

[Control de Acceso]

Eva Sofía García Reséndiz | 1581568

Laura Viridiana Suarez Rodríguez | 1694063

David Alejandro Herrera Pozos | 1552618

Diego Alejandro Elizondo Carrillo | 1600296

Contenido

[1. POLITICA DE CONTROL DE ACCESO 2](#_Toc450610673)

[1.1 Introducción 2](#_Toc450610674)

[1.2 Objetivo (#General) 2](#_Toc450610675)

[1.3 Alcance (#General) 2](#_Toc450610676)

[2. CONTROL DE ACCESO LÓGICO 2](#_Toc450610677)

[2.1 Objetivo 2](#_Toc450610678)

[2.2 Alcance 2](#_Toc450610679)

[2.3 Contenido 2](#_Toc450610680)

[Políticas Generales 2](#_Toc450610681)

[2.3.1 Requerimientos del control de acceso 2](#_Toc450610682)

[2.3.2 Gestión de acceso a usuarios 3](#_Toc450610683)

[2.3.3 Gestión de Privilegios #NoSeSiSeaLoMismoQueElAnterior 3](#_Toc450610684)

[2.3.4 Administración y uso de contraseñas 3](#_Toc450610685)

[2.3.5 Control de Acceso a Redes 3](#_Toc450610686)

[2.3.6 Gestión de Acceso a sistemas operativos 3](#_Toc450610687)

[2.3.7 Gestión de Acceso a las Aplicaciones de la compañía 4](#_Toc450610688)

[2.3.8 Equipos desatendidos #**YALAHABIAMOSPUESTOBIEN** 4](#_Toc450610689)

[2.3.9 Gestión de acceso Remoto 4](#_Toc450610690)

[3. Control de Acceso Físico 4](#_Toc450610691)

[3.1 Objetivo 4](#_Toc450610692)

[3.2 Alcance 4](#_Toc450610693)

[3.3 Contenido 5](#_Toc450610694)

[3.3.1 Acceso a las oficinas 5](#_Toc450610695)

[3.3.1.1 Perímetros 5](#_Toc450610696)

[3.3.2 Áreas restringidas 5](#_Toc450610697)

[3.3.2.1 Niveles de acceso 5](#_Toc450610698)

[4. Glosario 5](#_Toc450610699)

[3.4 Objetivo del glosario 5](#_Toc450610700)

[1.1.2 Glosario 5](#_Toc450610701)

[5. Procedimientos 7](#_Toc450610702)

[5.1 Acceso a la Red (#ActiveDirectory) 7](#_Toc450610703)

[5.2 Asignación de contraseñas por defecto 7](#_Toc450610704)

[6. Anexos 8](#_Toc450610705)

[1.2.1 Gestión de Privilegios 9](#_Toc450610706)

[Política 9](#_Toc450610707)

[1.2.2 Gestión de contraseñas 9](#_Toc450610708)

[1.2.2.1 Contraseñas seguras 9](#_Toc450610709)

[Política 9](#_Toc450610710)

[**Procedimiento: #**ESTO PUEDE IR EN UN CAPITULO DE PROCEDIMIENTOS 10](#_Toc450610711)

[Repercusiones 11](#_Toc450610712)

[1.5 Responsabilidades del usuario #Esto va en responsabilidades lelelel 11](#_Toc450610713)

[1.5.1 Uso de Contraseña: 11](#_Toc450610714)

[Política 11](#_Toc450610715)

[1.5.3 Políticas para escritorios y monitores limpios 12](#_Toc450610716)

[1.6 Gestión de Acceso a la Red 12](#_Toc450610717)

[Objetivo 12](#_Toc450610718)

[Alcance 12](#_Toc450610719)

[1.6.1 Acceso a internet 12](#_Toc450610720)

[Política 12](#_Toc450610721)

[1.7 Acceso A las aplicaciones de la empresa 13](#_Toc450610722)

[Objetivo 13](#_Toc450610723)

[Alcance 13](#_Toc450610724)

[Política 13](#_Toc450610725)

[1.8 Seguridad física y medio ambiente 14](#_Toc450610726)

[1.8.1 Controles de acceso físico 14](#_Toc450610727)

[1.8.2 Acceso áreas restringidas 15](#_Toc450610728)

1. POLITICA DE CONTROL DE ACCESO
   1. Introducción

El control de acceso conlleva mecanismos utilizados para limitar el acceso a la información y recursos de procesamiento de datos sólo a los usuarios o aplicaciones autorizadas, así como las tareas que pueden realizar los mismos.

