



Universidad Laica Eloy Alfaro de Manabí
Facultad de Ciencias Informáticas



Materia: Administración de Unidades Informáticas

Trabajo autónomo N°: 7

Tema: Control

Integrantes:

Alcívar Aguirre Juan José

Bustos Intriago Ricardo Antonio

López Anchundia Yandri Alexander

Curso: 9no semestre “A”

Docente: Ing. Johnny Larrea P.

Fecha: 1 de febrero de 2021

Año lectivo: 2020 (2)

Contenido

1. Control Interno..... 1

1.1 Control Administrativo 1

1.2 Control de Documentación 2

1.3 Control de Procesamiento 3

1.4 Control de Seguridad..... 4

1.5 Control de Personal..... 5

1. Control Interno

1.1 Control Administrativo

1) Política de adquisición de hardware y software - El proceso de adquisición se realizará una vez por año, llevado a cabo por el Director de TI.
2) Política de compromiso y responsabilidad de uso de los bienes informáticos - Esta política será definida una vez, pero se actualizará con cada bien informático adquirido sin previa existencia, y será puesta en práctica por los Jefes de Área.
3) Política de uso de Firmas Electrónicas - Las firmas electrónicas serán definidas y creadas una sola vez por medio de la institución correspondiente, bajo la supervisión del Especialista en Gestión de la Información.
4) Política de capacitación de personal de áreas internas - La capacitación del personal se realizará en períodos de 6 meses según requerimientos previamente establecidos, serán los Jefes de Áreas los encargados de las capacitaciones.
5) Política de cumplimiento de objetivos estratégicos - El cumplimiento de los objetivos serán evaluados en períodos de un año, serán los Jefes de Área en coordinación con el Director de TI los encargados de dicha actividad.
6) Política de proceso de selección de personal - Se seleccionará personal cuando sea necesario cubrir una vacante, esta operación se ejecutará conjuntamente entre los Jefes de Área y el Director de TI.
7) Política de auditoría interna - El proceso de auditoría interna se lo realizará en períodos de 6 meses, bajo la tutela del Jefe del Área de Pruebas y Aseguramiento de la Calidad.
8) Política de planificación departamental - Se planificará una vez al año o previo un período de tiempo que se requiera para cumplir un objetivo específico, lo ejecutarán los Jefes de Área junto al Director de TI.

1.2 Control de Documentación

1) Política de inventario

- Se definirá y actualizará el inventario de todo el material físico cada mes, lo realizará el Especialista en Gestión de la Información y Riesgo Tecnológico.

2) Política de sanciones por incumplimiento de estándares

- Se aplicarán sanciones correspondientes con incumplimientos documentados en el momento pertinente, será responsable de la aplicación de dichas sanciones el Director de TI.

3) Política de gestión de documentos físicos y electrónicos de archivo

- Se gestionarán documentos físicos y su conversión o aplicación en documentos digitales o electrónicos inmediatamente se realice su recepción por parte del Especialista en Gestión de la Información y Riesgo Tecnológico.

4) Política de formación en gestión documental y gestión del cambio

- Se capacitarán al nuevo personal que brinde servicio documental en el momento determinado de su incorporación laboral, por parte del Especialista en Gestión de la Información y Riesgo Tecnológico.

5) Política de adopción y actualización permanente de la regulación documental

- Se llevará a cabo una revisión y auditorías de los documentos en existencia para detectar anomalías y pérdidas, el encargado de esta actividad será el Especialista en Gestión de la Información y Riesgo Tecnológico.

6) Política de respaldo documental de información técnica de las Áreas de TI

- Se respaldará la información de manera digital y documentada cada mes de los proyectos vigentes y en desarrollo, esta actividad será una cooperación del Especialista en Gestión de la Información y Riesgo Tecnológico y los Jefes de Áreas del departamento de TI.

7) Política de preservación documental

- Se realizarán copias de seguridad de documentos físicos en formato virtual cada semana para contar con un respaldo, lo realizará el Especialista en Gestión de la Información y Riesgo Tecnológico.

8) Política de la actualización de servicios documentales

- Los servicios documentales se irán actualizando e incorporando mejoras tecnológicas cada 6 meses, el encargado de esta actividad será el Especialista en Gestión de la Información y Riesgo Tecnológico.

1.3 Control de Procesamiento

1) Política de cambios y modificaciones a los sistemas informáticos

- Se podrán realizar cambios necesarios a los sistemas informáticos cada semana previo creación de puntos de restauración y copias de seguridad de los mismos, lo llevarán a cabo el Jefe del Área de desarrollo.

2) Política de desarrollo de aplicaciones

- El desarrollo de nuevas aplicaciones se podrán realizar cada 6 meses previo análisis del proyecto a ejecutar, el responsable será Jefe de Área de Desarrollo y Proyectos Tecnológicos.

