INDICE

Generalidades 1

Objetivo 2

Alcance 2

Responsabilidades 2

Descripción de la Política 3

Creación de Usuarios 4

Gestión de accesos de Usuarios 4

Gestión de Privilegios 5

Seguimiento y Auditoria 5

Gestión de Contraseñas de Usuario 5

Revisión de los Derechos de Acceso de los Usuarios 6

Consecuencias y Sanciones 6

Estándares 6

Creación de cuentas 7

Registros 7

Generalidades

Proceso al cual pertenece:	SEGURIDAD CONTROL DE ACCESOS LOGICOS

Frecuencia de ejecución:		CONTÍNUA	
Tipo de Documento:		POLITICA	
Fecha de elaboración:	15 JULIO 2016	**Versión del documento:**	001

Objetivo

Proteger la información institucional, normando el acceso a través de los sistemas informáticos, considerando: perfiles, permisos, cuentas, contraseñas y protectores de pantalla.

Alcance

Las normas definidas en esta política cubren toda la información que se encuentra almacenada y gestionada en activos tecnológicos. Su cumplimiento es de carácter obligatorio para quienes necesitan hacer uso de a la misma.

Responsabilidades

El responsable de la División de Centro de Cómputo, estará a cargo de:

- Definir normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información.
- Participar y revisar los controles de cambios, aprobar o rechazar un cambio luego de poseer un informe de impacto de las áreas involucradas en el cambio.
- Verificar el cumplimiento del procedimiento de control de cambios.
- Verificar el cumplimiento relacionadas con control de accesos, registro de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, protección de puertos, control de conexiones a la red, etc.
- Autorizará o denegará el acceso remoto a la administración de servicios críticos de la UNIVERSIDAD DE GUAYAQUIL y a datos sensibles, luego de que el proceso de control, autorización y perfiles de usuario se hayan realizado, verificando que se adopten todas las medidas que correspondan en materia de seguridad de la información.
- Los administradores de los servicios junto con el responsable de Seguridad de información, estarán encargados de identificar los riesgos a los cuales se expone la información con el objeto de:

- ✓ Definir el plan de acción que permita mitigar los riesgos encontrados en: los controles de accesos y autenticación.

- ✓ Definir los eventos y actividades de usuarios a ser registrados en los sistemas para la revisión de los mismos.

- ✓ La Dirección del Centro de Computo, realizará auditorias periódicas a los sistemas, los mismo que tendrán acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad, así como también a los servidores, correos electrónicos y todo a lo referente a la seguridad de la información.

- **La Dirección Talento Humano se encargará de:**

  - ✓ Notificar vía correo electrónico al Director de Tecnología y al responsable de la seguridad de la información, el cambio de rol, o la salida o ingreso de un empleado para que los administradores de los servicios procedan a eliminar/crear inmediatamente accesos y permisos a los sistemas informáticos. Llenar Formulario de accesos.

  - ✓ Emitir un reporte mensual a la División de Centro de Computo, en el que se detalle todos los ingresos y salidas de personal.

Descripción de la Política

Normas y Disposiciones Generales

Consideraciones Generales

Los Directores y jefes de cada área de la UNIVERSIDAD DE GUAYAQUIL conjuntamente con el dueño del Servicio tienen la responsabilidad de crear procesos formales para la gestión de usuarios de los sistemas informáticos, en los cuales se debe considerar:

- ✓ Definición de roles y perfiles
- ✓ El rol está definido por la función que cumple un usuario dentro de un sistema.
- ✓ El perfil es la descripción detallada de las transacciones que un usuario puede realizar. Son los privilegios con los que cuenta un usuario.
- ✓ Procedimiento de autorización, acceso y nivel de privilegios en los sistemas.

- ✓ Procedimiento de entrega de usuarios y claves a los sistemas de manera adecuada y segura.

- ✓ Procedimientos de creación de usuarios.
- ✓ Procedimiento para dar de baja a los usuarios en los sistemas.
- ✓ Los sistemas informáticos deben estar configurados de tal manera que la sesión de los usuarios caduque cuando exista un tiempo de inactividad de 15 minutos. Esto obligatoriamente para los sistemas definidos como críticos y para los usuarios de administración de los sistemas.