Nuestra política de Control de Acceso tiene como referencia el estándar ISO 27001, que hace hincapié a la definición e implementación de un Sistema de Gestión de Seguridad de la Información en las entidades organizacionales.

Indudablemente, es importante ligar la política de control de acceso con un SGSI, ya que éste contemplará finitamente una pauta para mantener y crear los controles requeridos, entre estos, los controles de acceso; conforme a los riesgos y amenazas habidos y por haber.

* 1. Objetivo (#General)

#TEXTO#TEXTO

* 1. Alcance (#General)

#TEXTO#TEXTO

1. CONTROL DE ACCESO LÓGICO
   1. Objetivo

#TEXTO#TEXTO

* 1. Alcance

#TEXTO#TEXTO

* 1. Contenido

Políticas Generales

* + 1. Requerimientos del control de acceso
       1. Cada dispositivo que se desee conectar debe ser inspeccionado y aprobado por el departamento de TI.
       2. El departamento de TI se encargará de proveer un nombre de usuario y una contraseña que le dará acceso una vez aceptado; estas credenciales son únicas para cada usuario y no serán compartidas.

## Gestión de acceso a usuarios

* + - 1. Cada dispositivo que se desee conectar debe ser inspeccionado y aprobado por el departamento de TI.
      2. El departamento de TI se encargará de proveer un nombre de usuario y una contraseña que le dará acceso una vez aceptado; estas credenciales son únicas para cada usuario y no serán compartidas.
    1. Gestión de Privilegios #NoSeSiSeaLoMismoQueElAnterior
       1. Cada dispositivo que se desee conectar debe ser inspeccionado y aprobado por el departamento de TI.
       2. El departamento de TI se encargará de proveer un nombre de usuario y una contraseña que le dará acceso una vez aceptado; estas credenciales son únicas para cada usuario y no serán compartidas.
    2. Administración y uso de contraseñas
       1. Cada dispositivo que se desee conectar debe ser inspeccionado y aprobado por el departamento de TI.
       2. El departamento de TI se encargará de proveer un nombre de usuario y una contraseña que le dará acceso una vez aceptado; estas credenciales son únicas para cada usuario y no serán compartidas.
    3. Control de Acceso a Redes
       1. Cada dispositivo que se desee conectar debe ser inspeccionado y aprobado por el departamento de TI.
       2. El departamento de TI se encargará de proveer un nombre de usuario y una contraseña que le dará acceso una vez aceptado; estas credenciales son únicas para cada usuario y no serán compartidas.
    4. Gestión de Acceso a sistemas operativos
       1. Cada dispositivo que se desee conectar debe ser inspeccionado y aprobado por el departamento de TI.
       2. El departamento de TI se encargará de proveer un nombre de usuario y una contraseña que le dará acceso una vez aceptado; estas credenciales son únicas para cada usuario y no serán compartidas.
    5. Gestión de Acceso a las Aplicaciones de la compañía
       1. Cada dispositivo que se desee conectar debe ser inspeccionado y aprobado por el departamento de TI.
       2. El departamento de TI se encargará de proveer un nombre de usuario y una contraseña que le dará acceso una vez aceptado; estas credenciales son únicas para cada usuario y no serán compartidas.
    6. Equipos desatendidos #**YALAHABIAMOSPUESTOBIEN**
       1. Los usuarios deberán mantener sus equipos de cómputo con controles como contraseñas y protectores de pantalla previamente instalados y autorizados por el Departamento de TI cuando no se encuentren en su lugar de trabajo.
       2. Los usuarios deben concluir sus sesiones activas al finalizar las tareas.
       3. El Responsable de Seguridad Informática debe coordinar junto con el departamento de Recursos Humanos las tareas de concientización a todos los usuarios, acerca de los requerimientos y procedimientos de seguridad para la protección de equipos desatendidos.
    7. Gestión de acceso Remoto
       1. Cada dispositivo que se desee conectar debe ser inspeccionado y aprobado por el departamento de TI.
       2. El departamento de TI se encargará de proveer un nombre de usuario y una contraseña que le dará acceso una vez aceptado; estas credenciales son únicas para cada usuario y no serán compartidas.

