ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE ACCESO A LOS CENTROS DE DATOS DE LA DIRECCIÓN GENERAL DE REGISTRO CIVIL, IDENTIFICACIÓN Y CEDULACIÓN"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

EDDY ROBERTO ESPINOSA DAQUILEMA

GUAYAQUIL – ECUADOR

AÑO: 2016

AGRADECIMIENTO

A Dios, quien permite que todo esto sea posible.

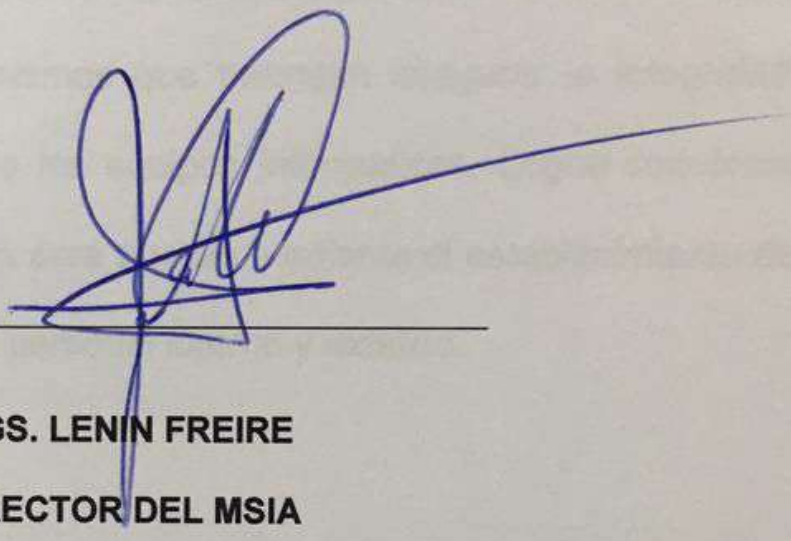
A mis padres, abuelitos, hermana y mi novia quienes son un pilar fundamental en mi vida.

A nuestros profesores, por todos los conocimientos y consejos entregados.

DEDICATORIA

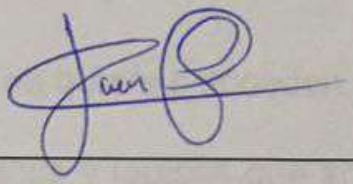
A Dios, a mis padres, a mis familiares y amigos

TRIBUNAL DE SUSTENTACIÓN



MGS. LENIN FREIRE

DIRECTOR DEL MSIA



MGS. JUAN C. GARCÍA

PROFESOR DELEGADO POR LA

UNIDAD ACADEMICA

RESUMEN

El propósito del presente proyecto es implementar Políticas de Acceso Físico a los Centros de Datos, los mismos que permitan asegurar la integridad, confiabilidad y disponibilidad de los equipos informáticos. Lograr mantener segura la plataforma tecnológica será posible mediante el establecimiento de medidas de control aplicables a personal interno y externo.

Con esta propuesta, la Dirección General de Registro Civil, Identificación y Cedulación podrá:

- Optimizar el monitoreo de quienes acceden a los Centros de Cómputo.
- Proteger los activos físicos y lógicos que son administrados dentro de los Centro de Datos.
- Conservar la operación normal del negocio mediante el cuidado de la plataforma tecnológica.
- Cumplir las regulaciones que favorecen y se alinean con la misión y visión de la DIGERCIC.
- Mejorar la productividad del personal de la Coordinación General TIC.

ÍNDICE GENERAL

INTRODUCCIÓN

La Dirección General de Registro Civil, Identificación y Cedulación (DIGERCIC) es la institución pública responsable de custodiar la identidad de todos los ciudadanos del Ecuador. Así mismo ofrece servicios de registro de hechos y actos civiles a través de medios físicos y electrónicos. Se evidencia por lo tanto que, el core de negocio de la DIGERCIC obedece en gran parte a la Gestión de las Tecnologías de la Información y Comunicación.

En este contexto, la Coordinación General TIC, tiene una competencia diferenciada con respecto a las demás áreas operativas y técnicas, ya que es la responsable de velar por el normal funcionamiento de la infraestructura tecnológica y de ésta depende la operación normal diaria.

Todas las empresas hoy en día necesitan implementar políticas, normas y procedimientos que optimicen la gestión del negocio y faciliten la administración de las TIC.

