POLITICAS DE SEGURIDAD DE INFORMACION UNACH 2018

Fecha de presentación

11/04/2018

Versión: 1.0

Presentado por:

Ing. Natalia Crespo.

nataliacrespo@unach.edu.ec

Ing. Pedro Orozco

porozco@unach.edu.ec

Aprobado por:

Ing. Daniel Haro M.

dharo@unach.edu.ec

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO

1. Introducción

La Universidad Nacional de Chimborazo es una Institución de Educación Superior cuyos procesos académicos y administrativos se soportan en sistemas, servicios y herramientas informáticas para su adecuado desarrollo, y en este contexto es importante mantener la confidencialidad, integridad y disponibilidad de la información.

Esta seguridad se basa en un conjunto de políticas que permitan una adecuada gestión de los activos de información institucional, previniendo la materialización de amenazas que ocasionen impactos negativos de tiempo, costo y calidad de información.

Las políticas de gestión de seguridad son un conjunto de reglas y procedimientos que permiten definir cómo gestionar cada uno de los elementos que forman parte de los activos de información institucional.

Conforme los procedimientos establecidos las políticas de seguridad deberán ser revisadas y actualizadas de forma periódica, con la finalidad de actualizar los controles de seguridad con base a nuevas amenazas identificadas y nuevos estándares de seguridad vigentes.

2. Propósito

Implementar, socializar y monitorear el cumplimiento de las políticas de seguridad de la información para la Universidad Nacional de Chimborazo.

3. Alcance

Las presente políticas de seguridad son de cumplimiento obligatorio para todos los miembros de la comunidad universitaria: estudiantes, docentes, empleados y trabajadores; así como proveedores o contratistas que tengan relación con la institución y por la naturaleza de la relación contractual, tengan acceso a activos de información institucional.

4. Objetivo

Establecer las directrices de gestión respecto a los activos de información institucional, obligaciones, responsabilidades, buen uso y procedimientos disciplinarios asociados a la vulneración de las presente políticas.

5. Base Legal

- Constitución de la República del Ecuador
    - artículo 66, numeral 19 dice: “El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo,

procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley".

- artículo 92 en su parte pertinente dice "… En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados".

- Ley Orgánica de Transparencia y acceso a la información pública.
  - El literal d) del artículo 2 dice: "Garantizar la protección de la información personal en poder del sector público y/o privado".
- Ley del Sistema Nacional de Registro de Datos Públicos
  - El artículo 4 dice: "Responsabilidad de la información. - Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados es exclusiva de la o el declarante cuando esta o este provee toda la información…"
  - Artículo 6: "Accesibilidad y confidencialidad. - Son confidenciales los datos de carácter personal, tales como: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales(…) La autoridad o funcionario que por la naturaleza de sus funciones custodie datos de carácter personal, deberá adoptar las medidas de seguridad necesarias para proteger y garantizar la reserva de la información que reposa en sus archivos.
- Ley de Comercio electrónico, firmas y mensajes de datos
  - El artículo 2 dice: Reconocimiento jurídico de los mensajes de datos. - Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento.
  - Artículo 57. - Infracciones informáticas. - Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.
- Código Orgánico Integral Penal
  - Sección Tercera Delitos contra la seguridad de los activos de los sistemas de información y comunicación. Artículos del 229 al 234.
- Normas de Control Interno de la Contraloría General del Estado
  - El grupo 400 actividades de control determina la necesidad de establecer políticas y procedimientos para proteger y conservar los activos de información, así como el acceso a los sistemas de información.
  - El subgrupo 410 Tecnología de la Información con las normas de las 01 hasta la 17 establece las directrices que deben tomar en cuenta las entidades del sector público respecto a todos los procesos de acceso a la información.

6. Mejores Prácticas

Para la definición de las políticas de seguridad se ha considerado las mejores prácticas de gestión de seguridad conforme el estándar internacional ISO/IEC 27000 y sus normas: 27001, 27002 y 27005.

7. Documentación

Toda política, procedimiento, formato y control relacionado a la seguridad de la información debe estar documentando, clasificado y archivado conforme su sensibilidad.

8. Vigencia

Las políticas de seguridad no tienen caducidad.
Son aprobadas por el Órgano Académico Colegiado Superior.
Su revisión y actualización se debe cumplir cada 2 años o cuando las necesidades institucionales lo ameriten.

9. Cumplimiento

La aplicación de las políticas de seguridad de la información de la Universidad Nacional de Chimborazo, son de cumplimiento obligatorio y cualquier transgresión o incumplimiento se considera cono una falta disciplinaria y será sancionada conforme la Ley Orgánica de Educación Superior, Ley Orgánica de Servicio Público, Reglamento de Régimen Académico, Estatuto Institucional y otras normas vigentes asociadas al cumplimiento de procedimientos de seguridad de la información.

10. Definiciones

a. **Activo de información:** Son de dos tipos:
    a. **Primarios.** – Constituyen los procesos y la información (en medio digital o físico).
    b. **De soporte.** – Abarca la infraestructura tecnológica (software, hardware, redes de comunicación) y los recursos humanos.
b. **Amenaza:** Cualquier evento con o sin intención de causar daño.
c. **Confidencialidad:** Garantía de que la información estará al alcance únicamente de las personas interesadas.
d. **CSIRT:** Por sus siglas en inglés (Computer Security Incident Response Team) es un equipo multidisciplinario de profesionales encargados de controlar y mitigar los efectos adversos de un incidente de seguridad, procurando un mínimo impacto respecto a los activos de información.
e. **EGSI:** Equipo de Gestión de Seguridad de la Información. Es un equipo multidisciplinario de profesionales del área informática, designado para la gestión de la seguridad de la información en la institución.
f. **Disponibilidad:** Garantía del acceso permanente a la información.
g. **Evento de seguridad:** Cualquier situación que no tiene implicaciones negativas respecto a la seguridad de la información. No provoca interrupción de servicios.
h. **Impacto:** Medición del daño que puede causar un incidente de seguridad.

i. **Incidente de seguridad:** Situación que provoca la interrupción de servicios, es la materialización de una amenaza.
j. **Infraestructura tecnológica:** Conjunto de herramientas de software y hardware orientados a la gestión académica y administrativa de los miembros de la comunidad universitaria.
k. **Integridad:** Garantía de que la información no ha sido modificada ni alterada sin autorización.
l. Riesgo: Probabilidad de que una amenaza se materialice sobre una vulnerabilidad y cause un impacto en la organización.
m. Seguridad de la Información: Medidas adoptadas que previenen la ejecución de operaciones no autorizadas sobre un activo de información.
n. Sistema de información: Conjunto de componentes que recolectan, procesan, almacena y distribuyen información.
o. Plan de mantenimiento: Se refiere al conjunto de acciones programadas que garantiza el funcionamiento permanente de la infraestructura tecnológica.
p. **Plataforma tecnológica:** Conjunto de componentes software y hardware que facilitan el acceso a los sistemas de información.
q. **Política:** Compendio de directrices que representan una posición del nivel jerárquico superior para áreas de control específicas que permiten establecer un canal de actuación en relación con los recursos y servicios de la Institución, normalmente soportadas por estándares, mejores prácticas, procedimientos y guías.
r. **Tipo de información:** Conforme su sensibilidad y usabilidad se clasifica en:
    a. Desclasifica. – De conocimiento público (noticias, disposiciones, normativas, etc.). Se encuentra disponible en la página web institucional, blogs y redes sociales oficiales que maneja la institución.
    b. De uso interno. – Para gestión interna institucional (información contenida en los sistemas de información). Su difusión requiere cumplir procedimientos de autorización.
    c. Confidencial. – De acceso y manipulación por usuarios autorizados (información personal, configuraciones y procedimientos de seguridad). Su acceso está restringido únicamente a personal autorizado.
s. **Vulnerabilidad:** Debilidad en un sistema que puede permitir que una amenaza se materialice.