1. Control de Acceso Físico
   1. Objetivo

#TEXTO#TEXTO

* 1. Alcance

#TEXTO#TEXTO

* 1. Contenido
     1. Acceso a las oficinas
        1. Perímetros
     2. Áreas restringidas
        1. Niveles de acceso

1. Responsabilidades
   1. Responsable de Seguridad Informática
      1. Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.
      2. Asegurar que las medidas de seguridad se cumplan.
      3. Asegurarse que todos los usuarios tengan conocimientos de las políticas de control de acceso establecidas.

* 1. Departamento de TI
     1. Realizar evaluaciones y preparar planes para la seguridad de los sistemas de información.
     2. Establecer procedimientos para el debido cumplimiento de la política.
     3. Establecer privilegios apropiados para usuarios, monitoreando las bitácoras de control de acceso.
     4. Reportar cualquier actividad sospechosa al Responsable de Seguridad informática, así como implementar los requerimientos de las políticas establecidas en el presente documento.
  2. Propietarios de la Información
     1. Tiene autoridad para adquirir, crear y mantener información y los sistemas que la manejan y que se ubican en su área de control.
     2. Autorizar el acceso a la información a los usuarios, basados en las funciones y necesidades laborales.
     3. Establecer y actualizar políticas específicas acerca de las categorías de usuarios que tendrán acceso a la información. Esas políticas deben especificar limitaciones sobre el uso de esa información hacia quienes tienen acceso a ella.
     4. Tomar decisiones acerca de los usos permitidos de la información incluyendo reglas laborales importantes.
     5. Deben definir las reglas de validación usadas para verificar la aceptabilidad y veracidad de los datos de ingreso. Estas reglas de validación y otros controles para protección de la información deben aprobarse formalmente por escrito por el Propietarios antes de que se realicen modificaciones considerables a los sistemas.
     6. Son responsables de las consecuencias asociadas con la revelación inapropiada, mantenimiento insuficiente, etiquetado y clasificación inadecuados, y otras deficiencias en los controles de seguridad relativos a la información por la cual fueron designados Propietarios.
  3. Custodios de la Información
     1. Los Custodios son individuos, en posesión física o lógica de la información de los Propietarios.
     2. Proteger, por medio del uso de sistemas de control de acceso físico y lógico la información en su posesión de la distribución no autorizada, acceso, alteración, destrucción o uso.
     3. Proveer y administrar controles generales como sistemas de recuperación y respaldo, así como el establecimiento, monitoreo, y operación de los sistemas de información, todo esto de manera acorde con las políticas y estándares.

* 1. Usuarios
     1. Cumplir con las políticas establecidas en este documento.
     2. Reportar al Responsable de Seguridad Informática de toda violación o vulnerabilidad que observen.
     3. Los Usuarios son individuos a quienes se les ha brindado autorización por parte del Propietario para acceder, modificar, borrar o usar información. Los Usuarios deben utilizar la información solo para los propósitos específicamente aprobados por el Propietario.
     4. Cumplir con todas las medidas de seguridad definidas por el Propietario, implementadas por el Custodio.

