad de las Instituciones Universitarias Públicas (Ver Cláusula 18 Cumplimiento).

17. Cláusula: Gestión de la Continuidad

Objetivo

Minimizar los efectos de las posibles interrupciones de las actividades normales de las Instituciones Universitarias Públicas (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.

Maximizar la efectividad de las operaciones de contingencia de las Instituciones Universitarias Públicas con el establecimiento de planes que incluyan al menos las siguientes etapas:

- a) Notificación/Activación: Consistente en la detección y determinación del daño y la activación del plan.
- b) Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.
- c) Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

Asegurar la coordinación con el personal de las Instituciones Universitarias Públicas y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

17.1 Categoría: Gestión de continuidad de las Instituciones Universitarias Públicas

Objetivo

Mitigar las interrupciones a las actividades de las Instituciones Universitarias Públicas y proteger los procesos críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

17.1.1 Control: Proceso de Administración de la continuidad de las Instituciones Universitarias Públicas

El Comité de Seguridad de la Información, será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades de las Instituciones Universitarias Públicas.

Este Comité tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información de las Instituciones Universitarias Públicas frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

- a) Identificar y priorizar los procesos críticos de las actividades de las Instituciones Universitarias Públicas.
- b) Asegurar que todos los integrantes de las Instituciones Universitarias Públicas comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad de las Instituciones Universitarias Públicas.
- c) Elaborar y documentar una estrategia de continuidad de las actividades de las Instituciones Universitarias Públicas consecuente con los objetivos y prioridades acordados.
- d) Proponer planes de continuidad de las actividades de las Instituciones Universitarias Públicas de conformidad con la estrategia de continuidad acordada.
- e) Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- f) Coordinar actualizaciones periódicas de los planes y procesos implementados.
- g) Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades de las Instituciones Universitarias Públicas.
- h) Proponer las modificaciones a los planes de contingencia.

17.1.2 Control: Continuidad de las Actividades y Análisis de los impactos

Con el fin de establecer un Plan de Continuidad de las Actividades de las Instituciones Universitarias Públicas se deben contemplar los siguientes puntos:

- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en

- los procesos de las actividades, por ejemplo, fallas en el equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación, incendio, desastres naturales, destrucción edilicia, atentados, etc.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.
 - Identificar los controles preventivos, como por ejemplo sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de backup, los registros no electrónicos vitales, etc.

Esta actividad será llevada a cabo con la activa participación de los propietarios de los procesos y recursos de información de que se trate y el Responsable de Seguridad de la Información, considerando todos los procesos de las actividades de las Instituciones Universitarias Públicas y no limitándose a las instalaciones de procesamiento de la información.

Según los resultados de la evaluación de esta actividad, se desarrollará un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades de las Instituciones Universitarias Públicas. Una vez que se ha creado este plan, el mismo debe ser propuesto por el Comité de Seguridad de la Información al Consejo Superior de las Instituciones Universitarias Públicas para su aprobación.

17.1.3 Control: Elaboración e implementación de los planes de continuidad de las Actividades de las Instituciones Universitarias Públicas

Los propietarios de procesos y recursos de información, con la asistencia del Responsable de Seguridad de la Información, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades de las Instituciones Universitarias Públicas. Estos procesos deben ser propuestos por el Comité de Seguridad de la Información.

El proceso de planificación de la continuidad de las actividades considerará los siguientes puntos:

- a) Identificar y acordar respecto a todas las funciones y procedimientos de emergencia.
- b) Analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.
- c) Implementar procedimientos de emergencia para permitir la contención, la

recuperación y el restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de las dependencias de actividades externas y a los contratos vigentes.

- d) Documentar los procedimientos y procesos acordados.
- e) Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.
- f) Instruir al personal involucrado en los procedimientos de reanudación y recuperación en los siguientes temas:
 - 1) Objetivo del plan.
 - 2) Mecanismos de coordinación y comunicación entre equipos (personal involucrado).
 - 3) Procedimientos de divulgación.
 - 4) Requisitos de la seguridad.
 - 5) Procesos específicos para el personal involucrado.
 - 6) Responsabilidades individuales.
- g) Probar y actualizar los planes, guardando evidencia formal de las pruebas y sus resultados.

Asimismo, el proceso de planificación debe concentrarse en los objetivos de las actividades requeridas de las Instituciones Universitarias Públicas, por ejemplo, restablecimiento de los servicios a los usuarios en un plazo aceptable. Deben considerarse los servicios y recursos que permitirán que esto ocurra, incluyendo, dotación de personal, recursos que no procesan información, así como acuerdos para reanudación de emergencia en sitios alternativos de procesamiento de la información.

17.1.4 Control: Marco para la Planificación de la Continuidad de las Actividades de las Instituciones Universitarias Públicas

Se mantendrá un solo marco para los planes de continuidad de las actividades de las Instituciones Universitarias Públicas, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes.

El administrador de cada plan de continuidad será el encargado de coordinar las tareas definidas en el mismo.

Estas modificaciones deben ser propuestas por el Comité de Seguridad de la Información para su aprobación.

El marco para la planificación de la continuidad de las actividades de las Instituciones Universitarias Públicas, tendrá en cuenta los siguientes puntos: Prever las condiciones de implementación de los planes que describan el proceso a seguir (cómo evaluar la situación, qué personas estarán involucradas, etc.) antes de poner en marcha los mismos.

- a) Definir los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones de las Instituciones Universitarias Públicas y/o la vida humana. Esto debe incluir disposiciones con respecto a la gestión de las relaciones públicas y a vínculos eficaces a establecer con las autoridades públicas pertinentes, por ejemplo, la policía, bomberos y autoridades locales.
- b) Realizar los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales de las Instituciones Universitarias Públicas o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos en los plazos requeridos.
- c) Redactar los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales de las Instituciones Universitarias Públicas.
- d) Definir un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan, y el proceso para el mantenimiento del mismo.
- e) Efectuar actividades de concientización e instrucción al personal, diseñadas para propiciar la comprensión de los procesos de continuidad las actividades y garantizar que los procesos sigan siendo eficaces.
- f) Documentar las responsabilidades y funciones de las personas, describiendo los responsables de la ejecución de cada uno de los componentes del plan y las vías de contacto posibles. Se deben mencionar alternativas cuando corresponda. Es de suma importancia definir a un responsable de declarar el estado de contingencia, lo cual dará inicio al plan.

Los administradores de los planes de contingencia se encuentran en el "Anexo - Administradores de los planes de contingencia", que será actualizado semestralmente por el Comité de Seguridad de la Información a propuesta del Responsable de Seguridad de la Información.

El cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad, deben contarse entre las responsabilidades de los administradores de cada plan. Las disposiciones de emergencia para servicios técnicos alternativos, como instalaciones de comunicaciones o de procesamiento de información, normalmente se cuentan entre las responsabilidades de los proveedores de servicios.