11. Referencias

Las presentes políticas de seguridad de la información se sustentan en:

- Constitución de la República del Ecuador
- Código Orgánico Integral Penal
- Ley Orgánica de Transparencia y Acceso a la Información Pública
- Ley Orgánica de Educación Superior
- Ley Orgánica de Servicio Público
- Ley del Sistema Nacional de Registro de Datos Públicos
- Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos
- Normas de Control Interno Contraloría General del Estado. Grupo 400 y Subgrupo 410
- Normas ISO/IEC 27002 y 27005

- Reglamento de Régimen Académico
- Estatuto institucional

12. Catálogo de políticas de seguridad

Conforme los requerimientos institucionales, la Universidad Nacional de Chimborazo cuenta con 7 políticas de seguridad de la información que son:

- PGS-UNACH-01 – Gestión de activos de información
- PGS-UNACH-02 – Gestión de credenciales
- PGS-UNACH-03 – Gestión de infraestructura hardware y entorno
- PGS-UNACH-04 – Gestión de Comunicaciones
- PGS-UNACH-05 – Gestión de proyectos de desarrollo y adquisición de software
- PGS-UNACH-06 - Gestión de monitoreo, continuidad y atención de incidentes de seguridad
- PGS-UNACH-07 – Gestión de seguridad para usuarios.

A continuación, se detallan cada una de ellas:

Código	PGS-UNACH-01	**Revisión:** 01	**Fecha:** 15-03-2018
Política de Seguridad	**Gestión de activos de información**		
Objetivo	Garantizar la gestión integral de la seguridad de los activos de información tecnológica de la UNACH (gestión de riesgos, respaldo, recuperación)		
Alcance	Esta política aplica a todos los activos de información tecnológica de la UNACH		
Responsables	Ejecución / Cumplimiento: Custodios de los activos de información Gestión / Administración: Centro de Tecnología Educativa Control / Seguimiento: Centro de Tecnología Educativa		
Gestión			
Identificación y clasificación de activos de información	a. El Centro de Tecnología Educativa debe identificar, clasificar y mantener actualizado el inventario de activos de información y sus custodios con base a la gestión de riesgos de activos de información. b. Los activos de información tanto primarios como de soporte deben ser clasificados y etiquetados por su sensibilidad y usabilidad, conforme el protocolo de clasificación de activos de información. c. Los activos de soporte deben contar, de forma visible, con la respectiva codificación que permita identificar el custodio del mismo. d. El acceso y uso de los activos de información está regulado por el protocolo de configuración y uso de activos de información.		
Propiedad y uso de los activos de información	**Activos Primarios:** a. La información que se genera, almacena, procesa y difunde a través de los sistemas de información institucional, son de propiedad de la Universidad Nacional de Chimborazo. b. Los usuarios de los sistemas de información deberán firmar el respectivo acuerdo de confidencialidad respecto a la información a la que tienen acceso y manipulan, previa asignación de credenciales. c. La relación contractual con terceros debe contemplar el acuerdo de confidencialidad respecto a la información que estos accedan por la naturaleza del contrato. d. La información contenida en los sistemas de información, se entrega previa autorización de la autoridad correspondiente. e. Los usuarios podrán hacer uso de la información institucional únicamente con fines de cumplimiento de su rol dentro de la institución. f. Las personas interesadas en acceder a información institucional, conforme establece la Ley Orgánica de Transparencia y Acceso a la Información Pública, deberán cumplir el procedimiento establecido a través del formulario vigente aprobado por el Comité de Transparencia. g. Las bases de datos, así como las aplicaciones local y web de los sistemas de información deben ser monitoreadas mediante la PGS-UNACH-07-Gestión del monitoreo, continuidad y atención de incidentes de seguridad **Activos de soporte:** h. Los activos de soporte de información deben ser adquiridos o aprobada su adquisición por el Centro de Tecnología Educativa, en consideración a la necesidad de contar con equipamiento homologado para el desarrollo de las actividades académicas y administrativas, y		

	que de igual forma faciliten los procesos de soporte, mantenimiento y reubicación, observando los principios de vigencia tecnológica. i. El sistema operativo, herramientas, aplicaciones y demás software requerido para el desarrollo de las actividades académicas y administrativas será el que considere el Centro de Tecnología Educativa en el PETI vigente. No se podrá utilizar software que no esté aprobado por dicha instancia. j. El Centro de Tecnología Educativa con el propósito de cumplir el mandato 1014, deberá promulgar y promover la utilización de Software Libre en la UNACH. Para los casos que no sea posible su aplicación, será el encargado de adquirir y garantizar la vigencia y periodicidad de actualización de las licencias de software propietario. k. No está permitida la descarga, instalación, almacenamiento y/o transferencia de juegos, archivos de audio, archivos de video, software y/o programas desde o hacia Internet, que atenten contra las leyes de derechos de autor o propiedad intelectual. l. No está permitida la extracción, préstamo, copia o venta de software corporativo. **Trazabilidad y auditabilidad:** m. Las bases de datos y sistemas de información deben tener activa y habilitada las funciones de log para todas las transacciones. n. Las bases de datos y sistemas de información deben tener configuradas bitácoras o pistas de auditoría (al menos para los datos sensibles), en el cual se pueda identificar al responsable de actualización, inserción o borrado de datos. o. Estas no deben ser editables, no deben comprometer la capacidad de gestión del sistema y deben permitir realizar copias de seguridad con la finalidad de respaldar las mismas y optimizar espacio en el servidor. p. Los administradores, conforme el Plan Anual de Mantenimiento de bases de datos y aplicaciones, deben revisar de forma periódica los logs a fin de detectar cualquier movimiento fuera de lo usual respecto al uso de la información.
Información confidencial	Conforme la definición de tipos de información, la UNACH clasifica a la siguiente como información confidencial: a. La información de carácter personal de docentes, empleados, trabajadores y estudiantes como: nombres, datos de contacto, datos familiares, ideología, etnia, estado de salud, orientación sexual, religión, condición migratoria y demás relacionados a la intimidad personal, se cataloga como confidencial y por lo tanto su uso está restringido al cumplimiento de actividades institucionales, estando prohibida su divulgación sin la autorización expresa del titular de la misma o de la autoridad competente. b. La información de carácter personal de terceros se sujeta a los mismos lineamientos establecidos en el literal a. de este apartado. c. La información referente a manuales técnicos, configuración de servidores y bases de datos, código fuente y configuraciones de la red de comunicaciones, debe estar documentada en el respectivo protocolo de seguridad, pero su acceso es restringido al personal designado por el Centro de Tecnología Educativa. d. Una copia de la información del punto anterior debe reposar, por seguridad, en la dirección del Centro de Tecnología Educativa, clasificada y archivada como confidencial.