1. Glosario
   1. Objetivo

Un glosario de términos relacionados con la Seguridad de la Información, garantiza la unificación de criterios y significados, y permite que se apliquen consistentemente en todas las áreas de lo Organización. Si existe algún término en la política de seguridad que necesita ser aclarado, por favor contáctese con el departamento de Seguridad.

* 1. Glosario

1. Acceso remoto

Conectarse a los recursos informáticos de red desde una ubicación externa a través de una red pública.

b) Activo

Todo aquello que tiene valor para la Organización.

c) Administrador de la información

Un Administrador de la información es una persona a la que los responsables de la información le delegaron obligaciones sobre el manejo  
de la misma.

d) Asociado de Negocio

Socio de D-dev en el negocio.

e) Autenticación

Un proceso por el cual un sistema informático confirma la identidad de usuario, equipos o sistemas, usualmente por medio de la validación de una cuenta y el esquema de verificación de contraseñas.

f) Autorización

Permisos asociados con la identidad de un usuario.

g) Cifrado

Aplicación de un algoritmo específico a los datos a fin de alterar su apariencia y volverlos incomprensibles, para que sólo puedan ser accedidos por el destinatario.

h) Confidencialidad

Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

i) Datos

Cualquier información, sin importar la forma, contenida o procesada por el equipamiento de sistemas de información, redes de comunicaciones, o medios de almacenamiento. Estos datos pueden presentarse en diferentes medios incluyendo: copias impresas, medios magnéticos, fichas, almacenamientos en línea, materiales físicos, etc.

j) Disponibilidad

La característica de los datos, información, y sistemas de información a ser accesibles y utilizables en el momento y formas requeridos.

k) Funcionario

Es todo el personal de D-dev.

l) Integridad

La característica de los datos y la información de ser correctos y completos; y la preservación de la corrección y completitud de los mismos a través de la certeza que el ingreso, modificación o eliminación de los datos es realizado solamente por personal autorizado.

m) Necesidad de conocer

Hace referencia a la necesidad que tiene un usuario, de conocer la información necesaria para el desempeño de las funciones que hacen a su rol en la organización.

n) Proveedor

Persona física o jurídica que provee o abastece a D-dev de Bienes o Servicios. Debe estar inscrito en el Registro de Proveedores del Estado y en el Registro de Proveedores del Organismo.

o) Registro

Se refiere a cualquier información generada como resultado de un procedimiento o utilizada de acuerdo con un procedimiento que tenga requerimientos de retención.

p) Seguridad Física

Se refiere al conjunto tangible de controles, aplicado al acceso a aquellos activos de información que impactan en la operación continua del ambiente informático, y/o aplicado en activos que tienen un valor intrínseco alto para D-dev

q) Seguridad Lógica

Se refiere a los controles basados en software, comúnmente en sistemas de información, que soportan los objetivos de la declaración de la política de seguridad.

r) Servicios de terceras partes

A propósito de este documento, los servicios de terceras partes incluyen:   
almacenamiento de datos y servicios de procesamiento de datos, proveedores de hardware/software, consultores de negocio y personal de seguridad. Los servicios de terceras partes también incluyen los tipos de servicios que no pueden proveerse internamente.

s) Sistemas de Información

Es el conjunto de activos de información que permiten la toma de decisiones en el negocio, independiente del medio en que se encuentren.

t) Usuarios principales del Sistema de Información:

Un Responsable de la Información

i. Comprende claramente la naturaleza de la Información, pudiendo advertir si la misma está completa y es correcta.

ii. en caso de no ser correcta, tiene la capacidad de corregirla en base a su propio conocimiento.

iii. conoce el tiempo de guarda requerido para la información.

Un Administrador de la Información es un funcionario, que tiene la responsabilidad de mantener y/o soportar la información corporativa.

Un Usuario de la Información es un funcionario, autorizado a utilizar la información en el desempeño de sus tareas.

1. Procedimientos
   1. Acceso a la Red (#ActiveDirectory)
   2. Asignación de contraseñas por defecto

Díganse más procesos.