En tal sentido, este proyecto está documentado y estructurado de 3 capítulos que permiten a los funcionarios cumplir procedimientos en base a criterios y normas de Seguridad Informática Aplicada. Al mismo tiempo facilita el

entendimiento para los demás lectores en cuanto a que hacer para mantener un Centro de Cómputo en condiciones favorables.

En el capítulo 1, se expone la descripción del problema que justifica la elaboración de este proyecto, así como también la solución que se propone para solventar los mismos.

Por otra parte en el capítulo 2, se analiza más a detalle, que metodología se utilizó para implementar la solución. En esta sección se abordan temas como las obligaciones, responsabilidades, permisos, registros de bitácora, desarrollo y descripción del proceso mediante un flujo de funciones donde se observa cómo interactúan los stakeholders.

Finalmente se desarrolló el capítulo 3, con el objetivo de argumentar y apoyar la política mediante el análisis de aspectos directamente proporcionales al acceso al Centro de Datos. Estos puntos son el mantenimiento de equipos, perdida de activos, la seguridad ambiental, operación en el centro de datos, cumplimiento y modificación de la política y seguridad ambiental.

CAPÍTULO 1

GENERALIDADES.

1.1. Descripción del problema

La DIGERCIC, al ser una entidad gubernamental con una competencia de servicio que depende de la tecnología y al tener como insumo de operación, la información de cada ciudadano; se vuelve indispensable disponer de los recursos necesarios para que sea capaz de dar una atención eficiente y oportuna a la ciudadanía y demás instituciones públicas y privadas que de ella dependen.

Por este motivo es importante determinar de qué obedece su operatividad, y es que, la DIGERCIC cuenta con 2 Centros de Cómputo con una

infraestructura tecnológica de gran costo y alto valor de impacto por la información crítica que administra.

Por lo que, nos vemos en la necesidad de implementar políticas de Seguridad de Acceso para los Centros de Datos de Quito y Guayaquil y así salvaguardar la integridad de los mismos.

En la actualidad no se cuenta con estos controles, lo que implica en riesgos y amenazas que comprometen los equipos de computación y a la vez la información que en estos residen.

Dada la importancia de la implementación de las Políticas de Acceso, a continuación se detallan los problemas principales que se encontraron:

- Acceso físico inapropiado.- El no tener un control adecuado del personal que ingresa y sale de los DC, incide en un riesgo que atenta contra la seguridad de la infraestructura tecnológica.
- Robo de Información.- Los DC cuentan con equipos de procesamiento de datos con información sensible, cuando una persona con conocimientos básicos de informática vulnera físicamente el acceso, es muy probable que también vulnere la seguridad lógica de los mismos.
- Robo de activos.- Ocurre muchas veces, que algunos de los equipos de computación suelen ser pequeños e imperceptibles y tratar de hurtar o tomar un dispositivo sin autorización con fines mal intencionados se vuelve sencillo. Por lo tanto es necesario tener el control de todos los activos y cuidar de ellos.

- Disponibilidad.- De tener un evento no controlado que ponga en riesgo el normal funcionamiento de los sistemas de información; nos veríamos inmersos probablemente en problemas complejos de solventar. Estos incidentes pueden incurrir en elevados costos de reparación y en muchos casos se deberá asumir inclusive, la pérdida total de los recursos lógicos y/o físicos.

1.2. Solución propuesta.

Con respecto a lo antes mencionado, para solventar estos problemas se genera la necesidad de crear Políticas de Acceso a los Centros de Datos.

Con el propósito de un mejor entendimiento de estas reglas, se ha dividido su análisis en 5 puntos que se detallan posteriormente y son:

- Responsabilidades de quienes ingresan o pueden hacerlo.
- Obligaciones para todo personal.
- Permisos de acceso:
    - Acceso Permanente
    - Acceso Temporal
- Desarrollo y descripción del flujo de funciones acerca de cómo se debería proceder.
- Registros en bitácora

CAPÍTULO 2

METODOLOGÍA DEL DESARROLLO DE LA SOLUCIÓN

2.1. Implementación de Responsabilidades

Es compromiso de todos los funcionarios de la Coordinación General TIC y terceros, cumplir con las Políticas de Acceso a los Centros de Datos.

En tal sentido se requiere definir las responsabilidades de los stakeholders que pueden, deben o podrían interactuar:

- ***Director de Infraestructura y Operaciones***.- Conceder y revocar los accesos físicos permanentes o temporales al DC. Responsable de coordinar e informar las actividades o cualquier eventualidad que pueda ocurrir en el DC.

