POLITICA

POLITICA DE SEGURIDAD DE LA INFORMACION

ENTRADA EN VIGOR
10-MAY-2021

CONTROL DE CAMBIOS

VERSION	CAMBIOS REALIZADOS	AUTOR		FECHA
		NOMBRE	PUESTO	
01	Documento de nueva creación	Emilio Javier Ramírez García	Subdirector de Servicios en la Nube, Calidad y Gestión de Servicios TI	01/11/2017
1.0	Liberación del documento	Emilio Javier Ramírez García	Subdirector de Servicios en la Nube, Calidad y Gestión de Servicios TI	05-01-2018
1.1	Descripción estructurada de controles de seguridad	Emilio Javier Ramírez García	Subdirector de Servicios en la Nube, Calidad y Gestión de Servicios TI	15-05-2018
1.2	Se agrega nota sobre los controles de seguridad de la información	Emilio Javier Ramírez García	Subdirector de Servicios en la Nube, Calidad y Gestión de Servicios TI	15-05-2018
1.3	Correcciones de formato y sintaxis. Alta y baja de algunas políticas	Emilio Javier Ramírez García	Subdirector de Servicios en la Nube, Calidad y Gestión de Servicios TI	11-06-2018
2.0	Ajustes resultantes de la auditoría interna 2021	Milton Martinez	Responsable del SGI	07-may-21

INDICE

CONTENIDO

1. ALCANCE

Este documento aplica para todos los servicios dentro del alcance del Sistema de Gestión Integral (SGI).

2. GENERAL

2.1. Aspecto General

Con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información propia o de terceros que ostenta Teledinámica México S.A. de C.V. (Teledinámica) para efecto de llevar a cabo sus operaciones, los usuarios de todos los niveles tienen el deber de acatar y ejecutar las medidas pertinentes que sean definidas en la presente Política de Seguridad de la Información, por el Responsable de la Seguridad de la Información dentro de Teledinámica, en representación operativa del Comité del Sistema de Gestión Integral (SGI).

Estas medidas se aplicarán sin excepción a todos los sistemas informáticos, equipos electrónicos y accesos físicos, de forma que estos garanticen la confidencialidad, integridad y disponibilidad de la información contra toda clase de amenaza que comprometa o pueda eventualmente comprometer, distorsionar o desviar el uso de la información hacia una actividad diferente para la que se tiene disponible.

El comité del SGI tiene como objetivo principal, implementar, definir y en su caso actualizar, los procedimientos necesarios para el cumplimiento de esta Política.

Esta Política de Seguridad de la Información será revisada al menos una vez al año para su actualización y autorización de cambios por el Comité del SGI, en caso de que se requiera, el Responsable de la Seguridad de la Información podrá presentar sus sugerencias de mejora en cualquier momento al Responsable del SGI.

2.2. Clasificación de la información

La clasificación de la información será realizada de acuerdo con los siguientes niveles, mismos que deberán utilizarse para describir la información documental que sea generada:

Nivel	Facultades
Restringido	Información que, si es divulgada a entidades no autorizadas, podría tener un impacto en obligaciones legales o reguladoras de la Organización, en sus estados financieros o clientes.
Confidencial	Información acerca de clientes, empleados y/o negocios de la Organización que la misma está obligada a proteger Información que la Dirección General de la Organización determine tiene potencial para proporcionar una ventaja competitiva u ocasionar un impacto significante en el negocio si es divulgada a entidades no autorizados
Interno	La información que se comparte común y libremente dentro de la Organización y que no esté clasificado como restringida o confidencial como pueden ser: 1. Procedimientos 2. Instrucciones de Trabajo 3. Políticas 4. Formatos 5. Comunicados
Público	Información que es libremente disponible al exterior de la Organización y que se haya elaborado para ser de uso público: 1. Folletos 2. Anuncios de productos y/o servicios 3. Solicitud de vacantes 4. Página web http://www.teledinamica.com.mx 5. Política de Seguridad de la Información

2.3. Sanciones previstas por incumplimiento

El área responsable de aplicar las sanciones correspondientes derivadas del incumplimiento de esta Política de Seguridad de la Información es la Dirección de Administración, debiendo recibir la notificación y evidencia (en caso de que aplique) por el Responsable de la Seguridad de la Información, siempre y sin excepción copiando en esta notificación al Jefe inmediato de la persona que haya incurrido en la violación de esta.