Gestión de copias de seguridad	a. La gestión de las copias de seguridad de configuraciones, bases de datos y aplicaciones locales y web es responsabilidad de los usuarios administradores de las mismas, con base al procedimiento respaldo de datos. b. Las copias de seguridad deben ser almacenadas en medios que garanticen su permanencia en el tiempo y considerando el principio de vigencia tecnológica. c. Las copias de seguridad deben ser encriptadas. d. Los medios deben ser etiquetados y clasificados conforme su antigüedad. e. Las copias de seguridad deberán ser resguardadas por un período de 5 años, tiempo tras el cual deberán ser eliminadas y documentado el procedimiento. f. Los medios de almacenamiento deben permanecer en un área restringida, bajo llave y con las adecuadas condiciones ambientales. g. El acceso a los medios de almacenamiento de copias de seguridad está autorizado únicamente al usuario administrador de copias de seguridad. h. Si la gestión de copias de seguridad se realiza con un proveedor externo, deberá estar respaldado con el respectivo acuerdo de confidencialidad y se debe llevar el registro de medios enviados y recibidos. i. La gestión de copias de seguridad de información institucional generada, procesada y almacenada en las estaciones de trabajo y equipos portátiles del personal institucional, es responsabilidad de dichos usuarios.
Gestión de medios extraíbles	a. Cuando se requiere la utilización de un medio extraíble para transferir o movilizar información institucional, el usuario de dicho medio es el responsable de la misma, por lo que, debe garantizar que: 1) El medio extraíble no esté al alcance de otras personas. 2) No se utilice el medio extraíble para almacenar otro tipo de información que pueda comprometer la seguridad del mismo como software o archivos descargado desde internet. 3) Cuidar de hurtos, olvidos o pérdidas respecto al medio extraíble. b. Borrar información de uso interno o confidencial previo: facilitar a terceros, transferir, eliminar o devolver el medio extraíble.
Borrado o eliminación de activos de información	a. En concordancia a la gestión de riesgos de activos de información, cuando los activos han cumplido un ciclo de vida se debe gestionar la eliminación adecuada de los mismos garantizando que la información institucional no pierda su confidencialidad. b. El Centro de Tecnología Educativa garantizará que un equipo que va a ser reasignado a otro usuario ha pasado por un proceso previo de borrado de información, y eliminación de virus que impida un acceso no autorizado a información sensible institucional. c. Las copias de seguridad que han cumplido su ciclo de vida deben ser borradas de forma permanente del medio en el que se encuentran almacenadas. d. Cuando la información es de uso interno o confidencial y se encuentra en medio físico, esta debe ser eliminada utilizando mecanismos de destrucción de papel.

	e. Cuando la información es de carácter público o no compromete información confidencial y se encuentra en medio físico, se debe utilizar procedimientos de reciclaje o reutilización que permita optimizar recursos institucionales. f. Cuando un equipo ha cumplido su ciclo de vida y por vigencia tecnológica ya no reúne las condiciones necesarias de operación, de forma independiente al cumplimiento del proceso de baja de bienes, el Centro de Tecnología Educativa deberá garantizar el borrado de información contenida en dicho equipo. g. La institución debe contar con un procedimiento estandarizado de gestión documental y archivista para la adecuada custodia de la información física.
Procesos Disciplinarios	La inobservancia a la presente política de seguridad de la información será sancionada conforme la normativa vigente.
Protocolos y procedimientos relacionados	a. Procedimiento respaldo de datos b. Gestión de riesgos de activos de información c. Protocolo de clasificación de activos de información d. Gestión documental y archivista
Formatos y formularios relacionados	

Código	PGS-UNACH-02	**Revisión:** 01	**Fecha:** 15-03-2018
Política de Seguridad	**Gestión de Credenciales**		
Objetivo	Garantizar un adecuado procedimiento de alta, modificación y revocación de privilegios de acceso a los usuarios de la plataforma tecnológica institucional.		
Alcance	Esta política aplica a todos los usuarios de la plataforma tecnológica de la UNACH		
Responsables	Ejecución / Cumplimiento: Usuarios de los sistemas Gestión / Administración: Centro de Tecnología Educativa Control / Seguimiento: Centro de Tecnología Educativa		
Gestión			
Roles de acceso	a. Son definidos en la concepción del sistema de información. b. La implementación y administración es responsabilidad del rol administrador de base de datos. c. El alta de un nuevo rol o la modificación de uno existente requiere de la aprobación del EGSI institucional. d. Los roles de acceso no pueden ser eliminados. Si un rol ya no será utilizado este permanecerá sin miembros en estado inactivo. Debe quedar documentada la razón de la inactividad de un rol.		
Credenciales de usuario operador y final	a. El alta, modificación y revocación de credenciales de usuario para el acceso a: equipos tecnológicos, red de comunicaciones, correo electrónico, sistemas de información se cumple conforme el protocolo de configuración y uso de activos de información. b. Las credenciales de acceso de usuario operador y final son administradas por el administrador del sistema de información. c. El alta de usuarios para acceso a los sistemas de información depende de las funciones o procesos asignados a este y que debe enmarcarse en uno de los roles de acceso aprobados para la aplicación. d. El administrador del sistema de información debe verificar de forma periódica que los roles y privilegios de acceso de los usuarios finales son acordes a las funciones de cada uno de ellos. e. La reubicación de personal al interior de una misma unidad que implique modificación o revocación de privilegios de acceso a un sistema de información debe ser notificada de forma inmediata por el titular de la unidad. f. El movimiento interno en la institución o la desvinculación de personal que accede a sistemas de información deberá ser notificado por el titular de la unidad, para la correspondiente revocación de credenciales. En el caso de desvinculación, esta notificación es de forma independiente al Formulario Paz y Salvo. g. Si la desvinculación corresponde al Titular de la Unidad, será el Departamento de Administración del Talento Humano el encargado de solicitar la revocación de privilegios de acceso.		
Credenciales de Usuario avanzado	b. Aplica a los usuarios que por sus funciones requieran acceso de usuario privilegiado a los sistemas, servicios y aplicaciones asignados. c. Ningún usuario avanzado podrá modificar información directamente de las bases de datos, sin previa autorización del		