1. Anexos

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

AHORA SI DESDE AQUÍ HAY QUE VER DONDE VA ESTO XDXDDXDD

**Política**

El Responsable de Seguridad Informática definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender:

* El propietario de la información se encargará de definir los privilegios del usuario para manejar la información
* El departamento de Ti se encargará de asignar los privilegios ya definidos por el propietario, al usuario generado por el departamento de TI.
* El departamento de TI debe verificar que el nivel de acceso otorgado es adecuado para cumplir únicamente la función correspondiente.
* El departamento de TI debe utilizar identificadores únicos, evitando la existencia de múltiples perfiles de acceso para un mismo empleado. *Ver anexo Formato Creación de Cuentas de Usuario.*
* Para el cambio de contraseña, el usuario deberá acudir con el Departamento de TI y este último deberá seguir el proceso de *Cambio de Contraseñas de Usuario.*
* El departamento de TI debe cancelar inmediatamente los permisos de los usuarios que cambiaron sus tareas o puestos, incluso de aquellos que se les revocó la autorización o se desvincularon de la Institución.

## 1.2.1 Gestión de Privilegios

### Política

* El Propietario de la información asignara los privilegios a los diversos roles de empleados sobre la base de la necesidad de uso, aplicando sólo el requerimiento mínimo para su rol funcional.
* El departamento de TI asignará, verificará gestionará los privilegios de los usuarios.
* El Propietario establecerá un periodo de vigencia para el mantenimiento de los privilegios (en base a la autorización que se les dará a los mismos) del cuál serán revocados.
* El departamento de TI será el encargado de modificar, asignar o revocar cualquier privilegio según los estipulado por el Propietario.

## 1.2.2 Gestión de contraseñas

* Cuando se cree el usuario de un empleado las contraseñas serán asignadas por el departamento de TI.
* Las contraseñas asignadas al usuario deberán ser cambiadas por este, siguiendo los lineamientos de contraseñas seguras incluidos en esta política, para que pueda acceder a la información y recursos de la empresa.
* El departamento de TI deberá validar las contraseñas creadas por el usuario.

### 1.2.2.1 Contraseñas seguras

Cuando hablamos de la seguridad de TI, las credenciales juegan un papel muy importante en esto porque estas pueden proporcionar diferentes niveles de autorización para personas. Los nombres de usuario pueden variar o seguir un formato especial por lo que son más fáciles de conocer, por lo tanto, las contraseñas son muy importantes.

### Política

* Se deben elegir contraseñas que sean difíciles de adivinar.
* La contraseña no puede incluir el nombre ni el cumpleaños, no debe usarse el número de placa del automóvil, el nombre del cónyuge o fragmentos de una dirección, no de ser una palabra que se encuentre en el diccionario o forme parte de vocablos populares.
* No está permitida la reutilización de contraseñas.
* La contraseña debe tener entre 10 y 16 caracteres.
* La contraseña debe contener por lo menos una mayúscula una minúscula un número y un signo.
* No se puede utilizar la misma contraseña para todas las cuentas y estas deben ser cambiadas cada 3 meses (revisar el anexo de Cambios de Contraseñas de Usuario).
* Si la contraseña contiene espacios, no puede ser separada por palabras.

Ejemplo:

Mi Contraseña Incorrecto

Micon traseña Correcto

### 

### **Procedimiento: #**ESTO PUEDE IR EN UN CAPITULO DE PROCEDIMIENTOS

A. **Solicitud Inicial / Renovación de Contraseña:** La solicitud de usuario y contraseñas (credenciales) se expide ante el administrador de cuentas de usuario.

B. **Administración de la Contraseña:** La contraseña es responsabilidad del usuario, de esta manera, es el usuario quien debe preocuparse del resguardo y recordatorio de la misma. Por lo tanto:

* Si una contraseña se olvida, el usuario debe solicitar el cambio de la misma al administrador de usuarios en el Departamento de TI. Sólo de esta manera, el Departamento está autorizado a utilizar el sistema para realizar un reset de los datos de la contraseña. Este sistema de gestión utilizado se realiza mediante un mecanismo que genera una contraseña aleatoria que se envía automáticamente por correo electrónico al usuario solicitante a la cuenta de E-mail que el mismo declaró como válida ante el Departamento de TI.