Creación de Usuarios

Cada administrador de servicios conjuntamente con el Dueño del Servicio deberán definir el flujo de autorización y procedimiento de creación de usuarios considerando: las solicitudes y autorizaciones, roles y perfiles.

El nombre de usuario debe estar creado según el estándar definido (Ver estándar: Creación de cuentas).

Gestión de accesos de Usuarios

Registro de Usuarios

El jefe de cada área de la UNIVERSIDAD DE GUAYAQUIL conjuntamente con el Dueño del Servicios debe definir el flujo de autorización para el acceso y el nivel de privilegios en los sistemas.

El otorgamiento de roles y perfiles de usuario deberá ser definido de acuerdo al principio del mínimo privilegio.

Todo el personal de la EPPUEP tendrá asignado un nombre único de usuario y contraseña para acceder a los sistemas informáticos permitidos según su perfil. Esta debe ser autorizada por el Oficial de Seguridad de información, Dirección Tecnología, Responsable de la seguridad de la información, Jefe inmediato, Dirección Talento Humano.

Los administradores de servicios deberán otorgar acceso a los diferentes sistemas siempre que el solicitante posea la respectiva autorización.

Los administradores de cada servicio deberán mantener actualizado sus registros de usuario. Así como una bitácora relacionada a accesos lógicos de los mismos.

Los administradores de servicios deberán, solicitar al usuario firmado y aprobado el formulario de solicitud de permiso para el acceso de una información que este solicitando Esto aplica cuando no es dueño de su propia información. (Solicitud de acceso información de terceros).

Gestión de Privilegios

Cada aplicación debe gestionar el nivel de privilegios que tienen los usuarios dentro del sistema informático.

Todo el personal de la UNIVERSIDAD DE GUAYAQUIL debe estar asociado a un rol/perfil en los sistemas informáticos de acuerdo a las actividades que realiza.

Es responsabilidad de los administradores de servidores y servicios, la correcta administración de las cuentas de acceso, el otorgamiento de privilegios de acuerdo a las autorizaciones que se especifiquen en el flujo de autorización.

Se deberá bloquear y prohibir el acceso y uso de servicios de redes sociales y entretenimiento. Salvo el caso que tengan la debida justificación y autorización del servicio.

Seguimiento y Auditoria

Se deberá activar el registro de auditoría en los servicios, servidores, equipos de comunicación y sistemas críticos y correo electrónico, para aquellos usuarios que mantengan privilegios administrativos.

Los registros de auditoría deberán ser eliminados periódicamente, para que no afecten el rendimiento de los servicios. (Mínimo 6 meses el cual deberá ser almacenado).

Gestión de Contraseñas de Usuario

Se debe aplicar el estándar de creación de contraseñas seguras para el acceso de usuarios finales a los diferentes sistemas. (ver estándar: Creación de Contraseñas para usuarios finales).

Se debe aplicar el estándar de creación de contraseñas seguras para el acceso a la administración de los sistemas, servidores o equipos de comunicación (ver estándar: Creación de Contraseñas para administración).

Permitir que el usuario cambie su clave obligatoriamente cuando ingresa por primera vez al sistema.

Bloquear al usuario en la aplicación por 15 minutos luego de 3 intentos fallidos.

Cambiar la contraseña al menos cada 6 meses para los usuarios finales, y 3 meses para las cuentas administradores de servicios, servidores o equipos de comunicación.

Verificar la robustez de las contraseñas según estándar de la UNIVERSIDAD DE GUAYAQUIL.

Se debe cambiar inmediatamente la contraseña al sospechar o detectar que ha sido comprometida.

Revisión de los Derechos de Acceso de los Usuarios

Los directores Y jefes de área de la UNIVERSIDAD GUAYAQUIL serán responsables de ejecutar una depuración de los derechos y privilegios de acceso de los colaboradores a su cargo, tanto en los sistemas informáticos, dispositivos de red, bases de datos, servidores. Esto se lo debe realizar mínimo dos veces al año.