	Coordinador de la Unidad de Administración y desarrollo de Software o su delegado. d. Se ejecuta conforme el protocolo de configuración y uso de activos de información.
Credenciales de usuario administrador	a. Aplica a todos aquellos usuarios cuyo cargo está relacionado con la administración funcional y/o tecnológica de sistemas de información y se asigna conforme el protocolo de configuración y uso de activos de información. b. Las actividades realizadas por los usuarios administradores deben reflejarse en un registro, que será monitoreado periódicamente por el director de Centro de Tecnología Educativa o su delegado.
Credenciales de súper usuario	a. Aplica a los usuarios que realizan actividades de dirección en los activos tecnológicos con los máximos privilegios que requiere su función. b. Son creados por defecto en la instalación de los componentes de la plataforma tecnológica. c. Estas credenciales no deben ser manejadas por el personal que realiza actividades de administración y soporte. d. La asignación de estas credenciales la realiza el Centro de Tecnología Educativa en responsabilidad de 2 personas designadas. e. Estas credenciales deben ser definidas por el Centro de Tecnología Educativa, almacenadas en adecuadas condiciones de seguridad y serán utilizadas únicamente en situaciones consideradas de emergencia y/o contingencia. Se debe entregar copia de esta en medio escrito y sobre sellado al director del Centro de Tecnología Educativa y será archivada como información confidencial.
Procesos Disciplinarios	La inobservancia a la presente política de seguridad de la información será sancionada conforme la normativa vigente.
Protocolos y procedimientos relacionados	a. Configuración y uso de activos de información
Formatos y formularios relacionados	a. Formulario Gestión de credenciales. b. Formato para registro de actividades usuario administrador

Código	PGS-UNACH-03	**Revisión:** 01	**Fecha:** 15-03-2018
Política de Seguridad	**Gestión de Infraestructura hardware y entorno**		
Objetivo	Garantizar el uso adecuado, mantenimiento, seguridad y funcionamiento de la infraestructura hardware institucional (servidores, equipos de comunicación, estaciones de trabajo, portátiles, tabletas, impresoras, etc.), así como las áreas donde dicha infraestructura está ubicada.		
Alcance	Esta política aplica a todos los equipos hardware que forman parte de la infraestructura tecnológica institucional		
Responsables	Ejecución / Cumplimiento: Custodios de los activos de soporte Gestión / Administración: Centro de Tecnología Educativa Control / Seguimiento: Centro de Tecnología Educativa		
Gestión			
Gestión del Data Center	a. Está bajo la responsabilidad del Centro de Tecnología Educativa y se considera un área restringida. b. En el Data Center deben estar alojados todos los servidores de información institucional. c. Su administración está a cargo del área de infraestructura y redes, conforme el protocolo de gestión de comunicaciones. d. La asignación de credenciales de acceso lógico a los servidores se realizará conforme la PGS-UNACH-02 - Gestión de Credenciales. e. El Data Center debe cumplir un estándar de redundancia y seguridad que garantice la disponibilidad de la información, con base al PETI vigente, procedimiento que debe estar documentado. f. La infraestructura tecnológica del Data Center debe contar con los respectivos manuales técnicos y de usuario actualizados y aprobados. El manual técnico será de uso del administrador del Data Center. El manual de usuario deberá ser conocido por el personal autorizado para el acceso al Data Center. g. El Data Center debe contar con un plan anual de mantenimiento aprobado por el Centro de Tecnología Educativa. Dicho plan se sujeta a la PGS-UNACH-07-Gestión del monitoreo, continuidad y atención de incidentes de seguridad.		
Gestión de equipamiento tecnológico	a. La asignación de equipamiento tecnológico a los usuarios institucionales la realiza la Unidad de Control de Bienes y la configuración para su uso es responsabilidad del Centro de Tecnología Educativa. b. Toda estación de trabajo y equipo portátil deberá ser configurada con credenciales de acceso, conforme el protocolo de configuración y uso de activos de información. c. Los equipos de usuarios finales deben estar configurados de forma que dicha configuración no pueda ser alterada, sin previa autorización del Centro de Tecnología Educativa. d. Si se detecta la instalación de algún aplicativo o herramienta software no autorizada, el Centro de Tecnología Educativa tiene potestad de desinstalar el mismo. e. Todo cambio a la configuración de los equipos debe efectuarse únicamente por el personal del Centro de Tecnología Educativa en coordinación con el área de administración de sistemas.		

	f. El Centro de Tecnología Educativa y la Unidad de Mantenimiento serán los responsables de adecuar las instalaciones eléctricas y de red para los equipos institucionales, así como autorizar las reubicaciones de equipos, garantizado la disponibilidad del sistema de comunicaciones y la seguridad de las conexiones. g. La Unidad de Mantenimiento debe garantizar adecuadas conexiones eléctricas que eviten daños a los equipos o cortes eléctricos. h. El equipamiento tecnológico debe contar con un plan anual de mantenimiento aprobado por el Centro de Tecnología Educativa. Dicho plan se sujeta a la PGS-UNACH-07-Gestión del monitoreo, continuidad y atención de incidentes de seguridad. i. Todo equipo tecnológico de alimentación eléctrica cableada deberá estar conectado a un regulador de voltaje y no directamente a la toma eléctrica. No se deberán conectar al regulador o toma eléctrica otros equipos que no sean aprobados por la Unidad de Mantenimiento. j. La ubicación de puestos de trabajo a parte de las regulaciones descritas debe contar con la revisión y aprobación por parte de la Unidad de Riesgos Laborales, Salud Ocupacional y Gestión Ambiental, conforme sus competencias (sitios seguros de trabajo). k. El Centro de Tecnología Educativa debe manejar el inventario de activos de información tecnológica de la institución. Este inventario debe ser actualizado de forma permanente conforme la PGS-UNACH-01- Gestión de activos de información. l. El equipamiento tecnológico es para uso exclusivo de las actividades institucionales, no estando permitida la salida de los mismos de las instalaciones de la UNACH. Se exceptúan los procesos de mantenimiento externo y ejecución de garantías, siempre y cuando el proceso de contratación lo contemple. m. El personal del Centro de Tecnología Educativa no podrá realizar tareas de soporte o mantenimiento a equipamiento que no pertenezca a la institución. n. La salida de un equipo portátil de la institución deberá ser autorizada por el jefe inmediato del custodio del equipo previo registro del formulario de salida de bienes.
Gestión de las instalaciones	**Gestión de acceso:** a. Las áreas de acceso para estudiantes, docentes, empleados y trabajadores, portando la respectiva identificación, dentro de los horarios de atención y cumpliendo los protocolos de seguridad establecidos, son: bibliotecas, laboratorios, salas de internet, salas de videoconferencias, auditorios, ventanillas de atención a usuarios, etc., y están regulados conforme el protocolo de configuración y uso de activos de información. b. El acceso a áreas seguras está limitado únicamente para quienes cumplen una función relacionada a la misma y son: archivo, áreas de infraestructura y redes, desarrollo, monitoreo y vigilancia. c. El acceso a áreas restringidas está permitido únicamente a personal autorizado, siguiendo los procedimientos de seguridad pertinentes, así: a) Data Center: personal del área de redes e infraestructura. b) Ductos de redes y cableado eléctrico: personal de infraestructura y redes y mantenimiento.