C. **Vencimiento de la Contraseña:** Las contraseñas tienen fecha de vencimiento. El vencimiento equivale a los 3 meses, teniendo que solicitar la renovación al Departamento de TI.

### Repercusiones

El incumplimiento de alguno de los requisitos establecidos en este documento dará lugar a repercusiones que se establecerán por el departamento de TI de acuerdo con el nivel de riesgo al que se expone la empresa.

## Responsabilidades del usuario #Esto va en responsabilidades lelelel

### 1.5.1 Uso de Contraseña:

### Política

* El Responsable de Seguridad Informática deberá asegurarse que todos los usuarios conozcan los lineamientos para crear sus contraseñas. **#Responsabilidad de seg info**
* El usuario deberá cambiar las contraseñas que le fueron asignadas por primera vez por el departamento de TI.
* Los usuarios deberán notificar cualquier incidente relacionado con un fallo de acceso al sistema al departamento de TI o en su defecto al Responsable de Seguridad Informática.
* Los usuarios deben cuidar que sus credenciales no estén expuestas, es decir, dejándolas fuera de alcance de cualquier persona no autorizada; las contraseñas no deben almacenarse con formato legible dentro de archivos de lote, scripts de ejecución automática, macros de software, funciones de terminal, software de comunicaciones, navegadores Web, discos duros, libretas o notas adhesivas, archivos .txt o cualquier otro medio donde puedan estar expuestas.
* En caso que se sospeche que la contraseña se ha revelado y que podría ser utilizada por un individuo no autorizado, esta deberá ser cambiada inmediatamente solicitando al departamento de TI por el cambio.
* Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá acudir al Departamento de Ti para que pueda crear una nueva contraseña.

### 1.5.3 Políticas para escritorios y monitores limpios

Esta política aplica para todos los empleados de D-Dev.

* Almacenar bajo llave, cuando corresponda, los documentos en papel y los  
  medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando  
  no están siendo utilizados, especialmente fuera del horario de trabajo.
* Guardar bajo llave la información sensible o crítica de la Institución  
  (preferentemente en una caja fuerte o gabinete a prueba de incendios)  
  cuando no está en uso, especialmente cuando no hay personal en la oficina.
* Desconectar de la red / sistema / servicio las computadoras personales,  
  terminales e impresoras asignadas a funciones críticas, cuando están  
  desatendidas. Las mismas deben ser protegidas mediante cerraduras de  
  seguridad, contraseñas u otros controles cuando no están en uso.
* Proteger los puntos de recepción y envío de correo electrónico y postal y las  
  máquinas de fax no atendidas.

### 

## Gestión de Acceso a la Red

### Objetivo

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto.

### Alcance

Esta política aplica a todos los empleados de la empresa incluyendo los trabajadores temporales que mantengan un acceso a los sistemas, base de datos y servicios de la organización.

### Acceso a internet

### Política

Requisitos:

* Se aplicarán controles y herramientas en función a los bloqueos de páginas no aprobadas y autorizadas por el responsable de Seguridad Informática.

Segregación de la red

* Área externa: Dentro de esta área se encuentran los invitados de la empresa, para hacer uso de la red aquí, se deberá solicitar un usuario temporal en el área de recepción.
* Acceso remoto: Todo usuario que requiera conectarse de manera remota a la red será a través de una VPN
* Área interna: Dentro de esta área se encuentran todos los empleados, ya sean permanentes o temporales, que requieran hacer uso de los recursos de la organización para realizar su trabajo.

## Acceso A las aplicaciones de la empresa

### Objetivo

Impedir el acceso no autorizado a la información contenida en las diferentes aplicaciones de la organización.