3) Política de gestión de base de datos

- Se deberán crear copias de seguridad de manera diaria, semanal y mensual, y se podrán borrar dichas copias después de 2 meses en desuso, lo llevará a cabo el Administrador de base de datos.

4) Política de uso de correos electrónicos

- Los correos electrónicos institucionales será de pertenencia provisional mientras el empleado trabaje en la empresa y será vaciados cada 5 años, lo realizará el Analista de Administración de Plataformas y Servicios Tecnológicos.

5) Política de acceso a Internet

- Se realizará una lista negra de las páginas a las que no se tiene acceso y se actualizará cada mes, y lo realizará el Analista Administrador de Redes y Telecomunicaciones.

6) Política de soporte a usuario

- El soporte a los usuarios internos se realizará cada día dependiendo de las necesidades presentadas, y lo llevará a cabo el Técnico responsable de Soporte a Usuarios.

7) Política de disponibilidad de servicios tecnológicos

- Los servicios tecnológicos que ofrece el departamento serán evaluados cada mes para asegurar su disponibilidad, lo realizará el Analista de Administración de Plataformas y Servicios Tecnológicos

8) Política de mantenimiento de equipos

- Se realizará el mantenimiento de los equipos tecnológicos cada mes, por parte del Técnico de Gestión Técnica y Mantenimiento a Equipos.

1.4 Control de Seguridad

1) Política de control de contraseñas

- Las contraseñas para el acceso a equipos y cuentas institucionales deberán ser cambiadas cada semana, lo realizará Analista Administrador de Seguridad Informática.

2) Política de acceso físico al Departamento de TI

- Se realizará un monitoreo constante de manera diaria en el acceso físico al departamento de TI, por parte de la Secretaría.

3) Política de copias de respaldo de información

- La información debe ser respaldada cada hora en servidores internos para evitar la pérdida de la misma, y lo realizará el Analista Administrador de Servidores y Plataformas.

4) Política para uso de dispositivos extraíbles

- Se revisarán y desinfectarán los dispositivos extraíbles usados dentro del departamento de TI cada día, la desinfección la ejecutará Técnico responsable de Soporte a Usuarios.

5) Política de acceso a la red

- Se deberá actualizar las contraseñas de Wifi y conexiones de internet cada semana para evitar ataques o filtración de información, de lo que se encargará el Analista Administrador de Redes y Telecomunicaciones.

6) Política de seguridad de la información

- La información debe ser protegida y encriptada con programas especiales de manera continua es decir cada día, y lo realizará el Analista Administrador de Seguridad Informática.

7) Política de software antivirus y antimalware

- Se deberán instalar y actualizar el software antivirus y relacionados cada semana en todos los equipos que lo requieran, lo realizará el Técnico responsable de Soporte a Usuarios.

8) Política de actualización de software

- Se deberá realizar revisiones de actualizaciones periódicas cada semana y ejecutarlas en caso de ser necesarias, esto lo llevará a cabo el Técnico responsable de Soporte a Usuarios.

1.5 Control de Personal

1) Política de control de presencia laboral

- Se llevará un control diario de la asistencia al trabajo de cada uno de los empleados, vía registro de asistencia biométrico, del cual se encargará la Secretaría.

2) Política de horas de trabajo y flexibilidad de agenda

- El horario de trabajo será definido antes de comenzar las labores del trabajador y se hará conocer el tipo del mismo y si puede variar en el transcurso de un tiempo, esto lo comunicará el Director de TI.

3) Política de horas extras

- Se establecerán el número de horas extras que puede realizar un trabajador dependiendo la necesidad y previo aviso de un Jefe de Área o Director de TI a los empleados a cargo.

4) Política de día de pago

- Se establecerán los días de pago en el contrato el cual se podrá realizar cada 15 días o en su defecto cada mes, lo definirá la Secretaría.

5) Política de estilo o etiqueta de vestimenta laboral

- Se debe prever que días se debe llevar un tipo de ropa en concreto, estos cambios pueden ser puntuales en días especiales para el departamento de TI o la Institución, lo definirá el Director de TI.

6) Política de seguridad de prendas de valor de empleados

- Se tomarán medidas para prevenir pérdida de prendas personales de los empleados corroborando cada semana la pertenencia de las mismas, lo realizará el encargado de servicios generales.

7) Política de evaluación de desempeño

- Se realizará una evaluación del desempeño de los trabajadores cada 3 meses para valorar y mejorar puntos relevantes con respecto a sus labores, las realizarán los Jefes de Área.

8) Política de ascensos laborales

- Se concederán ascensos de puestos de trabajo a empleado que cumplan con cierto tiempo de labores las que se pueden considerar a partir de un año de servicio, mismos que serán promovidos por el Director de TI.