	c) Áreas de monitoreo y vigilancia: personal del área de soporte tecnológico. d. El personal de áreas seguras tiene acceso a las instalaciones dentro de su horario de trabajo. Los accesos fuera de dicho horario deberán ser aprobados por el jefe inmediato. e. El personal de limpieza accederá al cumplimiento de sus funciones en áreas seguras previa autorización de ingreso. La limpieza en áreas restringidas se realiza en presencia del responsable o su delegado. **Gestión de seguridad física:** f. El Centro de Tecnología Educativa debe sujetarse al Plan de Emergencia aprobado por la Unidad de Riesgos Laborales, Salud Ocupacional y Gestión Ambiental y cumplir las directrices de seguridad y recomendaciones establecidas en el mismo. g. El Centro de Tecnología Educativa debe contar con personal de seguridad y sistema de video vigilancia permanente que precautele la seguridad de los usuarios, instalaciones y equipamiento. h. Las personas particulares que requieran realizar un trámite en dicha instalación deberán registrarse en la bitácora respectiva, presentando una identificación y el personal de guardianía será el responsable de controlar el ingreso y salida de los mismos. i. Ninguna persona podrá acceder a estas instalaciones fuera del horario regular de atención, salvo autorización expresa del director del Centro de Tecnología Educativa o su delegado.
Gestión de vulnerabilidades técnicas	Se debe gestionar dentro de los planes de mantenimiento conforme la PGS-UNACH-07-Gestión del monitoreo, continuidad y atención de incidentes de seguridad y garantizar: a. Utilización de un método de protección antivirus. b. Revisión, prueba y actualización periódica de parches de seguridad críticos. c. Revisión, prueba y actualización de versiones de software que cuenten con soporte por parte del fabricante y que no se contrapongan a la operación actual de los sistemas de información. d. Crecimiento de los sistemas de información. e. Capacidad de conexión multiusuario. f. Seguridad perimetral g. Filtro de contenidos, páginas y monitoreo de navegación. h. Pruebas de vulnerabilidad (interna y externa) i. Capacitación técnica al personal de soporte, desarrollo, infraestructura y redes y administración de bases de datos.
Procesos Disciplinarios	La inobservancia a la presente política de seguridad de la información será sancionada conforme la normativa vigente.
Protocolos y procedimientos relacionados	a. Plan anual de Infraestructura y Redes. b. Protocolo de configuración y uso de activos de información. c. Plan anual de mantenimiento del equipamiento tecnológico
Formatos relacionados	a. Formulario de salida de bienes

Código	PGS-UNACH-04	**Revisión:** 01	**Fecha:** 15-03-2018
Política de Seguridad	**Gestión de Comunicaciones**		
Objetivo	Garantizar la confidencialidad, integridad, disponibilidad y no repudio de la información que se transmite a través de la red de comunicaciones interna y externa institucional.		
Alcance	Esta política aplica a toda la infraestructura de la red de comunicaciones institucional.		
Responsables	Ejecución / Cumplimiento: Usuarios de los sistemas Gestión / Administración: Centro de Tecnología Educativa Control / Seguimiento: Centro de Tecnología Educativa		
Gestión			
Gestión de usuarios	a. La gestión de credenciales de acceso a los servicios de comunicaciones (red interna y externa) está bajo la responsabilidad del área de infraestructura y redes, en aplicación del protocolo de configuración y uso de activos de información.		
Gestión de red externa - Internet	a. Se cumple conforme el protocolo de parametrización y seguridad de redes. b. El servicio de Internet a docentes, estudiantes, empleados y trabajadores es para uso exclusivo de las actividades académicas, de investigación, vinculación y gestión administrativa conforme el rol que le compete cumplir a cada usuario. c. No se podrá utilizar el internet como un medio de participación, acceso y distribución de actividades o materiales que vayan en contra de la legislación ecuatoriana y con fines ajenos a los que persigue la UNACH. d. La gestión de la seguridad hacia el internet es responsabilidad del área de infraestructura y redes del Centro de Tecnología Educativa. e. Todo requerimiento referente a enlaces de datos e internet, aumento de ancho de banda, compartimiento de redes, etc.; será receptada y autorizada por el director del Centro de Tecnología Educativa e implementada por el área de infraestructura y redes. f. El área de infraestructura y redes es responsable del monitoreo y revisión periódica del uso apropiado de Internet, así como la gestión de ancho de banda conforme la priorización de necesidades institucionales. g. El usuario es responsable del uso racional del servicio internet, considerándose un uso indebido cuando: 1. Atenta contra la confidencialidad e integridad de la información de la UNACH. 2. Reduce la productividad del personal. 3. Pone en riesgo la disponibilidad de los recursos informáticos. 4. Se accede a sitios no seguros, de pornografía o descarga de material con derechos de autor. 5. Se vulnera o modifica las configuraciones de seguridad institucional para acceder a sitios no autorizados. 6. Descarga e instala software que no esté aprobado por el Centro de Tecnología Educativa. 7. Uso de sitios de entretenimiento, redes sociales y mensajería instantánea que no estén autorizadas. 8. Exceso de uso de sitios no destinados al cumplimiento de labores institucionales.		

Gestión de red interna - Intranet	a. Se cumple conforme el protocolo de parametrización y seguridad de redes. b. La red de comunicaciones interna disponible a docentes, empleados y trabajadores permite el acceso a sistemas de información y carpetas compartidas que conforme el rol de cada usuario requiere para el cumplimiento de sus funciones. Puede ser utilizada dentro de los predios institucionales. c. La gestión de la seguridad de la intranet es responsabilidad del área de infraestructura y redes del Centro de Tecnología Educativa. d. La información de uso en intranet debe ser utilizada únicamente por los usuarios autorizados, mismos que no pueden redireccionar información que aparezca en la intranet hacia terceros, sin autorización de la institución. e. El usuario no puede modificar ni vulnerar la configuración de la red interna. f. La información compartida en la intranet debe ser revisada periódicamente por los usuarios para garantizar su actualidad y relevancia.
Gestión de encriptación	a. El Centro de Tecnología Educativa debe garantizar que la transmisión de datos a través de la red de comunicaciones maneje adecuados procedimientos de encriptación, que aseguren la confidencialidad e integridad de los mismos. b. La plataforma tecnológica institucional debe cifrar sus comunicaciones mediante un certificado digital. La custodia, administración y buen uso de dicho certificado es responsabilidad del Centro de Tecnología Educativa, conforme el protocolo de parametrización y seguridad de redes
Accesos remotos	a. El acceso remoto a servidores previa autorización del Centro de Tecnología Educativa, será gestionado por la unidad de Infraestructura y Redes mediante el uso de redes privadas virtuales VPN con encriptación. b. Se debe realizar una supervisión de los accesos remotos. c. El acceso remoto a equipos de cómputo para usuarios finales no está permitido, salvo requerimiento expreso del titular de la unidad al Centro de Tecnología Educativa, instancia que analiza y autoriza los mismos. d. Los soportes remotos por terceros o proveedores de servicios deben ser asignados, aprobados y documentados por el Centro de Tecnología Educativa. Las credenciales de acceso se asignan de forma temporal mientras duren las actividades de soporte y se debe monitorear las actividades desarrolladas durante la vigencia de las mismas. e. El soporte remoto a usuarios finales lo autoriza el director del Centro de Tecnología Educativa en casos excepcionales.
Gestión del correo electrónico institucional	a. El uso del correo electrónico institucional es obligatorio para todos los miembros de la comunidad universitaria para la realización de actividades académicas, de investigación, vinculación o gestión administrativa inherentes al cumplimiento de sus funciones. No está permitido el uso de correos electrónicos personales para el desarrollo de actividades institucionales.