### Alcance

Esta política aplica a todos los empleados de la empresa incluyendo los trabajadores temporales que mantengan un acceso a los sistemas que interactúen con servicios internos de la organización, como lo son bases de datos u infraestructura.

### Política

1. Restricción de acceso a la información:
   1. Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:
      1. Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación
      2. Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.
      3. Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.
2. Aislamiento de los Sistemas Sensibles
   1. Las siguientes consideraciones son considerables en función a la criticidad asignada a la aplicación ó sistema.
      1. Identificar y documentar claramente la sensibilidad de un sistema de aplicación. Esta tarea será llevada a cabo por el administrador de la aplicación.
      2. Considerar la seguridad en la administración de las copias de respaldo de la información que procesan las aplicaciones.
      3. Considerar las mismas precauciones de seguridad y privacidad, en la elaboración del plan de continuidad y/o contingencia de la ejecución de la aplicación. Ejemplo: el equipamiento alternativo o las instalaciones de emergencia donde restablecer la aplicación.

\*Las contraseñas utilizadas en cada aplicación, tendrán que estar alineadas en base a la política de “*Contraseñas seguras*” incluida en este documento.

## Seguridad física y medio ambiente

### Controles de acceso físico

Propósito

Controlar el acceso a los sitios y áreas físicas restringidas y así proteger la información y los bienes informáticos.

Alcance

Esta política aplica para la persona que tenga acceso a las instalaciones, sin excepción, desde el área de limpieza y visitantes, deberán registrar al momento de su entrada, el equipo de cómputo, medios de almacenamiento y herramientas que no sean propiedad de la entidad, en el área de recepción, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.

Ejemplo de dispositivos.

|  |  |  |
| --- | --- | --- |
| Laptop | USB | Memory stick |
| Tablet | DISCOS | Backpacks |
| Celular | Memoria externa. |  |

Repercusiones

El incumplimiento de alguno de los requisitos establecidos en este documento dará lugar a Sanciones que se establecerán por el departamento de TI de acuerdo con el nivel de riesgo al que se expone la empresa.

### Acceso áreas restringidas

Propósito

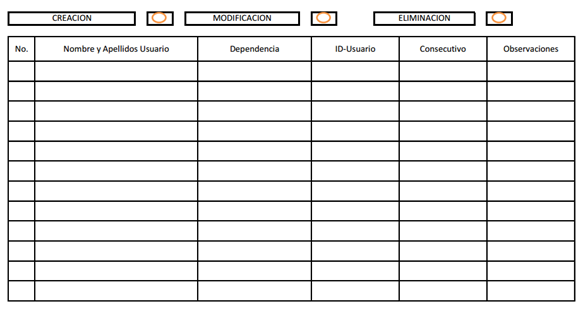
Cuando una persona no autorizada o un visitante requieran la necesidad de ingresar a los centros de datos, donde se encuentran los servidores, deberá solicitar mediante un comunicado interno debidamente firmado y autorizado por el Jefe inmediato de su sección o dependencia, y para un visitante se debe solicitar la visita con anticipación, y donde se especifique tipo de actividad a realizar, siempre contando con la presencia de un administrador de TI.

Alcance

Esta política aplica a todos los empleados de la empresa incluyendo los trabajadores temporales que mantengan un acceso a los sistemas, base de datos y servicios de la organización.

***Anexos***

Formato creación de cuentas de usuario.



Control de cambios

|  |  |  |  |
| --- | --- | --- | --- |
| Fecha de cambio | Número de versión | Explicación del cambio | Responsable |
| 23 de abril del 2016 | 2.0 | Adecuaciones | Área de Seguridad en Informática |
|  |  |  |  |

Control de emisión

|  |  |  |
| --- | --- | --- |
| Elaboro | Reviso | Aprobo |
| Eva Sofía García Reséndiz  Laura Viridiana Suarez Rodriguez  David Alejandro Herrera Pozos  Diego Alejandro Elizondo Carrillo |  |  |

**ANOTACIONES DE EVA kawaii**