- ***Analistas de Infraestructura y Operaciones***.- Monitorear las actividades de usuarios autorizados, no autorizados y visitantes durante el periodo que permanezcan en el DC. Responsable de registrar en la bitácora de registros, tanto los ingresos como salidas y demás actividades.

  Custodiar, revisar e informar en conjunto las actividades o cualquier eventualidad que ocurra en el DC.

- ***Visitantes internos o externos***.- Las responsabilidades que los visitantes deben cumplir están descritas en el punto de Implementación de Obligaciones.

2.2. Implementación de Obligaciones

Esta sección tiene como objetivo describir todas y cada una de las obligaciones que se deben cumplir por parte de todo el personal que accede al Centro de Datos.

Es válido indicar que estas obligaciones están sujetas a cambios o mejoras siempre que se cuente con la aprobación del Comité de la Coordinación General TIC.

1. Los DC deben contar con acceso a través de sistema biométrico, huella digital o mano (Ver Figura 2.1).

Figura 2.1
Acceso a Centro de Datos a través de huella digital y tarjeta magnética
Fuente: Eddy Espinosa

2. Se debe anotar en la bitácora de registros todas las visitas realizadas con sus respectivas firmas de constancia.
3. Las cámaras deben colocarse en cada uno de los pasillos que tengan racks, con el objeto de que puedan ser monitoreadas constantemente.
4. Se deberá contar con cámaras al exterior del DC.
5. Las cámaras deberán grabar las 24 horas del día, los 365 días del año [1] (Ver Figura 2.2).

Figura 2.2
Sistema de cámara dentro del Centro de Datos
Fuente: Eddy Espinosa

6. No podrán almacenar ningún objeto de tipo inflamable o peligroso (cartón, cajas, papel, etc.) dentro del DC.
7. Se prohíbe el ingreso de cámaras fotográficas o de video, celulares, dispositivos de almacenamiento, pendrives, CD, armas, explosivos, químicos, drogas, alcohol, tabaco, materiales radioactivos, comidas, bebidas o cualquier otro artículo o material que la DIGERCIC lo considere.
8. No podrán ingresar al DC con vestimenta inapropiada (pantalones cortos, camisetas sin mangas, zapatillas).
9. Se deberá tener limpio y ordenado el DC [2].

10. No se podrán tomar fotos ni videos del área.
11. No se podrán instalar ni conectar ninguna clase de equipos inalámbricos.
12. Los Centros de Operación de Red (NOC) en el DC, deberán tener acceso restringido mediante huella digital o tarjeta de acceso.

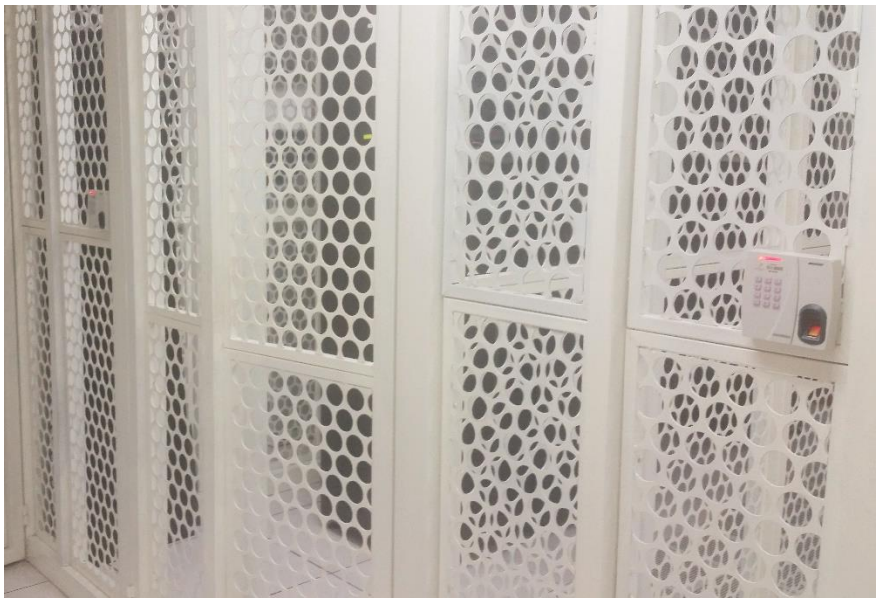


Figura 2.3
División de NOC mediante huella digital o tarjeta de acceso dentro del Centro de Datos
Fuente: Eddy Espinosa

13. Sólo bajo vigilancia de personal autorizado, puede el visitante acceder al DC.
14. Se deberá cumplir la fecha y hora de salida de acuerdo a los tiempos establecidos de permiso.
15. Al finalizar cualquier trabajo, el funcionario encargado de DIGERCIC, debe validar al final de la visita que no existan problemas, ni alarmas de ninguna índole.