17.1.5 Control: Ensayo, Mantenimiento y Reevaluación de los Planes de continuidad de las Instituciones Universitarias Públicas

Debido a que los planes de continuidad de las actividades de las Instituciones Universitarias Públicas pueden fallar, por suposiciones incorrectas, errores o cambios en el equipamiento, se establecen las siguientes pautas de acción:

- El Comité de Seguridad de la Información establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.
- El cronograma indicará quiénes son los responsables de llevar a cabo cada una de las pruebas y de elevar el resultado obtenido al citado Comité.

Se deben utilizar diversas técnicas para garantizar que los planes de contingencia funcionarán ante un hecho real, y éstas incluirán por lo menos:

- a) Efectuar pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación de las actividades utilizando ejemplos de interrupciones).
- b) Realizar simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis).
- c) Efectuar pruebas de recuperación técnica (garantizando que los sistemas de información puedan ser restablecidos con eficacia).
- d) Realizar ensayos completos probando que las Instituciones Universitarias Públicas, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.

Para las operaciones críticas de las Instituciones Universitarias Públicas se tomarán en cuenta, además, los siguientes mecanismos:

- a) Efectuar pruebas de recuperación en un sitio alternativo (ejecutando los procesos de las actividades de las Instituciones Universitarias Públicas en paralelo, con operaciones de recuperación fuera del sitio principal).
- b) Realizar pruebas de instalaciones y servicios de proveedores (garantizando que los productos y servicios de proveedores externos cumplan con los compromisos contraídos).

Todas las pruebas efectuadas deben ser documentadas, resguardándose la evidencia formal de la ejecución y de los resultados obtenidos.

Los planes de continuidad de las actividades de las Instituciones Universitarias Públicas serán revisados y actualizados periódicamente, para garantizar su eficacia permanente. Se incluirán procedimientos en el programa de administración de cambios de las Instituciones Universitarias Públicas para garantizar que se aborden adecuadamente los tópicos de continuidad de las actividades.

La periodicidad de la revisión de los planes de contingencia se encuentra en el "Anexo - Revisión de los planes de contingencia", que será actualizado

semestralmente por el Comité de Seguridad de la Información a propuesta del Responsable de Seguridad de la Información. Cada uno de los Responsables de Procesos es el responsable de las revisiones periódicas de cada uno de los planes de continuidad de su incumbencia, como así también de la identificación de cambios en las disposiciones relativas a las actividades de las Instituciones Universitarias Públicas aún no reflejadas en dichos planes.

Debe prestarse atención, especialmente, a los cambios de:

- a) Personal.
- b) Direcciones o números telefónicos.
- c) Estrategia de las Instituciones Universitarias Públicas.
- d) Ubicación, instalaciones y recursos.
- e) Legislación.
- f) Contratistas, proveedores y clientes críticos.
- g) Procesos, o procesos nuevos / eliminados.
- h) Tecnologías.
- i) Requisitos operacionales.
- j) Requisitos de seguridad.
- k) Hardware, software y otros equipos (tipos, especificaciones, y cantidad).
- l) Requerimientos de los sitios alternativos.
- m) Registros de datos vitales.

Todas las modificaciones efectuadas serán propuestas por el Comité de Seguridad de la Información para su aprobación por el superior jerárquico que corresponda.

Por otra parte, el resultado de este proceso será dado a conocer a fin de que todo el personal involucrado tenga conocimiento de los cambios incorporados.

17.2 Categoría: Redundancias

Objetivo

Asegurar la continuidad de la información y que esté integrada a los sistemas de gestión.

17.2.1 Control: Disponibilidad de las instalaciones de procesamiento de la información

Se deben implementar las instalaciones de procesamiento de la información con la debida redundancia a efectos de cumplir con los requisitos definidos.

Para cumplir con lo anterior las Instituciones Universitarias Públicas debe identificar los requisitos funcionales para considerar los componentes o arquitecturas redundantes. Hay que tener en cuenta durante el diseño, la actividad de la gestión de los riesgos de integridad y confidencialidad de la información que puedan acarrear las redundancias.

18. Cláusula: Cumplimiento

Objetivos

Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a las Instituciones Universitarias Públicas y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.

Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad de las Instituciones Universitarias Públicas.

Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.

Determinar los plazos para el mantenimiento de información y para la recolección de evidencia de las Instituciones Universitarias Públicas.

18.1 Categoría: Cumplimiento de Requisitos Legales

Objetivo

Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.

El diseño, operación, uso y gestión de los sistemas de información pueden estar sujetos a requerimientos de seguridad estatutarios, reguladores y

contractuales.

18.1.1 Control: Identificación de la Legislación Aplicable

Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

18.1.2 Control: Derechos de Propiedad Intelectual

Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

En el equipamiento informático brindado por las Instituciones Universitarias Públicas, solo se podrá utilizar el material autorizado por el mismo.

Las Instituciones Universitarias Públicas sólo podrá autorizar el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

La infracción a estos derechos puede tener como resultado acciones legales que podrían derivar en demandas penales.

Se deben tener presentes las siguientes normas:

- Ley de Propiedad Intelectual N° 11.723: Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales.
- Ley de Marcas N° 22.362: Protege la propiedad de una marca y la exclusividad de su uso.
- Ley de Patentes de Invención y Modelos de Utilidad N° 24.481: Protege el derecho del titular de la patente de invención a impedir que terceros utilicen su producto o procedimiento.

Derecho de Propiedad intelectual del Software

El software es considerado una obra intelectual que goza de la protección de la Ley 11.723 de Propiedad Intelectual.

Esta Ley establece que la explotación de la propiedad intelectual sobre los programas de computación incluirá, entre otras formas, los contratos de licencia para su uso o reproducción.

Los productos de software se suministran normalmente bajo acuerdos de licencia que suelen limitar el uso de los productos al equipamiento específico y su copia a la creación de copias de resguardo solamente.

El Responsable de Seguridad de la Información, con la asistencia del Área Jurídica, analizará los términos y condiciones de la licencia, e implementará los siguientes controles:

- a) Definir normas y procedimientos para el cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software.
- b) Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Propiedad Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las infrinja.
- c) Mantener un adecuado registro de activos.
- d) Conservar pruebas y evidencias de propiedad de licencias, discos maestros, si los hubiere, manuales, etc.
- e) Implementar controles para evitar el exceso del número máximo permitido de usuarios.
- f) Verificar que sólo se instalen productos con licencia y software autorizado.
- g) Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.
- h) Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.
- i) Utilizar herramientas de auditoría adecuadas.
- j) Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

18.1.3 Control: Protección de los Registros de las Instituciones Universitarias Públicas

Los registros críticos de las Instituciones Universitarias Públicas se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales de las Instituciones Universitarias Públicas.

Los registros se clasificarán en diferentes tipos, por ejemplo registros contables, registros de base de datos, registros de auditoría y procedimientos operativos, cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento, por ejemplo papel, microfichas, medios magnéticos u

ópticos.