	b. La creación de cuentas de correo electrónico se realiza al momento de dar de alta al nuevo usuario (docente, estudiante, empleado o trabajador). c. El correo electrónico institucional no puede ser utilizado para difundir mensajes ofensivos, denigrantes, de contenido sexual o que atenten contra la integridad de las personas. d. Los protocolos de seguridad deben resguardar a las cuentas de usuarios respecto al spam, sin embargo, es responsabilidad del usuario no abrir vínculos, archivos anexos, ni reenviar mensajes de usuarios no conocidos o que suponga riesgo a la seguridad de la red y los equipos. e. Las cuentas de correo electrónico bajo el dominio unach.edu.ec pertenecen a la Universidad Nacional de Chimborazo, por lo tanto, la institución podrá monitorear el uso de dichas cuentas, a fin de precautelar los intereses institucionales. f. La información de uso institucional que requiera ser enviada por mensajería electrónica, deberá hacerlo utilizando el correo electrónico del usuario que está bajo el dominio unach.edu.ec. g. El correo electrónico institucional es para uso exclusivo de actividades académicas y administrativas, conforme el rol del usuario. h. No está permitido utilizar otros medios de comunicación como redes sociales y el correo electrónico personal para realizar trámites o enviar información institucional. i. Se excluye del punto anterior a las noticias e información que difunde el Departamento de Relaciones Nacionales e Internacionales a través de las redes sociales oficiales con las que cuenta la institución. j. El Departamento de Relaciones Nacionales e Internacionales es el único canal institucional autorizado para enviar correos electrónicos masivos. k. No está permitido utilizar la cuenta de correo electrónico institucional para suscribirse a páginas, blogs o redes sociales, de uso particular. l. El usuario debe analizar con la herramienta de protección antivirus los archivos adjuntos que recibe a través del correo electrónico, y que provienen de fuentes confiables. m. Conforme la normativa legal vigente, los mensajes enviados por correo electrónico, tienen el mismo valor jurídicos que los documentos escritos, por lo tanto, es responsabilidad de los usuarios monitorear de forma permanente los mensajes recibidos a la cuenta institucional, que permita acatar o cumplir las disposiciones recibidas a través de este medio. n. Es responsabilidad de los usuarios de correo electrónico mantener o archivar los mensajes enviados y/o recibidos que sustenten el cumplimiento de acciones, así como depurar la información almacenada en el buzón por pérdida de vigencia o relevancia. o. Las cuentas de correo electrónico deben manejar el pie de firma conforme la imagen corporativa institucional aprobada, no debiendo realizar parametrizaciones con logos o imágenes fuera de dicha imagen.
Gestión de telefonía IP	f. La telefonía IP está orientada al cumplimiento de actividades inherentes al rol que desempeña el personal académico y administrativo y se ejecuta conforme el protocolo de configuración y uso de activos de información.

Procesos Disciplinarios	La inobservancia a la presente política de seguridad de la información será sancionada conforme la normativa vigente.
Protocolos y procedimientos relacionados	a. Protocolo de parametrización y seguridad de redes.

Código	PGS-UNACH-05	**Revisión:** 01	**Fecha:** 15-03-2018
Política de Seguridad	**Gestión de desarrollo y adquisición de software**		
Objetivo	Gestionar el desarrollo y adquisición de sistemas seguros, que garanticen su integración, actualización y mantenimiento.		
Alcance	Esta política aplica a todos los proyectos de desarrollo internos y para contratación con terceros que requiera la institución		
Responsables	Ejecución / Cumplimiento: Centro de Tecnología Educativa Gestión / Administración: Centro de Tecnología Educativa Control / Seguimiento: Centro de Tecnología Educativa		
Gestión			
Proyectos de desarrollo y adquisición	a. Para la gestión de proyectos propios o contratación de terceros para desarrollo de software, el Centro de Tecnología Educativa debe manejar la metodología de desarrollo de aplicativos y sus formatos relacionados que permita documentar las siguientes actividades: 1) Informe de factibilidad 2) Acta de Constitución del Proyecto 3) Documento de Especificación de Requisitos de Software 4) Documento de la Arquitectura de la Solución 5) Documento de la Arquitectura de la Aplicación 6) Diccionario de datos 7) Plan de Pruebas 8) Plan de Capacitación 9) Documento de Cierre del Proyecto b. La documentación precontractual, términos de referencia y contractual para los casos de desarrollo con terceros debe contemplar la necesidad de: 1) Firma de acuerdo de confidencialidad conforme la PGS-UNACH-01-Gestión de activos de información. 2) Documentación de desarrollo de aplicativos 3) Requerimientos de seguridad respecto a los aplicativos. 4) Responsabilidad del contratista respecto al uso de la infraestructura tecnológica a la que tenga acceso, conforme los servicios prestados. c. Los proyectos de contratación a terceros deben cumplir además las regulaciones del procedimiento de contratación pública.		
Ciclo de vida	a. Debe definirse y aplicarse una metodología de desarrollo de aplicativos que contemple como mínimo las siguientes fases: 1) Concepción / análisis de negocio: levantamiento de información, análisis situacional y documentación. 2) Planeación y diseño: diseño de la solución y plan de ejecución. 3) Desarrollo: Especificar herramientas de desarrollo, estructura y arquitectura de la solución, modelos entidad-relación y diccionarios de datos. 4) Prototipo y pruebas: presentación de prototipos de evaluación y ajuste. 5) Instalación y estabilización: plan de implementación, migración y estabilización de la solución. 6) Soporte y mantenimiento: plan de mantenimiento correctivo, niveles de acuerdo con servicios y plan de continuidad de la solución que incluya planes de respaldo, recuperación y contingencia.		

	7) Para cada solución se deben entregar y mantener actualizado: manual de usuario, manual de administración, manual técnico de instalación y configuración.
Ambientes de trabajo	a. Para la adecuada gestión de proyectos de desarrollo, mantenimiento, prueba e implementación, se debe implementar la infraestructura mínima de seguridad que garantice la adecuada gestión y control de los proyectos de software, con los siguientes ambientes tecnológicos: 1) Ambiente de desarrollo: configuración orientada al desarrollo de software, en el cual se puede crear y modificar los objetos a solicitud del área responsable de la Información 2) Ambiente de Pruebas: configuración orientada a la generación de pruebas, replica del ambiente de producción en donde se realizarán todas las pruebas necesarias para garantizar el buen funcionamiento de los aplicativos. 3) Ambiente de Producción: configuración orientada al usuario final donde se realiza el procesamiento real de la información utilizada para la toma de decisiones de la UNACH. b. Para cada ambiente debe existir una configuración independiente en sistema operativo, base de datos y aplicación. c. Cada ambiente debe manejar roles y credenciales de acceso diferentes.
Plan de pruebas	a. Debe definirse un plan de pruebas que defina actividades y responsables, así como niveles y tipos de pruebas que se deban realizar a los aplicativos. b. Los datos del ambiente de pruebas deben ser una réplica del ambiente de producción. c. El resultado de las pruebas debe documentarse por los desarrolladores en conjunto con los usuarios del área solicitante.
Control de cambios	1) Se debe mantener actualizado el inventario de aplicativos, detallando su estado: desarrollo o producción y si ha sido un desarrollo propio o adquisición a terceros. 2) Para todos los cambios y ajustes autorizados se debe seguir la metodología de desarrollo de aplicativos y el formato de control de cambios. 3) Los cambios de emergencia deben ser debidamente aprobados, auditados y documentados, conforme el procedimiento anterior. 4) Las modificaciones a los aplicativos podrán ser solicitadas por el titular de la unidad y aprobado por el Centro de Tecnología Educativa. Si se requieren cambios a los datos, deben ser aprobados por el responsable de la información y se debe llenar el registro de cambios de información. 5) Se debe manejar el procedimiento de solicitud, autorización y aprobación de cambios a aplicativos. 6) La documentación y manuales de todas las aplicaciones debe ser actualizada de forma permanente por los desarrolladores y una copia de los mismos debe reposar en el Centro de Tecnología Educativa archivada como información confidencial (a excepción de los manuales de usuario).
Gestión segura de desarrollo	a. El Centro de Tecnología Educativa debe implementar los mecanismos y herramientas necesarias para garantizar la seguridad en los procedimientos y métodos de desarrollo, operaciones y gestión de