16. No está permitido levantar las baldosas del piso falso. Esta labor debe ser realizada por personal autorizado de la DIGERCIC.
17. Se prohíbe mover o reubicar los equipos.
18. Se prohíbe retirar sellos de los equipos, en caso de requerir realizarlo se deberá coordinar con Jefe de Desarrollo Organizacional y funcionario técnico de la Dirección de Infraestructura y Operaciones [3].
19. Se prohíbe colocar objetos encima de los equipos o cubrir los orificios de ventilación de los equipos de computación.
20. En caso de mantenimientos emergentes, el ingreso de algún dispositivo o equipo externo al DC deberá ser únicamente por personal de Infraestructura y Operaciones.
21. El permiso para el ingreso de algún equipo externo al DC, deberá ser justificado previamente con la autorización del Director de Infraestructura y Operaciones.
22. Las puertas de los Centros de Datos deben permanecer cerradas al menos que se estén realizando trabajos.

2.3. Permisos de Acceso

Los permisos para el ingreso al DC se han clasificado como permanentes o temporales, en este sentido, se debe seguir las siguientes consideraciones:

- Se otorga ***permiso permanente*** al personal de la Dirección de Infraestructura y Operaciones responsable de mantener operativa todas las funciones del negocio.

La entrada para estos funcionarios será las 24 horas del día, los 7 días de la semana, los 365 días del año; esto debe ser comunicado y oficializado oportunamente por el Director de Infraestructura y Operaciones vigente.

- Serán los permisos temporales a aquellos terceros (funcionarios interno de la Coordinación TIC u otras áreas de la DIGERCIC), contratistas, proveedores de servicios externos y demás personal externo que no tenga sustentado su ingreso permanente a DC.

  Todo tercero deberá ser acompañado desde el inicio al fin de la visita por funcionario autorizado de la Dirección de Infraestructura y Operaciones.

Cada ingreso deberá ser registrado en la bitácora de registros y será de conocimiento del Director de Infraestructura y Operaciones los motivos que ameritan la visita.

2.4. Implementación de Desarrollo y Descripción del Proceso

A continuación vamos a describir como se ha pensado el proceso de acceso físico a los Centros de Datos [4]: (Ver Figura 2.5)

1. La persona/entidad que requiera realizar la solicitud de acceso al Centro de Datos (Guayaquil o Quito), lo debe hacer mediante correo electrónico a la cuenta soportic@registrocivil.gob.ec.

   El asunto del correo debe ser claro y conciso por Ej.: “Solicitud de Visita al Centro de Datos GYE”

Deberá estar dirigido con copia al Director de Infraestructura y Operaciones y el cuerpo del email debe detallar lo siguiente: (Ver Figura 2.4).

Solicitud de Visita al Centro de Datos GYE

Borrador guardado 04:38

Estimados Sres. Registro Civil,
Mediante la presente solicito su gentil ayuda otorgando los permisos necesarios para el ingreso de 2 Ingenieros a su Centro de Datos ubicado en la ciudad de Guayaquil con el fin de evaluar un problema de conexión en el router que pertenece a MINTEL. Y que actualmente se tiene en su rack de comunicaciones.

MOTIVO DE LA VISITA:
Se requiere realizar la visita al Centro de Datos ubicado en la ciudad de Guayaquil, agencia Matriz, con el objetivo de verificar el enlace punto a punto que actualmente tenemos en sus instalaciones, ya que el mismo presenta intermitencias.

ACTIVIDADES:
1. Se realizarán pruebas en el router de MINTEL, con serie GSKJ283782.
2. De validar que se tienen problemas, se reemplazará el mismo por uno nuevo. En este punto se requiere la autorización para el ingreso del router CISCO 1800 con serie PO9298HAG.