Las claves criptográficas asociadas con archivos cifrados se mantendrán en forma segura y estarán disponibles para su uso por parte de personas autorizadas cuando resulte necesario.

Se debe considerar la posibilidad de degradación de los medios utilizados para el almacenamiento de los registros. Los procedimientos de almacenamiento y manipulación se implementarán de acuerdo con las recomendaciones del fabricante.

Si se seleccionan medios de almacenamiento electrónicos, se incluirán los procedimientos para garantizar la capacidad de acceso a los datos (tanto legibilidad de formato como medios) durante todo el periodo de retención, a fin de salvaguardar los mismos contra eventuales pérdidas ocasionadas por futuros cambios tecnológicos.

Los sistemas de almacenamiento de datos serán seleccionados de modo tal que los datos requeridos puedan recuperarse de una manera que resulte aceptable para un tribunal de justicia, por ejemplo que todos los registros requeridos puedan recuperarse en un plazo y un formato aceptable.

El sistema de almacenamiento y manipulación garantizará una clara identificación de los registros y de su período de retención legal o normativa. Asimismo, se permitirá una adecuada destrucción de los registros una vez transcurrido dicho período, si ya no resultan necesarios para las Instituciones Universitarias Públicas.

A fin de cumplir con estas obligaciones, se tomarán las siguientes medidas:

- a) Elaborar y divulgar los lineamientos para la retención, almacenamiento, manipulación y eliminación de registros e información.
- b) Preparar un cronograma de retención identificando los tipos esenciales de registros y el período durante el cual deben ser retenidos.
- c) Mantener un inventario de programas fuentes de información clave.
- d) Implementar adecuados controles para proteger la información y los registros esenciales contra pérdida, destrucción y falsificación.

En particular, se deben tener presente las siguientes normas:

- **Ética en el Ejercicio de la Función Pública. Ley 25.188:** Establece que las personas que se desempeñen en la función pública deben proteger y conservar la propiedad del Estado y sólo emplear sus bienes con los fines autorizados.
- **Código de Ética de la Función Pública:** Dispone que el funcionario público debe proteger y conservar los bienes del Estado y utilizar los que le fueran asignados para el desempeño de sus funciones de manera racional, evitando su abuso, derroche o desaprovechamiento.
- **Código Penal Art. 255:** Sanciona a quien sustrajere, ocultare, destruyere o inutilizare objetos destinados a servir de prueba ante la autoridad

competente, registros o documentos confiados a la custodia de un funcionario o de otra persona en el interés del servicio público. Si el culpable fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

- Ley N° 24.624. Artículo 30: Autoriza el archivo y la conservación en soporte electrónico u óptico indeleble de la documentación financiera, de personal y de control de la Administración Pública Nacional y otorga valor jurídico y probatorio a la documentación existente que se incorpore al Archivo General de la Administración, mediante la utilización de tecnología que garantice la estabilidad, perdurabilidad, inmutabilidad e inalterabilidad del soporte de guarda físico de la mencionada documentación.
- Decisión Administrativa 43/96: Reglamenta el Art. 30 de la Ley 24.624. Determina su ámbito de aplicación, define conceptos y precisa los requisitos de carácter general, los relacionados con los documentos en particular y con el soporte a utilizar en la redacción, producción o reproducción de aquellos.
- Ley de Propiedad Intelectual N° 11.723: Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo las compilaciones de datos o de otros materiales.
- Ley N° 25.506: Establece que la exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.
- Código Penal: Sanciona a aquel que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos (Art. 183).

18.1.4 Control: Protección de Datos y Privacidad de la Información Personal

Todo el personal debe conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

Las Instituciones Universitarias Públicas redactará un "Compromiso de Confidencialidad", el cual debe ser suscrito por todos los funcionarios públicos y contratistas. La copia firmada del compromiso será retenida en forma segura por las Instituciones Universitarias Públicas.

Mediante este instrumento el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del Responsable del Activo de que se trate. A través del "Compromiso de Confidencialidad" se debe advertir al empleado que determinadas actividades

pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

En particular, se deben tener presente las siguientes normas:

- Ley Marco de Regulación de Empleo Público Nacional. Ley 25.164: Establece que los Funcionarios Públicos deben observar el deber de fidelidad que se derive de la índole de las tareas que le fueron asignadas y guardar la discreción correspondiente o la reserva absoluta, en su caso, de todo asunto del servicio que así lo requiera.
- Convenio Colectivo de Trabajo General: Dispone que todos los agentes deben observar el deber de fidelidad que se derive de la índole de las tareas que le fueran asignadas y guardar la discreción correspondiente, con respecto a todos los hechos e informaciones de los cuales tenga conocimiento en el ejercicio o con motivo del ejercicio de sus funciones.
- Ética en el Ejercicio de la Función Pública. Ley 25.188: Obliga a todas las personas que se desempeñen en la función pública a abstenerse de utilizar información adquirida en el cumplimiento de sus funciones para realizar actividades no relacionadas con sus tareas oficiales o de permitir su uso en beneficio de intereses privados.
- Código de Ética de la Función Pública: Establece que el funcionario público debe abstenerse de difundir toda información que hubiera sido calificada como reservada o secreta conforme a las disposiciones vigentes, ni la debe utilizar, en beneficio propio o de terceros o para fines ajenos al servicio, información de la que tenga conocimiento con motivo o en ocasión del ejercicio de sus funciones y que no esté destinada al público en general.
- Protección de Datos Personales. Ley 25.326: Establece responsabilidades para aquellas personas que recopilan, procesan y divulgan información personal y define criterios para procesar datos personales o cederlos a terceros.
- Confidencialidad. Ley N° 24.766: Impide la divulgación a terceros, o su utilización sin previo consentimiento y de manera contraria a los usos comerciales honestos, de información secreta y con valor comercial que haya sido objeto de medidas razonables para mantenerla secreta.
- Código Penal: Sanciona a aquel que abriere o accediere indebidamente a una comunicación electrónica o indebidamente la suprimiere o desviare (Art. 153), al que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido (Art. 153 bis), al que el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros. (Art. 155), al que teniendo noticias de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa (Art. 156), al funcionario público que revelare hechos, actuaciones o documentos que por

la ley deben quedar secretos (Art. 157), al que a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales, ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley e ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales (Art. 157 bis), al que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos (Art. 183), al que revelare secretos políticos o militares concernientes a la seguridad, a los medios de defensa o a las relaciones exteriores de la Nación, o al que por imprudencia o negligencia diere a conocer los secretos mencionados anteriormente, de los que se hallare en posesión en virtud de su empleo u oficio (Art. 222 y 223).

Asimismo, debe considerarse lo establecido en el Decreto 1172/03, que regula el acceso a la información pública por parte de los ciudadanos.

18.1.5 Control: Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información

Los recursos de procesamiento de información de las Instituciones Universitarias Públicas se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido.