	cambios de las aplicaciones que se desarrollen o contraten a terceros para la institución. b. A los sistemas de información se debe poder acceder únicamente con credenciales (seguras). La contraseña debe estar encriptado. c. Todo sistema de información debe tener configuraciones de acceso por perfil de usuario. d. Únicamente el administrador del sistema de información debe tener acceso a los roles de usuario. e. Las bases de datos y aplicaciones deben tener pistas de auditoría conforme establece la PGS-UNACH-01 Gestión de activos de información. f. Todos los cambios a programas deben realizarse en el ambiente de desarrollo, los desarrolladores no deben tener acceso al ambiente de producción. g. Los desarrolladores deben tener acceso únicamente al ambiente de desarrollo y pruebas. h. Cada ambiente (desarrollo y prueba) debe manejar una base de datos independiente, con igual configuración y parametrización del ambiente en producción. i. Se debe considerar lenguajes de programación que garanticen una fácil integración con los demás sistemas de información, conforme el licenciamiento que cuente la institución.
Procesos Disciplinarios	La inobservancia a la presente política de seguridad de la información será sancionada conforme la normativa vigente.
Protocolos y procedimientos relacionados	a. Metodología de desarrollo de aplicativos b. Plan de pruebas c. Solicitud, autorización y aprobación de cambios a aplicativos.
Formatos relacionados	a. Formatos desarrollo de aplicativos b. Resultados pruebas c. Registro de control de cambios d. Registro de cambios de información

Código	PGS-UNACH-06	**Revisión:** 01	**Fecha:** 15-03-2018
Política de Seguridad	**Gestión de Monitoreo, Continuidad y atención de incidentes de seguridad**		
Objetivo	Garantizar el monitoreo y continuidad de la seguridad respecto a los activos de información de la UNACH. Garantizar la confidencialidad, integridad y disponibilidad de la información antes, durante y después de un incidente de seguridad.		
Alcance	Esta política cubre todos los procesos relacionados al monitoreo y continuidad de la gestión de seguridad para los activos de información de la UNACH; así como todos los procesos relacionados a un incidente de seguridad su prevención, mitigación y recuperación.		
Responsables	Ejecución / Cumplimiento: Usuarios de los sistemas de información Gestión / Administración: Centro de Tecnología Educativa Control / Seguimiento: Centro de Tecnología Educativa		
Gestión			
Equipo de gestión de seguridad de la información - EGSI	a. La institución debe contar con un equipo multidisciplinario de gestión de la seguridad de la información, nombrado por la máxima autoridad (preside el director del Centro de Tecnología Educativa) y encargado de: i. Revisión, socialización y monitoreo del cumplimiento de las políticas de seguridad de la información, aprobadas por el Órgano Académico Colegiado Superior. ii. Gestión de procedimientos disciplinarios por incumplimiento de políticas de seguridad, con base a la normativa legal vigente. iii. Evaluación de los resultados de los incidentes de seguridad. iv. Elaboración, ejecución y seguimiento del plan de continuidad de la seguridad de la información, con base a los resultados de la gestión de monitoreo y la evaluación de incidentes de seguridad. v. Elaboración, ejecución y evaluación del plan anual de capacitación en seguridad para los usuarios de la institución. vi. Coordinación con las áreas involucradas respecto a la gestión de riesgos de los activos de información. vii. Coordinación y supervisión de las actividades del CSIRT institucional. viii. Coordinación con autoridades y proveedores externos relacionados a los servicios de los sistemas de información (suministro eléctrico, internet, soporte técnico de infraestructura, etc.)		
Equipo de atención de incidentes de seguridad - CSIRT	a. Es designado por el equipo de gestión de seguridad de la información, con aprobación de la máxima autoridad, y sus responsabilidades son: 1. Trabajar de forma coordinada con el CSIRT de CEDIA. 2. Notificar y gestionar la implementación de controles de seguridad ante nuevas amenazas identificadas. 3. Controlar y mitigar el impacto adverso de un incidente de seguridad con base al plan de recuperación de desastres. 4. Documentar los resultados de los incidentes de seguridad para su evaluación y aprendizaje. 5. Notificar los resultados de incidentes de seguridad al EGSI, con las evidencias respectivas en los casos que corresponda.		

Gestión de eventos e incidentes de seguridad	a. Los usuarios de la plataforma tecnológica tienen la responsabilidad de informar al Centro de Tecnología Educativa respecto a cualquier evento de seguridad detectado en la operación de la misma. b. Las situaciones catalogadas para comunicar un evento de seguridad son: 1. Control ineficaz de seguridad 2. Incumplimiento de políticas de seguridad 3. Falla en el funcionamiento de los sistemas de información o comportamiento anómalo. 4. Detección de links de publicidad o similares que no forman parte de la configuración de la plataforma tecnológica. 5. Redireccionamiento a otros sitios web cuando se está navegando en la red. 6. Pérdida de activos de información 7. Hurto de credenciales de acceso. 8. Detección de accesos no autorizados. 9. Otra que se considere pueda comprometer la confidencialidad, integridad y disponibilidad de la información. c. El Centro de Tecnología Educativa con el EGSI verificará los eventos de seguridad reportados y analizará si el mismo debe ser catalogado como un incidente de seguridad, en cuyo caso deberá activar de forma inmediata al CSIRT para su correspondiente atención. d. Si el evento de seguridad no cumple las características para ser catalogado como incidente, se coordinará con la instancia correspondiente para dar solución al mismo. e. El resultado del análisis debe ser documentado para futuras referencias y se debe llevar el registro respectivo de todos los eventos de seguridad.
Gestión del monitoreo	a. El monitoreo de la seguridad de los activos de información se cumple de forma transversal conforme los resultados de los siguientes elementos de gestión de seguridad: 1. Plan anual de mantenimiento de Infraestructura y Redes 2. Plan anual de mantenimiento de la infraestructura tecnológica 3. Plan anual de mantenimiento de bases de datos y aplicaciones 4. Gestión de riesgos de los activos de información b. Los resultados del cumplimiento de dichos planes sirven al EGSI para evaluar el estado de la seguridad y proponer el plan de continuidad.
Gestión de la Continuidad	a. Se basa en la ejecución, evaluación y actualización del plan de continuidad de la seguridad de la información a cargo del EGSI. b. El EGSI debe realizar un informe anual para conocimiento de las autoridades, respecto al estado de seguridad de la información en la institución. c. La gestión de la continuidad de la seguridad de la información debe formar parte del PETI vigente.
Procesos Disciplinarios	La inobservancia a la presente política de seguridad de la información será sancionada conforme la normativa vigente.
Protocolos relacionados	a. Plan de atención de desastres b. Plan anual de capacitación c. Plan de continuidad de seguridad de la información
Formatos relacionados	