PERSONAL:
- CC.: 0923548750 - JUAN CARLOS BASURTO PIGUAVE - TELCONET - ANALISTA DE SOPORTE TÉCNICO CORPORATIVO
- CC.: 1745654440 - JORGE LUIS SOLANO VIZUETA - TELCONET - ANALISTA DE SOPORTE TÉCNICO CORPORATIVO

TIEMPO:
Ingreso: 2016-02-18 20:00
Salida: 2016-02-18 22:30

Ing. David Vizueta Montesdeoca
Coordinador Zonal 1
Av. 9 de Octubre #505 y Pichincha esq.
(02) 2592-470 ext. 10333
www.mintel.gob.ec
Quito - Ecuador

Figura 2.4
Ejemplo de Correo Electrónico para solicitud de Acceso a Centro de Datos
Fuente: Eddy Espinosa

- **Motivo de Visita** - ¿Cuál es el objetivo de la visita? ¿Qué logrará con la visita?
- **Actividades** - ¿Cuáles son los procedimientos, observaciones, revisiones y demás actividades que realizará una vez que acceda al DC?
- **Personal** - ¿Cuáles son los funcionarios, personas naturales o externos que requieren realizar la visita?
    - Cédula
    - Nombres completos
    - Institución en la que trabaja

        - Cargo
    - **Tiempo (Fecha y Hora)** de Ingreso
    - **Tiempo (Fecha y Hora)** de Salida

2. El Director de Infraestructura y Operaciones deberá aprobar o negar la solicitud.
    a. En caso de que sea aprobada la misma, se debe señalar disponibilidad de la fecha y hora indicada, caso contrario debe coordinar nueva fecha y hora.

       Además designará funcionario que acompañará la visita.
    b. En caso de que la solicitud no sea aprobada, se deberá indicar los motivos por la cual no fue aprobada la visita.

3. El funcionario de la Dirección de Infraestructura y Operaciones delegado deberá registrar y programar la visita en la bitácora de registros.

4. Al momento de la visita:
    a. ***Personal interno:*** El funcionario técnico delegado de DIGERCIC deberá registrar ingreso y solicitar firma en la bitácora de registros.
    b. ***Personal externo:*** Se debe registrar ingreso en la bitácora del guardia de seguridad y realizar los respectivos chequeos para evitar el ingreso de objetos no permitidos (detallado en Implementación de Obligaciones), al menos que se justifique con

las respectivas comprobaciones (debe ser validado por el funcionario técnico delegado).

5. Se realizan las actividades propias del trabajo dentro del DC.
6. Una vez que concluya la visita, el funcionario delegado debe revisar el estado del DC indicando si existen problemas o no.
    a. ***De existir problemas***: Se notifica al Director de Infraestructura y Operaciones y se activa el procedimiento de Gestión de Incidentes.
    b. ***De no existir problemas****:*
        i. Se registra la salida y se solicita firma en la bitácora de registros para personal interno.
        ii. Se registra la salida en la bitácora del guardia de seguridad.

2.5. Implementación de Registros

Se ha diseñado para este objetivo un modelo de bitácora de registros a través de un formulario, el cual deberá ser llenado al ingresar o salir de los Centros de Datos de la DIGERCIC (Ver Tabla 1).

El mismo debe estar legible y sin adulteraciones. El aseo del mismo deberá ser de responsabilidad del custodio del Centro de Datos o del funcionario delegado por el Director.