Todo el personal debe conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

En particular, se debe respetar lo dispuesto por las siguientes normas:

- Ley Marco de Regulación de Empleo Público Nacional. Ley 25.164: Prohíbe hacer uso indebido o con fines particulares del patrimonio estatal.
- Convenio Colectivo de Trabajo General: Obliga a los agentes a no hacer uso indebido o con fines particulares del patrimonio estatal.
- Ética en el Ejercicio de la Función Pública. Ley 25.188: Obliga a las personas que se desempeñen en la función pública a proteger y conservar la propiedad del Estado y sólo emplear sus bienes con los fines autorizados.
- Código de Ética de la Función Pública: Obliga al funcionario público a proteger y conservar los bienes del Estado y utilizar los que le fueran asignados para el desempeño de sus funciones de manera racional, evitando su abuso, derroche o desaprovechamiento.
- Código Penal: Sanciona a aquel que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere,

hiciera circular o introdujere en un sistema informático, cualquier programa destinado a causar daños (Art. 183).

18.1.6 Control: Regulación de Controles para el Uso de Criptografía

Al utilizar firmas digitales o electrónicas, se debe considerar lo dispuesto por la Ley 25.506 y su decreto reglamentario Decreto 2628/02, que establecen las condiciones bajo las cuales una firma digital es legalmente válida.

Respecto a la comercialización de controles criptográficos, nuestro país ha suscrito el acuerdo Wassenaar, que establece un listado de materiales y tecnologías de doble uso, cuya comercialización puede ser considerada peligrosa.

El Decreto 603/92 regula el Régimen de Control de las Exportaciones Sensitivas y de Material Bélico, estableciendo un tratamiento especial para la exportación de determinados bienes que pueden ser comprendidos dentro del concepto de material bélico.

Se debe obtener asesoramiento antes de transferir a otro país información cifrada o controles criptográficos. Para ello se puede consultar a la Dirección General de Política, de la Secretaría de Asuntos Militares, Ministerio de Defensa, a fin de saber si el material exportable requiere algún tratamiento especial.

18.1.7 Control: Recolección de Evidencia

Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos.

Cuando la acción implique la aplicación de una ley, la evidencia presentada debe cumplir con lo establecido por las normas procesales. Para lograr la validez de la evidencia, las Instituciones Universitarias Públicas garantizará que sus sistemas de información cumplen con la normativa y los estándares o códigos de práctica relativos a la producción de evidencia válida.

Para lograr la calidad y totalidad de la evidencia es necesaria una sólida pista de la misma. Esta pista se establecerá cumpliendo las siguientes condiciones:

- a) Almacenar los documentos en papel originales en forma segura y mantener registros acerca de quién lo halló, dónde se halló, cuándo se halló y quién presenció el hallazgo. Cualquier investigación debe garantizar que los originales no sean alterados.

- b) Copiar la información para garantizar su disponibilidad. Se mantendrá un registro de todas las acciones realizadas durante el proceso de copia. Se almacenará en forma segura una copia de los medios y del registro.

Cuando se detecta un incidente, puede no resultar obvio si éste derivará en una demanda legal por lo tanto se deben tomar todos los recaudos establecidos para la obtención y preservación de la evidencia.

Se debe tener presente lo dispuesto por el Reglamento de Investigaciones Administrativas, procedimiento administrativo especial, de naturaleza correctiva interna que constituye garantía suficiente para la protección de los derechos y correcto ejercicio de las responsabilidades impuestas a los agentes públicos. Este Decreto debe ser complementado por lo dispuesto en la Ley N° 19.549 (Ley de Procedimientos Administrativos) y por toda otra normativa aplicable, incluido el Código Penal, el que sanciona a quien sustrajere, alterar, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público (Art. 255).

18.1.8 Control: Delitos Informáticos

Todo el personal deben conocer la existencia de la Ley 26.388 de Delitos Informáticos, a partir de cuyo dictado se castigan penalmente ciertas conductas cometidas mediante medios informáticos. En tal sentido, los agentes públicos deben conocer con exactitud el alcance de los nuevos tipos penales introducidos por la norma mencionada.

Cabe señalar que la mayoría de las conductas descritas por dicha norma vinculada ya han sido señaladas en los apartados precedentes.

18.2 Categoría: Revisiones de la Política de Seguridad y la Compatibilidad Técnica

Objetivo

Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.

La seguridad de los sistemas de información se debiera revisar regularmente.

Estas revisiones deben realizarse en base a las políticas de seguridad apropiadas y las plataformas técnicas, y los sistemas de información deben ser auditados en cumplimiento con los estándares de implementación de seguridad aplicables y los controles de seguridad documentados.

18.2.1 Control: Cumplimiento de la Política de Seguridad

Cada Responsable de Unidad Organizativa, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

El Responsable de Seguridad de la Información, realizará revisiones periódicas de todas las áreas de las Instituciones Universitarias Públicas a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

- a) Sistemas de información.
- b) Proveedores de sistemas.
- c) Propietarios de información.
- d) Usuarios.

Los Propietarios de la Información brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

18.2.2 Control: Verificación de la Compatibilidad Técnica

El Responsable de Seguridad de la Información verificará periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. En caso de ser necesario, estas revisiones contemplarán la asistencia técnica especializada.

El resultado de la evaluación se volcará en un informe técnico para su ulterior interpretación por parte de los especialistas. Para ello, la tarea podrá ser realizada por un profesional experimentado (en forma manual o con el apoyo de herramientas de software), o por un paquete de software automatizado que genere reportes que serán interpretados por un especialista técnico.

La verificación del cumplimiento comprenderá pruebas de penetración y tendrá como objetivo la detección de vulnerabilidades en el sistema y la verificación

de la eficacia de los controles con relación a la prevención de accesos no autorizados. Se tomarán los recaudos necesarios en el caso de pruebas de penetración exitosas que comprometan la seguridad del sistema.

Las verificaciones de cumplimiento sólo serán realizadas por personas competentes, formalmente autorizadas y bajo la supervisión.

18.3 Categoría: Consideraciones de Auditorías de Sistemas

Objetivo

Maximizar la efectividad de y minimizar la interferencia desde/hacia el proceso de auditoría del sistema de información.

Durante las auditorías de los sistemas de información debieran existir controles para salvaguardar los sistemas operacionales y herramientas de auditoría.

Con relación a las auditorías, serán de aplicación las Normas de Control Interno para Tecnologías de Información, aprobadas por la resolución SIGEN N° 48/05.

18.3.1 Controles de Auditoría de Sistemas

Cuando se realicen actividades de auditoría que involucren verificaciones de los sistemas en producción, se tomarán recaudos en la planificación de los requerimientos y tareas, y se acordará con las áreas involucradas a efectos de minimizar el riesgo de interrupciones en las operaciones.