Los administradores de servicios deberán reportar trimestralmente al Director de Centro de Computo, los derechos y privilegios de acceso de los usuarios con altos privilegios en los activos de información.

Consecuencias y Sanciones

En caso de existir incumplimiento de la presente Política de Seguridad de la Información por parte de un trabajador de la UNIVERSIDAD DE GUAYAQUIL, se comunicará a la Dirección de Talento Humano, para que tomen las medidas de sanción respectivas por incumplimiento de acuerdo a las normativas internas oficiales a mas de las responsabilidades civiles y penales a que hubiere lugar.

Estándares

Creación de contraseñas para usuarios finales de sistemas o aplicaciones

- ✓ La contraseña debe tener una longitud mínima de seis caracteres
- ✓ La contraseña debe ser una combinación de letras y números.
- ✓ Nombre de Equipo de estaciones de trabajo

Creación de contraseñas para administración

- ✓ La contraseña debe tener una longitud mínima de ocho caracteres
- ✓ La contraseña debe ser una combinación de letras mayúsculas, minúsculas, números y caracteres especiales
- ✓ La contraseña no debe estar conformada por nombres o palabras comunes.

Creación de cuentas

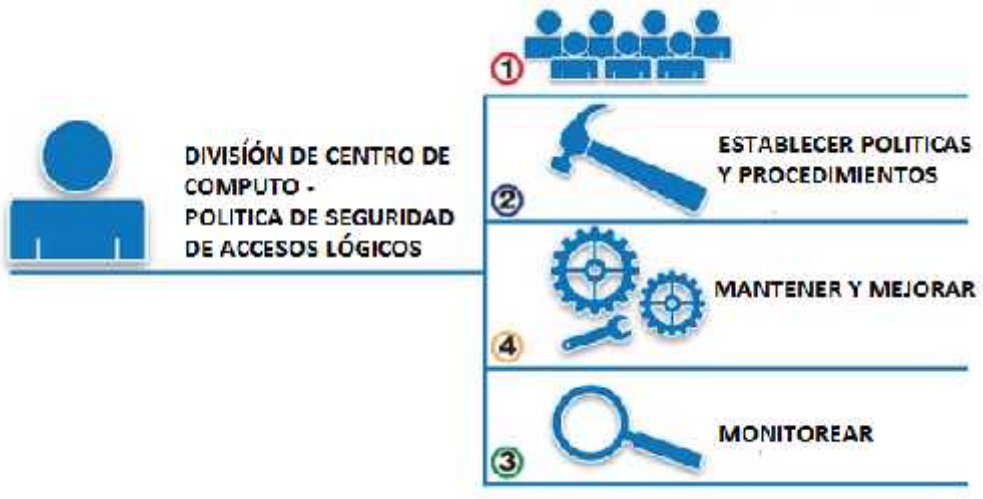
El nombre de usuario estará conformado por:

- ✓ Primer nombre
- ✓ Apellido
- ✓ Letra del segundo apellido
- ✓ En caso que ya exista el nombre de usuario agregar letra del segundo nombre.
- ✓ Ejemplo:

- Usuario: Patricio Juan Carbo Aguilar

Cuenta de usuario: patricio.carboa (Si ya existe el usuario, se cambiaría patricioj.carboa)
Cuando las combinaciones existan nombres inapropiados,(que sea objeto de burla), se cambiaria las combinaciones.

GESTIÓN DE SEGURIDAD



Registros

Fecha: 15 de Julio 2016		

Elaborado Por :	**Revisado Por :**	**Aprobado Por :**
Nombre: Ing. Jenny Arízaga Gamboa, Msia	**Nombre:** Ing. Inelda Martillo Alcívar , Mgs	**Nombre:** Arq. Felipe Espinoza , Mgs
Cargo: Jefa de Infraestructura Tecnológica **Firma**	**Cargo:** Directora de División Centro de Computo **Firma:**	**Cargo:** Vicerrector Administrativo **Firma:**