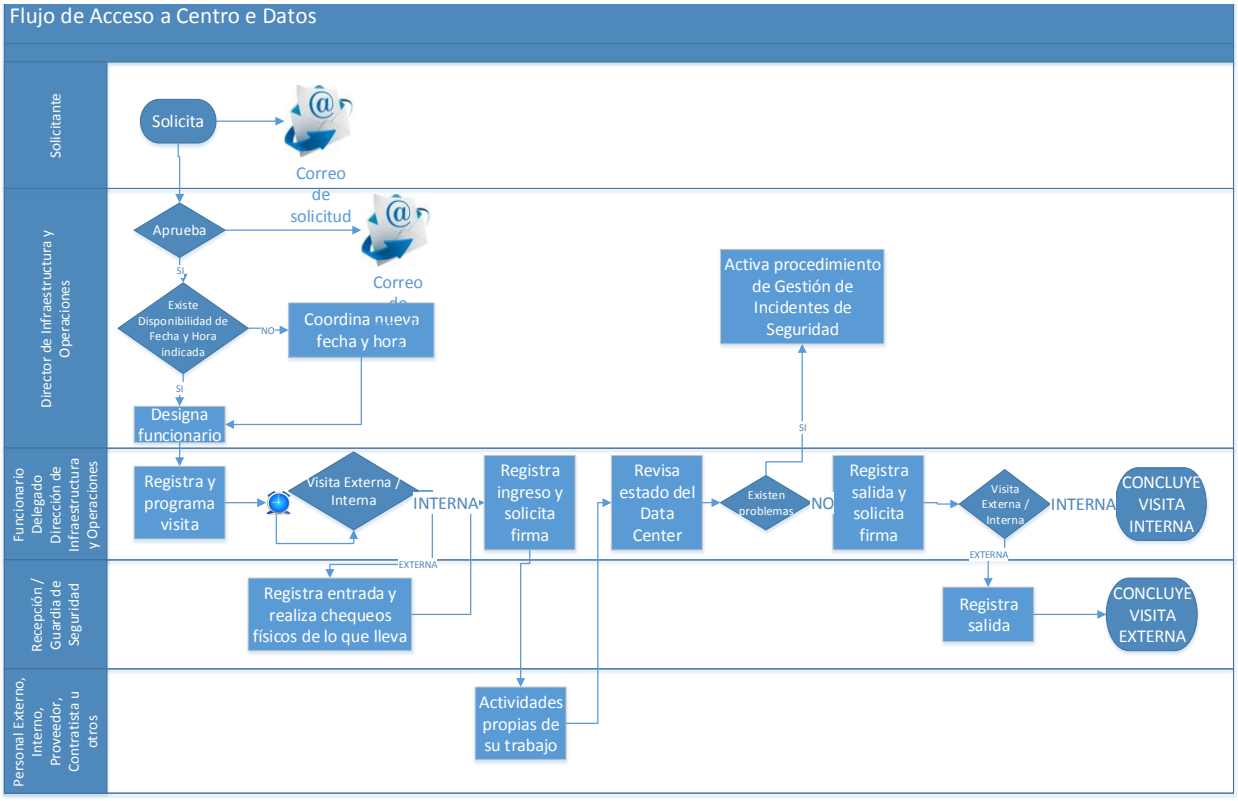


Figura 2.5
Diagrama de Flujo de Funciones para Acceso a Centro de Datos
Fuente: Eddy Espinosa

1. No se deben eliminar ni romper ninguna hoja, sino por el contrario deben ser escaneadas y deben alimentar la base de conocimientos (Ver Figura 2.8).

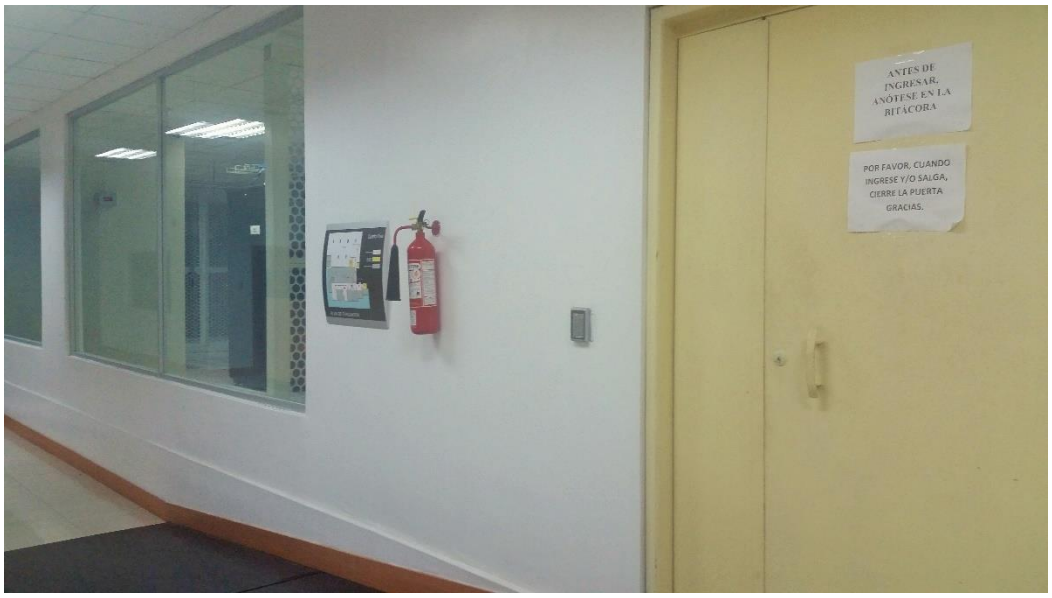


Figura 2.8
Entrada a Centro de Datos, indicando Registrarse en la Bitácora previamente
Fuente: Eddy Espinosa

Bitácora de Registros de Ingreso y Salida al Centro de Datos

REGISTRO DE INGRESO/SALIDA AL DATA CENTER DE LA DIGERCIC GUAYAS

NOMBRE	CÉDULA/ PASAPORTE	INSTITUCIÓN (CARGO)	MOTIVO DE INGRESO	INGRESO		SALIDA		OBSERVACIONES	FIRMA
				Fecha	Hora	Fecha	Hora		