Se contemplarán los siguientes puntos:

- a) Acordar con el Área que corresponda los requerimientos de auditoría.
- b) Controlar el alcance de las verificaciones. Esta función será realizada por el responsable de auditoría.
- c) Limitar las verificaciones a un acceso de sólo lectura del software y datos de producción. Caso contrario, se tomarán los resguardos necesarios a efectos de aislar y contrarrestar los efectos de las modificaciones realizadas, una vez finalizada la auditoría. Por ejemplo:
 - Eliminar archivos transitorios.
 - Eliminar entidades ficticias y datos incorporados en archivos maestros.
 - Revertir transacciones.
 - Revocar privilegios otorgados
- d) Identificar claramente los recursos de tecnologías de información (TI) para llevar a cabo las verificaciones, los cuales serán puestos a disposición de los

auditores. A tal efecto, la Unidad de Auditoría o en su defecto quien sea propuesto por el Comité de Seguridad de la Información completará el siguiente formulario, el cual debe ser puesto en conocimiento de las áreas involucradas:

- e) Identificar y acordar los requerimientos de procesamiento especial o adicional.
- f) Monitorear y registrar todos los accesos, a fin de generar una pista de referencia. Los datos a resguardar deben incluir como mínimo:
 - Fecha y hora.
 - Puesto de trabajo.
 - Usuario.
 - Tipo de acceso.
 - Identificación de los datos accedidos.
 - Estado previo y posterior.
 - Programa y/o función utilizada.
- g) Documentar todos los procedimientos de auditoría, requerimientos y responsabilidades.

18.3.2 Control: Protección de los Elementos Utilizados por la Auditoría de Sistemas

Se protegerá el acceso a los elementos utilizados en las auditorías de sistemas, o sea archivos de datos o software, a fin de evitar el mal uso o el compromiso de los mismos.

Dichas herramientas estarán separadas de los sistemas en producción y de desarrollo, y se les otorgará el nivel de protección requerido.

Se tomarán los recaudos necesarios a efectos de cumplimentar las normas de auditoría dispuestas por la Sindicatura General de la Nación.

18.3.3 Control: Sanciones Previstas por Incumplimiento

Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente Política de Seguridad conforme a lo dispuesto por las normas estatutarias, escalafonarias y convencionales que rigen al personal de la Administración Pública Nacional, y en caso de corresponder, se realizarán las acciones correspondientes ante el o los Organismos pertinentes.

Las sanciones sólo pueden imponerse mediante un acto administrativo que así lo disponga cumpliendo las formalidades impuestas por los preceptos

constitucionales, la Ley de Procedimiento Administrativo y demás normativas específicas aplicables.

Amén de las sanciones disciplinarias o administrativas, el agente que no da debido cumplimiento a sus obligaciones pueden incurrir también en responsabilidad civil o patrimonial —cuando ocasiona un daño que debe ser indemnizado— y/o en responsabilidad penal —cuando su conducta constituye un comportamiento considerado delito por el Código Penal y leyes especiales.

Anexo - Conformación del comité de seguridad de la información.

Este anexo debe ser revisado semestralmente por el Comité de Seguridad y las propuestas de cambio deberán ser elevadas al Consejo Superior de las Instituciones Universitarias Públicas.

Conformación:

El comité de seguridad de la información no es un comité técnico, sino que toma las decisiones de gobierno que hacen a la implementación de seguridad de la información en las Instituciones Universitarias Públicas. Las áreas técnicas están representadas por el responsable de seguridad y el responsable de TI pero también deben estar otras áreas de gobierno. En caso de que se considere necesario se puede armar un comité técnico de seguridad que actúe como asesor.

La conformación aquí establecida incluye los roles que son necesarios mínimamente. Las Instituciones Universitarias Públicas también podrá incluir otros roles que lo conformarán de acuerdo a sus características y funcionamiento.

1. Responsable de seguridad de la información de la Universidad.
2. Responsable(s) de TI (del área central).
3. Responsable del área RRHH.
4. Responsable del área legal.
5. Responsable del área económica.
6. Vicerrector y/o secretario general o a quienes estos deleguen.

Anexo - Procesos de Seguridad y sus responsables

Este anexo debe ser revisado y actualizado semestralmente, o cuando sea necesario, por el Comité de Seguridad, que deberá actualizar los procesos de seguridad, los nombres y cargos de los responsables de cada proyecto en función del alcance de la política definida.

Proceso	Nombre del Responsable	Cargo del responsable
Seguridad de las personas		
Seguridad física y ambiental		
Seguridad de las comunicaciones		
Seguridad de las operaciones		
Control de accesos		
Seguridad de los desarrollos		
Mantenimiento de los sistemas		
Continuidad operativa		
Gestión de incidentes		
....		

Anexo - Informaciones

Este anexo debe ser revisado y actualizado semestralmente, o cuando sea necesario, por el Comité de Seguridad, que deberá actualizar las informaciones, los nombres y cargos de los propietarios de cada una de ellas en función del alcance de la política definida. Se recomienda revisar la definición de Propietario de la información en la sección "2. Términos y Definiciones".

Información	Nombre del Propietario	Cargo del propietario
Académica de estudiantes		
Personal de empleados		
Personal de estudiantes		
Económica-financiera		
Acceso a los sistemas		

Anexo - Dispositivos móviles

Cualquier dispositivo móvil y/o removible, incluyendo: Notebooks, Laptop o PDA (Asistente Personal Digital), Teléfonos Celulares y sus tarjetas de memoria, Dispositivos de Almacenamiento removibles, tales como CDs, DVDs, Disquetes, Tapes, y cualquier dispositivo de almacenamiento de conexión USB, Tarjetas de identificación personal (control de acceso), dispositivos criptográficos, cámaras digitales, etc.

Anexo - Materiales de capacitación

Este Anexo debe ser revisado y actualizado semestralmente, o cuando sea necesario, por el Comité de Seguridad, debe incluir la lista de los materiales de capacitación relacionados con el alcance de la política, los nombres y cargos de los responsables de la actualización de los mismos y la fecha de la última revisión.

Material	Nombre del responsable	Cargo del responsable	Fecha de la última revisión

Anexo - Política de contraseñas

ver

<https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/contrasenas.pdf>

El Responsable de Seguridad Informática será deberá revisar a lo sumo anualmente y mantener actualizado el presente anexo:

- 1) Mantener las contraseñas en secreto.
- 2) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- 3) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el Responsable del Activo de Información de que se trate, que:
 - 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.
- 4) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
- 5) Cambiar las contraseñas provisionales en el primer inicio de sesión ("log on").
- 6) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
- 7) Notificar de acuerdo a lo establecido en la cláusula 16 Gestión de Incidentes de Seguridad, cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Anexo - Asignación de funciones en controles criptográficos

Este anexo lo completará el comité de seguridad de la información de acuerdo al inventario de activos de las Instituciones Universitarias Públicas. Para ello deberá rellenar las tablas que forman parte del mismo con la información correspondiente.