Código	PGS-UNACH-07	**Revisión:** 01	**Fecha:** 15-03-2018
Política de Seguridad	**Gestión de Seguridad de la información para usuarios**		
Objetivo	Garantizar el uso adecuado de los activos de información por parte de los usuarios, proveedores y contratistas que tengan relación con la institución.		
Alcance	Esta política aplica a todos los usuarios de la plataforma tecnológica de la UNACH, así como proveedores y contratistas que por la naturaleza de la relación contractual accedan a información de la institución.		
Responsables	Ejecución / Cumplimiento: Usuarios de los sistemas Gestión / Administración: Centro de Tecnología Educativa Control / Seguimiento: Centro de Tecnología Educativa		
Gestión			
Gestión de la información	a. El uso de los activos de información se sujeta a las directrices de la PGS-UNACH-01- Gestión de activos de información b. Todo usuario que utilice recursos informáticos institucionales tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad, y auditabilidad de la información que maneje. c. El uso de medio extraíbles para almacenar, respaldar o transferir información institucional, se sujeta a las directrices de la PGS-UNACH-01- Gestión de activos de información d. No se debe guardar archivos que contengan información sensible en el escritorio del equipo.		
Uso de equipamiento tecnológico institucional	a. Los usuarios custodios del equipamiento tecnológico (estaciones de trabajo, portátiles, tabletas, impresoras, etc.), son los responsables del buen uso y cuidado de los mismos, así como de la información contenida en ellos. b. El equipamiento tecnológico asignado a un usuario, deben sujetarse al cumplimiento de la PGS-UNACH-03- Gestión de Infraestructura hardware y entorno c. El acceso al sistema de comunicaciones está regulado conforme la PGS-UNACH-04- Gestión de Comunicaciones. d. Los usuarios de equipamiento tecnológico portátil no tienen potestad de prestar o reasignar dichos equipos a personas ajenas a la institución. e. En caso de robo, pérdida o hurto de equipamiento portátil, debe ser notificado de forma inmediata al Centro de Tecnología Educativa. f. Las sesiones de acceso a los sistemas de información deben estar activas únicamente cuando el usuario está haciendo uso de los mismos. g. Cuando el usuario debe alejarse momentáneamente del equipo tecnológico, este debe ser protegido por bloqueo de pantalla. h. El usuario tiene la responsabilidad de apagar los equipos cuando estos no estén en uso. i. No consumir alimentos, bebidas o fumar cerca de la infraestructura tecnológica. j. No insertar objetos extraños en las ranuras de los equipos de cómputo y periféricos. k. No realizar actividades de mantenimiento de hardware.		

	l. No tener peceras, maceteros, ambientadores o cualquier otro que pueda derramarse y provocar daños a los equipos.
Credenciales de usuario	a. Las credenciales de acceso a la plataforma tecnológica institucional (equipamiento, sistemas de información, mensajería electrónica y redes de comunicación) otorgadas al usuario para el desempeño de sus funciones, son de uso exclusivo del titular de las mismas. b. El usuario es custodio y responsable de dichas credenciales no debiendo facilitar las mismas a ninguna persona, ni enviarlas por ningún medio de mensajería electrónica. c. El usuario es responsable de la información que se accede, procesa y entrega bajo las credenciales asignadas al mismo. d. Las credenciales deben ser fáciles de recordar, pero no basadas en información personal o fechas especiales. e. No se debe utilizar la característica "recordar contraseña" de las aplicaciones. f. No ingresar las credenciales de la plataforma tecnológica en un equipo que no se considere confiable. g. El usuario que sea reubicado en la institución para cumplir otra función deberá asegurarse que las credenciales de acceso a la plataforma tecnológica que ya no utilizará sean revocadas. No deberá acceder a información que conforme su nueva función ya no le compete acceder. h. El usuario que termine su relación laboral con la institución deberá llenar el Formulario Paz y Salvo, garantizando la revocación de sus credenciales a todos los sistemas de información institucional. i. Los usuarios de equipos tecnológicos institucionales podrán almacenar información de uso personal en los equipos institucionales, siempre y cuando la misma no comprometa la seguridad y capacidad de operación del equipo.
Responsabilidades y Restricciones	a. Los usuarios de la infraestructura tecnológica de la UNACH tienen la responsabilidad de verificar que el uso de activos de información se cumpla conforme las políticas de seguridad institucionales, debiendo notificar de forma inmediata al Equipo de Gestión de Seguridad de la Información cualquier procedimiento que no esté conforme las políticas vigentes. b. De igual forma es responsabilidad de los usuarios, informar sobre cualquier incidente de seguridad, vulnerabilidad o amenaza detectada en la utilización de los sistemas de información, que pueda comprometer la seguridad de los mismos, conforme la PGS-UNACH-06 – Gestión de monitoreo, continuidad y atención de incidentes de seguridad. c. Está prohibido el acceso no autorizado a la plataforma tecnológica institucional y el uso indebido de los recursos informáticos. Se considera que hay uso indebido de la información y de los recursos, cuando la persona incurre en cualquiera de las siguientes conductas: 1) Suministrar o hacer pública la información sin la debida autorización, o usa la información con el fin de obtener beneficio propio o de terceros. 2) Hurtar software de la UNACH (copia o reproducción entre usuarios).

	3) Copiar un producto informático de la UNACH. 4) Instalar, modificar, reubicar o sustraer equipos de cómputo, software, información o periféricos sin la debida autorización. 5) Transgredir o burlar los mecanismos de autenticación u otros sistemas de seguridad. 6) Utilizar la infraestructura de la UNACH (computadores, software, información o redes) para acceder a recursos externos con propósitos ilegales o no autorizados. 7) Descargar o publicar material ilegal, con derechos de propiedad o material nocivo usando un recurso de la UNACH. 8) Uso personal de cualquier recurso informático de la UNACH para acceder, descargar, imprimir, almacenar, redirigir, transmitir o distribuir material pornográfico. 9) Violar cualquier Ley o Regulación nacional respecto al uso de sistemas de información, información personal y derechos de propiedad intelectual. 10) Inobservar las políticas de seguridad de la información de la UNACH.
Procesos Disciplinarios	La inobservancia a la presente política de seguridad de la información será sancionada conforme la normativa vigente.
Procedimientos relacionados	
Formatos relacionados	a. Formulario de salida de bienes b. Formulario Paz y Salvo

13. PROTOCOLOS DE SEGURIDAD

Los protocolos mencionados en estas políticas de Seguridad, se encuentran documentados y clasificados como información confidencial en el Centro de Tecnología Educativa de la Universidad Nacional de Chimborazo.