OBLIGACIONES DEL VISITANTE

No podrá ingresar	No podrá introducir ninguno de los siguientes materiales	Otras obligaciones
• Bajo los efectos de alcohol/droga • Portando armas de fuego, cuchillos o similares • Con vestimenta inapropiada (pantalones cortos, camisetas sin mangas, zapatillas) • Fumando	• Productos derivados del Tabaco • Explosivos, elementos inflamables o corrosivos • Armas • Químicos • Drogas ilegales / alcohol • Artículos electromagnéticos • Materiales radioactivos • Cámaras fotográficas o de video, celulares • Se encuentra prohibido tomar fotografías dentro del Centro de Computo	• Al finalizar cualquier trabajo en el Data Center, deberá asegurarse que los cables estén bien instalados y ordenados, dentro de sus gabinetes, así como asegurarse que todas las puertas están cerradas. • Remover desechos y cajas vacías antes de salir • No se permiten comidas ni bebidas dentro del Data Center • No se permite el uso de aspiradoras, taladros o similares en el área de la sala de equipos (piso falso) • No podrá instalar equipos inalámbricos o antenas en las dependencias del Centro de Computo

Nota: **Cualquier excepción por motivo del trabajo a realizar deben ser informadas y fundamentadas previamente a la Dirección de Infraestructura y Operaciones**

Tabla 1

CAPÍTULO 3

CONSIDERACIONES ADICIONALES

3.1. Mantenimiento de Equipos

1. Únicamente personal autorizado por la Dirección de Infraestructura y Operaciones será la responsable de llevar a cabo servicios de mantenimiento de los equipos del DC.

2. Los funcionarios delegados de la DIGERCIC serán responsables de tener los respaldos probados con el fin de precautelar perdida de información en caso de una falla en el mantenimiento.

3.2. Pérdida de Equipos

1. Los inventarios de los equipos son de responsabilidad del área de Desarrollo Organizacional. Esta área debe contar con las actas firmadas como constancia que el funcionario tiene conocimiento de responsabilidad hacia ese equipo. [5]

2. El funcionario que tenga bajo su responsabilidad algún activo del DC será responsable de su uso y custodia, por lo cual debe responder por ese bien en caso de extravío o robo.

3. En caso de conocer de la pérdida de algún equipo debe notificar inmediatamente a Dirección de Infraestructura y Operaciones y al Departamento de Desarrollo Organizacional.

4. Todos los funcionarios deberán devolver los activos que se encuentren en su poder una vez que dejen de prestar sus servicios en la institución.

3.3. Operación en el Centro de Datos

1. Todo equipo ingresado al DC deberá ser registrado en la bitácora de visitas, así también deberá ser anotado en los inventarios de equipos llevados por Departamento de Desarrollo Organizacional.

2. El robo o pérdida de las tarjetas magnéticas deben ser notificadas.

3. Cuando se deje de usar una tarjeta magnética de ingreso, ésta debe ser devuelta al funcionario técnico delegado de la Coordinación TIC.

4. No pueden asignarse las tarjetas a otras personas mientras no haya pasado el proceso de re enrolamiento.

3.4. Modificación y Cumplimiento de la Política

1. La Dirección de Infraestructura y Operaciones tiene la obligación de revisar la política regularmente, con el objeto de certificar que se cumpla correctamente.

2. Acciones que violen la política deben ser detectadas y analizadas por el comité de Seguridad Informática establecido por el Coordinador General TIC y las áreas pertinentes para su análisis y solución inmediata.

3. En caso de requerir aplicar un cambio en la política, esta deberá ser aprobada por el Director Infraestructura y Operaciones y/o Coordinador General de TIC.

4. Los cambios aprobados en la política deben ser notificados mediante correo electrónico a todo el personal de TIC y autoridades de la Institución, así como al personal externo que amerite conocer.

3.5. Control de Ambiente

1. En el Centro de Cómputo deberán existir sistemas de detección y extinción automática de incendios e inundación y alarmas en caso de detectarse condiciones inapropiadas.

2. Los niveles de temperatura y humedad en el Centro de Cómputo deben ser mantenidos dentro del rango dependiendo la infraestructura que mantenga Ej.: 21 – 23 ºC.

3. Verificar constantemente con personal de especialidad eléctrica, el sistema de UPS y planta eléctrica. [6]

4. Verificar regularmente con personal de mantenimiento el sistema de detección y extinción de incendios y sistema de data aires.