Cifrado en los servicios: El responsable de cada servicio será el responsable de implementar la configuración del mismo para la implementación de criptografía (protocolos, configuración de certificados, etc). A continuación se presenta la tabla para completar el responsable para cada servicio. Se listan algunos servicios a modo de ejemplo, la tabla puede ampliarse agregando todos los servicios que deban configurarse en forma segura en las Instituciones Universitarias Públicas:

Servicios	Nombre del Responsable de la implementación del cifrado en el servicio	Cargo del responsable
Servicio WEB	
Servicio de Mail	
Portal de educación a distancia	
Copias de respaldo	
VPN		
Firma digital		

Cifrado de la copias de respaldo: El responsable de realizar la copia de respaldo será también el responsable de llevar a cabo el cifrado y de resguardar adecuadamente las claves asociadas.

Anexo - Algoritmos de cifrado.

En este anexo se enumeran los algoritmos cuyo uso es recomendado por NIST para hash, cifrado simétrico y cifrado asimétrico²:

Algoritmos de hash³:

- SHA1
- Familia de algoritmos SHA2: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256.
- Familia de algoritmos SHA3: SHA3-224, SHA3-256, SHA3-384, SHA3-512
- SHAKE128 and SHAKE256

Algoritmos de cifrado y descifrado⁴:

- AES
- 3DES

Algoritmos de firma digital⁵:

- DSA
- RSA
- ECDSA

² <https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines>

³ <https://csrc.nist.gov/projects/hash-functions>

⁴ <https://csrc.nist.gov/projects/block-cipher-techniques>

⁵ <https://csrc.nist.gov/projects/digital-signatures>

Anexo - Métodos de control de acceso físico

Este Anexo debe ser revisado y actualizado semestralmente, o cuando sea necesario, por el Comité de Seguridad, debe incluir la lista de los métodos de control de acceso físico autorizados por las Instituciones Universitarias Públicas.

(por ejemplo: personal de guardia con listado de personas habilitadas o por tarjeta magnética o inteligente y número de identificación personal (PIN), etc.).

Anexo - Áreas protegidas y lugares seguros.

A los efectos del ítem "11.1.3 Control: Seguridad de oficinas, despachos, instalaciones" se definen como áreas protegidas las que se indican en la tabla a continuación.

Este Anexo debe ser revisado y actualizado semestralmente, o cuando sea necesario, por el Comité de Seguridad, debe incluir la lista de las áreas seguras y protegidas, la localización, los nombres y cargos de los responsables de cada una de ellas.

Área	Localización	Nombre del responsable	Cargo del responsable

Anexo - Métodos de detección de intrusos

Este Anexo debe ser revisado y actualizado semestralmente, o cuando sea necesario, por el Comité de Seguridad, debe incluir la lista de los métodos de detección de intrusos autorizados por las Instituciones Universitarias Públicas.

Por ejemplo, alarmas, sensores de movimientos, cámaras de vigilancia, etc.

Anexo - Herramientas de auditoría.

Este Anexo debe ser revisado y actualizado semestralmente, o cuando sea necesario, por el Comité de Seguridad, debe incluir la lista de las herramientas de auditoría autorizadas por las Instituciones Universitarias Públicas.

Sistema/Información	Recursos tecnológico
Sistema de gestión académica	registro de eventos

Anexo - Segregación de ambientes

A continuación se presenta un modelo ideal formado por tres ambientes que debe ser adaptado a las características propias de de las Instituciones Universitarias Públicas, teniendo en cuenta las capacidades instaladas, los recursos y el equipamiento existente.

Ambiente de Desarrollo

Es donde se desarrollan los programas fuentes y donde se almacena toda la información relacionada con el análisis y diseño de los sistemas. El analista o programador (desarrollador) tiene total dominio sobre el ambiente. Puede recibir algún fuente para modificar, quedando registrado en el sistema de control de versiones que administra el "administrador de programas fuentes".

El desarrollador realiza las pruebas con los datos de la base de desarrollo. Cuando considera que el programa está terminado, lo pasa al ambiente de pruebas junto con la documentación requerida que le entregará al implementador de ese ambiente.

Ambiente de Pruebas

El implementador de este ambiente recibe el programa y la documentación respectiva y realiza una prueba general con un lote de datos para tal efecto, junto con el usuario de ser posible.

El testeador realiza las pruebas con los datos de la base de pruebas. Si no detectan errores de ejecución, los resultados de las rutinas de seguridad son correctos de acuerdo a las especificaciones y considera que la documentación presentada es completa, entonces remite el programa fuente al implementador de producción por medio del sistema de control de versiones y le entrega las instrucciones. Caso contrario, vuelve atrás el ciclo devolviendo el programa al desarrollador, junto con un detalle de las observaciones.

Ambiente de Producción

Es donde se ejecutan los sistemas y se encuentran los datos productivos. Los programas fuentes certificados se guardan en un repositorio de fuentes de

producción, almacenándolos mediante un sistema de control de versiones que maneja el "administrador de programas fuentes" y donde se dejan los datos del programador que hizo la modificación, fecha, hora y tamaño de los programas fuentes y objetos o ejecutables.

El "implementador" compila el programa fuente dentro del ambiente de producción en el momento de realizar el pasaje para asegurar de esta forma que hay una correspondencia biunívoca con el ejecutable en producción y luego se elimina, dejándolo en el repositorio productivo de programas fuentes.

Deben aplicarse procedimientos de la misma naturaleza y alcance para las modificaciones de cualquier otro elemento que forme parte del sistema, por ejemplo: modelo de datos de la base de datos o cambios en los parámetros, etc. Las modificaciones realizadas al software de base (Sistemas Operativos, Motores de bases de datos, Productos middleware) deben cumplir idénticos pasos, sólo que las implementaciones las realizan los propios administradores.

Cabe aclarar que tanto el personal de desarrollo, como el proveedor de los aplicativos, no deben tener acceso al ambiente de producción, así como tampoco a los datos reales para la realización de las pruebas en el Ambiente de Prueba. Para casos excepcionales, se debe documentar adecuadamente la autorización, los trabajos realizados y monitorearlos en todo momento.

Anexo - Administradores de los planes de contingencia

Este Anexo debe ser revisado y actualizado semestralmente, o cuando sea necesario, por el Comité de Seguridad, debe incluir la lista de los planes de contingencia, la versión vigente los nombres y cargos de los administradores (responsables) de cada uno de ellos.

Plan de contingencia	Nombre del administrador	Cargo del administrador	Versión vigente

Anexo - Revisión de los planes de contingencia.

Este Anexo debe ser revisado y actualizado semestralmente, o cuando sea necesario, por el Comité de Seguridad, debe incluir la lista de los planes de contingencia, el plazo de revisión, los nombres y cargos de los responsables de la revisión de cada uno de ellos.

Plan de contingencia	Revisar Cada	Nombre del Responsable de la revisión	Cargo del responsable

Anexo - Partidas presupuestarias

Este anexo debe ser revisado y actualizado anualmente, o cuando sea necesario, por el Responsable del Área Administrativa, que deberá actualizar las partidas presupuestarias, la descripción, montos, la unidad organizativa o proyectos, el nombre del responsable y cargo del responsable de cada una de ellas. Las partidas a las que se refiere este anexo son las que correspondan a las acciones derivadas de la política de seguridad.