CONCLUSIONES Y RECOMENDACIONES.

CONCLUSIONES

1. Toda organización requiere mejorar continuamente y esto más en los centros de cómputo, con la implementación de políticas, de tal forma que se dé la posibilidad de una posible certificación a mediano plazo.
2. Con la aplicación adecuada de la política se garantiza un DC ordenado, limpio y seguro.
3. Todo personal debe cumplir rigurosamente cada una de las obligaciones y responsabilidades descritas en la presente política.
4. Toda visita y demás actividades en los DC deben obligatoriamente quedar registradas en la bitácora de ingreso/salida.

5. Cuando se evidencia un evento no controlado en el DC se levantará el registro de incidencia al Director de Infraestructura y Operaciones y demás personal que deba saber del mismo.
6. Las solicitudes de acceso tendrán que estar registradas electrónicamente mediante email, la misma que debe ser gestionada a través de la herramienta de soporte técnico OTRS (soportic).

RECOMENDACIONES

1. Personal de seguridad que realiza el chequeo físico deberá estar capacitado para identificar objetos o materiales que no son permitidos para ingresar al DC.
2. Verificar constantemente las grabaciones de las cámaras, las mismas que serán las 24 horas del día, los 7 días de la semana, los 365 días del año y deben estar disponibles en todo momento.
3. Mantener impecable las hojas de bitácora de registros, sin correctores ni adulteraciones.
4. En caso de tener algún evento no controlado validarlo con el Director de Infraestructura y Operaciones.
5. Evaluar y monitorear constantemente la ejecución y cumplimiento de la Política.
6. Validar que la política sea de utilidad y en caso de requerir algún cambio, ponerlo en consideración de las autoridades de la Coordinación General TIC para que sea analizada.

BIBLIOGRAFÍA

[1] CLAVES DE SEGURIDAD FÍSICA EN EL DATA CENTER , [En línea]. Available: http://www.datacenterdynamics.es/focus/archive/2012/10/claves-de-seguridad-f%C3%ADsica-en-el-data-center-ii. [Último acceso: febrero 2016].

[2] TRICOM, Política de Uso del Data Center, [En línea]. Available: http://www.tricom.net/media/doc/Pol%C3%ADticadeUsodelDataCenter.pdf. [Último acceso: diciembre 2015].

[3] Poder Judicional de Sinaloa, Manual de Políticas y Estándares de Seguridad Informática para Usuarios, [En línea]. Available: http://www.stj-sin.gob.mx/files/leyes/ManualProcedimientos.pdf. [Último acceso: octubre 2015].

[4] MIN. SALUD CHILE, Control de Acceso Fisico Data Center, [En línea]. Available: http://web.minsal.cl/sites/default/files/files/2013%20Procedimiento%20control%20acceso%20Data%20Center.pdf. [Último acceso: octubre 2014].

[5] Universidad Virtual Internacional, Incorporación de TIC en Procesos Educativos, [En línea]. Available: https://www.uvirtual.edu.co/Documents/Documentos-Institucionales/POLITICA-SEGURIDAD.pdf. [Último acceso: noviembre 2015].

[6] Políticas de Uso de Servicios de Red y Servicios Informáticos del Ministerio de Salud Pública, [En línea]. Available: http://www.salud.gob.ec/direccion-nacional-de-tecnologias-de-la-informacion-y-comunicaciones/. [Último acceso: enero 2016].

GLOSARIO

DIGERCIC	Dirección General de Registro Civil, Identificación y Cedulación.
TIC	Tecnologías de la Información y las Comunicaciones.
DC	Centro de Datos o Centro de Computo
Centro de Computo	Es un área física o departamento en el que se alojan equipos informáticos (red, servidores, bases de datos, entre otros), los mismos que permiten el procesamiento y almacenamiento de información de manera automatizada.
Acceso	Privilegio de una persona para utilizar un recurso, objeto o infraestructura.
Acceso Lógico	Habilidad para conectarse o comunicarse con un dispositivo tecnológico para su uso.
Confidencialidad	Obligación de los funcionarios y demás personal a no divulgar información restringida.
Control de Acceso	Mecanismo de seguridad para prevenir, cuidar y detectar acceso no autorizado, o en su defecto permitir el acceso.
Disponibilidad	Información o recurso disponible en cualquier momento.
Integridad	Mantener los sistemas de información libres de modificaciones, a menos que exista autorización
Incidente de seguridad	Evento que incurra en un riesgo para la confidencialidad, integridad o disponibilidad de la información.
NOC	Centro de Operación de Red