Partida	Descripción	Monto	Unidad Organizativa o proyecto	Nombre del Responsable	Cargo del Responsable

Anexo - Modelo acuerdo de confidencialidad o no divulgación

Este Anexo debe ser revisado y actualizado semestralmente, o cuando sea necesario, por el Comité de Seguridad y el Responsable del Área Legal.

Modelo 1 - contrato de locación de obra

Contratos de Locación de Obra de Profesionales de Informática

Contratante:

Profesional:

El presente Anexo expresa las condiciones de seguridad lógica y física impuestas por LA UNIVERSIDAD para sus sistemas de información, y que EL/LA PROFESIONAL contratado/a acepta respetar.-

Primero: EL/LA PROFESIONAL acepta voluntariamente colaborar con el resguardo de la seguridad (lógica y física) de los sistemas de información de LA UNIVERSIDAD con los que interactúa como consecuencia del presente contrato a través del ejercicio de las siguientes acciones o precauciones:

- Brindar protección a los datos de LA UNIVERSIDAD procurando que la información contenida en los sistemas de LA UNIVERSIDAD cuente con el mejor nivel posible de seguridad lógica y física.-
- Mantener la integridad y disponibilidad de la información en los sistemas de LA UNIVERSIDAD, evitando acciones que puedan vulnerar, modificar sin autorización, eliminar o corromper los contenidos de tales sistemas.-
- Registrar y comunicar a la Prosecretaría de Informática, de modo fehaciente y en plazos no superiores a las 24 horas, sobre los incidentes de seguridad que EL/LA PROFESIONAL detectare en los sistemas de información de LA UNIVERSIDAD.-
- Suministrar a LA UNIVERSIDAD las claves, programas fuentes, documentación o cualquier otro recurso o componente que corresponda a los sistemas, en la oportunidad y modalidad en que les sean solicitados por la Prosecretaría de Informática.-
- Mantener la confidencialidad sobre los datos y sistemas de LA UNIVERSIDAD, evitando copiarlos o darlos a conocimiento a personal o terceros no autorizados, entendiéndose que se trata de material reservado, excepto en aquellos casos autorizados por la Prosecretaría de Informática.

Esta condición de privacidad y confidencialidad mantendrá su vigencia aún después de extinguida la presente relación contractual.-

- No ceder a terceros las claves de acceso a los sistemas de información de LA UNIVERSIDAD, en términos y modalidades similares a los expresados en el párrafo anterior.-
- Evitar y suprimir los accesos lógicos remotos que apliquen procedimientos no encriptados o transmisión en "texto claro" de las claves de acceso a los sistemas antes referidos.-
- Presentar los informes de avance sobre las obras desarrolladas a los fines de permitir una adecuada supervisión o control que, en defensa de la seguridad e integridad de los sistemas, disponga la Prosecretaría de Informática, la Unidad de Auditoría Interna o cualquier otro organismo de LA UNIVERSIDAD al que le sean otorgadas funciones de contralor sobre los sistemas de información.-
- Ejecutar las políticas de respaldo de la información y sistemas, de acuerdo a lo normado por el Prosecretaría de Informática, o por la Autoridad Universitaria competente.-
- Aplicar cualquier política o consigna adicional dispuesta por LA UNIVERSIDAD en resguardo de los sistemas de información o recursos informáticos que operan en su jurisdicción.-

Segundo: EL/LA PROFESIONAL declara conocer y aceptar voluntariamente que corresponde a LA UNIVERSIDAD la plena potestad y derecho para aplicar políticas y procedimientos de supervisión, control o monitoreo sobre la actividad que desarrolla EL/LA PROFESIONAL como consecuencia de la presente relación contractual, en resguardo de la seguridad de los sistemas de información de aquélla. A tales fines LA UNIVERSIDAD queda facultada a:

- Auditar o contratar auditorías por terceros sobre la gestión de sus sistemas de información.-
- Aplicar periódicamente, perfeccionar o disponer acciones y procedimientos de control para la protección física y lógica de los sistemas de información y de los recursos informáticos de su propiedad.-
- Monitorear la actividad que EL/LA PROFESIONAL desarrolle como consecuencia del presente vínculo contractual.-

Tercero: EL/LA PROFESIONAL acepta voluntariamente y concuerda con que:

- Corresponde al Prosecretario de Informática la gestión y gerenciamiento de los sistemas de información de LA UNIVERSIDAD que operan bajo la tutela de la Prosecretaría de Informática. A tal efecto, en materia de seguridad de sistemas de información que operen bajo tecnologías informáticas (TICs), serán de aplicación, bajo la modalidad que LA UNIVERSIDAD disponga en

sus reglamentaciones, los principios rectores, recomendaciones, procedimientos y terminología contenidos en la política de Seguridad de la Información aprobada por Ordenanza HCS 3/2008

- La información, claves de acceso, protocolos y procedimientos que residen en los sistemas de LA UNIVERSIDAD poseen el carácter de reservados y confidenciales, salvo disposición en contrario expresa de la Autoridad Universitaria.

Modelo 2 - Contrato de locación de servicios.

Condiciones de Seguridad de Sistemas de Información

Contratos de Locación de Servicios de Profesionales de Informática

Universidad Nacional de Córdoba

Profesional:

El presente Anexo expresa las condiciones de seguridad lógica y física impuestas por LA UNIVERSIDAD para sus sistemas de información, y que EL PROFESIONAL contratado acepta respetar.-

Primero: EL PROFESIONAL acepta voluntariamente colaborar con el resguardo de la seguridad (lógica y física) de los sistemas de información de LA UNIVERSIDAD a través del ejercicio de las siguientes acciones o precauciones:

- Brindar protección a los datos de LA UNIVERSIDAD procurando que, por medio de sus servicios profesionales y de la aplicación eficaz de los recursos disponibles de equipamiento y programas informáticos, la información contenida en los sistemas de LA UNIVERSIDAD cuenten con el mejor nivel posible de seguridad lógica y física.-
- Mantener la integridad y disponibilidad de la información en los sistemas de LA UNIVERSIDAD, evitando acciones que puedan vulnerar, modificar sin autorización, eliminar o corromper los contenidos de tales sistemas.-
- Registrar y comunicar a la Prosecretaría de Informática, de modo fehaciente y en plazos no superiores a las 24 horas, sobre los incidentes de seguridad que EL PROFESIONAL detectare en los sistemas de información de LA UNIVERSIDAD.-
- Suministrar a LA UNIVERSIDAD las claves, programas fuentes, documentación o cualquier otro recurso o componente que corresponda a los sistemas, en la oportunidad y modalidad en que les sean solicitados por la Prosecretaría de Informática.-
- Mantener la confidencialidad sobre los datos y sistemas de LA UNIVERSIDAD, evitando copiarlos o darlos a conocimiento a personal o

terceros no autorizados, entendiéndose que se trata de material reservado, excepto en aquellos casos autorizados por la Prosecretaría de Informática. Esta condición de privacidad y confidencialidad mantendrá su vigencia tanto en horarios laborables como en no-laborables, y regirá aún después de extinguida la presente relación contractual.-

- No ceder a terceros las claves de acceso a los sistemas de información de LA UNIVERSIDAD, en términos y modalidades similares a los expresados en el párrafo anterior.-
- Ejercer tareas de control sobre los accesos lógicos o físicos a los sistemas de información de LA UNIVERSIDAD.-
- Evitar y suprimir los accesos lógicos remotos que apliquen procedimientos no encriptados o transmisión en "texto claro" de las claves de acceso a los sistemas antes referidos.-
- Presentar informes periódicos sobre las tareas que desarrolla a los fines de permitir una adecuada supervisión o control que, en defensa de la seguridad e integridad de los sistemas, disponga la Prosecretaría de Informática, la Unidad de Auditoría Interna o cualquier otro organismo de LA UNIVERSIDAD al que le sean otorgadas funciones de contralor sobre los sistemas de información.-
- Mantener el almacenamiento de los archivos de registro de sistemas (archivos de "logs") por el tiempo y bajo la modalidad que LA UNIVERSIDAD determine, y facilitar el acceso de la Prosecretaría de Informática o de la Unidad de Auditoría Interna a tales archivos que sean generados por los sistemas de información. A los fines del ejercicio de acciones de monitoreo por parte de LA UNIVERSIDAD, tales archivos de registro no podrán ser alterados o modificados, sea en sus contenidos o en los parámetros que permitan determinar sus fechas o tiempos de generación.-
- Llevar un registro de las modificaciones solicitadas por las Unidades Académicas y demás Dependencias de LA UNIVERSIDAD, preferentemente en libros de registro (formato de libros de actas) sobre soporte papel, asentando el tipo de modificación producida, organismo solicitante, fecha y hora de producción, y cualquier otro detalle que facilite el posterior monitoreo de los cambios producidos.-
- Aplicar las modificaciones mencionadas sólo en tanto y cuanto estén cuenten con el visto bueno del Prosecretario de Informática.-
- Ejecutar las políticas de respaldo de la información y sistemas, de acuerdo a lo normado por el Prosecretaría de Informática, o por la Autoridad Universitaria competente.-
- Aplicar cualquier política o consigna adicional dispuesta por LA UNIVERSIDAD en resguardo de los sistemas de información o recursos informáticos que operan en su jurisdicción.-

Segundo: EL PROFESIONAL declara conocer y aceptar voluntariamente que corresponde a LA UNIVERSIDAD la plena potestad y derecho para aplicar políticas y procedimientos de supervisión, control o monitoreo sobre la actividad que desarrolla EL PROFESIONAL como consecuencia de la presente relación contractual, en resguardo de la seguridad de los sistemas de información de aquélla. A tales fines LA UNIVERSIDAD queda facultada a:

- Auditar o contratar auditorías por terceros sobre la gestión de sus sistemas de información.-
- Aplicar periódicamente, perfeccionar o disponer acciones y procedimientos de control para la protección física y lógica de los sistemas de información y de los recursos informáticos de su propiedad.-
- Monitorear la actividad que EL PROFESIONAL desarrolle como consecuencia del presente vínculo contractual.-
- Solicitar, a los fines de esclarecimiento en caso de incidentes de seguridad, el apartamiento temporario de las funciones o tareas de EL PROFESIONAL, si LA UNIVERSIDAD lo considerase de necesidad o conveniencia.-
- Incluir programas periódicos de entrenamiento y capacitación del personal en cuestiones relativas a la seguridad y operación segura de los sistemas de información, quedando EL PROFESIONAL obligado a colaborar con su experiencia y conocimientos en tales acciones, o bien a perfeccionarse a través de los mismos. Tales programas se llevarán a cabo bajo la supervisión exclusiva de la Prosecretaría de Informática.-

Tercero: EL PROFESIONAL acepta voluntariamente y concuerda que:

- Corresponde al Prosecretario de Informática la gestión y gerenciamiento de los sistemas de información de LA UNIVERSIDAD que operan bajo la tutela de la Prosecretaría de Informática. A tal efecto, en materia de seguridad de sistemas de información que operen bajo tecnologías informáticas (TICs), serán de aplicación, bajo la modalidad que LA UNIVERSIDAD disponga en sus reglamentaciones, los principios rectores, recomendaciones, procedimientos y terminología contenidos en la Norma Argentina IRAM-ISO/IEC 17799 que EL PROFESIONAL declara conocer.-
- El desarrollo y verificación (testeo) de sistemas operativos, bases de datos y aplicaciones, o de las actualizaciones o cambio de versiones de los mismos, deberán contar con la aprobación previa del Prosecretario de Informática y, en los casos que correspondiere, de la Facultad, Instituto o Escuela propietaria de los recursos de información afectados. A tales efectos, y salvo el caso de circunstancias excepcionales debidamente justificadas, para tales iniciativas EL PROFESIONAL deberá solicitar por medios fehacientes la correspondiente autorización y aprobación con al menos treinta (30) días de antelación al inicio de las actividades o acciones pertinentes, incluyendo en el

pedido un análisis de los factores de riesgo ante fallas eventuales de los productos a aplicar o instalar.-

- La información, claves de acceso, protocolos y procedimientos que residen en los sistemas de LA UNIVERSIDAD poseen el carácter de reservados y confidenciales, salvo disposición en contrario expresa de la Autoridad Universitaria.-
- Los desarrollos de programas, aplicaciones o sistemas, que en todo o en parte realice EL PROFESIONAL como consecuencia de la presente relación contractual, constituyen propiedad exclusiva de LA UNIVERSIDAD, y en consecuencia, le corresponde a la misma el acceso y posesión de la totalidad de la documentación, programas fuente, programas ejecutables, claves de acceso, reportes y archivos de registro ("logs").-----

Anexo - Activos de información

Este Anexo debe ser revisado y actualizado semestralmente, o cuando sea necesario, por el Comité de Seguridad, debe incluir la lista de los activos de información, los nombres y cargos de los propietarios de cada uno de ellos. Se recomienda revisar la definición de Propietario de la información en la sección "2. Términos y Definiciones".

Activo	Nombre del propietario	Cargo del propietario

Anexo - Sistemas Sensibles y Críticos

Este Anexo debe ser revisado y actualizado semestralmente, o cuando sea necesario, por el Comité de Seguridad, debe incluir la lista de los sistemas sensibles y críticos, los nombres y cargos de los propietarios de cada uno de ellos. Se recomienda revisar la definición de Propietario de la información en la sección "2. Términos y Definiciones".

Sistema	Nombre del propietario	Cargo del propietario