Ante cualquier dificultad o impedimento que se presente en la aplicación de las sanciones anteriormente descritas, el Comité del SGI e incluso el Director General auxiliarán a la Dirección de Administración en la aplicación de la sanción correspondiente.

2.4. Comité del Sistema de Gestión Integral

El Comité del Sistema de Gestión Integral está conformado por la Dirección General, el Representante de la Dirección y el Responsable del SGI, y cuenta con las atribuciones, obligaciones y restricciones para la elaboración, revisión y cumplimiento tanto de esta política como de los procedimientos de seguridad que se incluyen en la misma. Con la diferencia que la Dirección General o el Representante de la dirección, están facultados para agregar, modificar o derogar elementos de esta política.

2.5. Verificación de la aplicación de la Política de Seguridad de la Información

La verificación de la aplicación de la Política de Seguridad de la Información se revisará a través de la ejecución de la auditoría de Seguridad de la Información.

2.6. Administración de excepciones.

El manejo de excepciones en la presente Política de Seguridad de la Información serán validadas por el Responsable de la Seguridad de la Información, siempre que sean evaluadas y autorizadas por la Dirección General y/o un representante de esta y/o del Comité del SGI.

Si la EXCEPCIÓN se encuentra documentada, su aplicación dependerá de la acción establecida para llevarla a cabo

Ante la necesidad de una NUEVA EXCEPCIÓN a la política de seguridad se deberá solicitar al Responsable de Seguridad de la Información mediante el registro de un incidente de seguridad (conforme al proceso de gestión de incidentes de seguridad), analizar el riesgo correspondiente y determinar las acciones de mitigación para llevar a cabo la excepción.

3. POLITICA DE SEGURIDAD DE LA INFORMACIÓN

3.1. Política de cierre de sesión por inactividad

- Cuando el usuario se separe de cualquier equipo de cómputo o comunicación, realizará un bloqueo de pantalla de manera manual.
- El sistema operativo del equipo de cómputo o comunicación bloqueará la pantalla por inactividad a los 3 minutos.
- En ambos casos se requerirán las credenciales de usuario o método de desbloqueo para continuar la operación del equipo de cómputo o comunicación.
- Para el caso de aplicaciones específicas que requieran tener una sesión activa se considerará la excepción a lo mencionado en la sección 3.1 de este documento.

3.2. Política de creación de contraseñas

El uso de contraseñas, credenciales de usuario o método de desbloqueo en el software que así lo permita deberá incluir las siguientes características:

- Longitud mínima de 8 caracteres alfanuméricos.
- Incluir al menos un carácter en mayúscula.
- Incluir al menos un carácter en minúscula.
- Incluir al menos un número.
- No debe repetir consecutivamente 2 o más veces el mismo carácter.
- No debe incluir parte del nombre de usuario.
- No debe incluir secuencias alfabéticas o numéricas de 3 o más caracteres.
- Las contraseñas, credenciales de usuario o método de desbloqueo serán cambiadas por el usuario en su primer ingreso, ya sea por alta o restauración.

- Las contraseñas, credenciales de usuario o método de desbloqueo solo podrán ser cambiadas por el Gestor de Servicios TI al ser solicitada por el usuario o Jefe inmediato del mismo por medio de un correo electrónico a la dirección soporte@teledinamica.com.mx

3.3. Uso de medios removibles

- El uso de medios removibles (USB) se encuentra habilitado en todos los equipos de la empresa.
- Al utilizar medios removibles, estos deberán ser revisados inmediatamente con el software antimalware instalado en el equipo de cómputo.
- En el supuesto que se requiera la salida de información de la empresa en un medio removible y de alguna forma no considerada en algún proceso operativo previamente definido, dicha salida deberá ser solicitada por medio de un correo electrónico a la dirección soporte@teledinamica.com.mx para realizar el análisis, evaluación del riesgo y autorización por el Responsable de Seguridad de la Información.
- El mecanismo de autorización será en respuesta a petición escrita por medio de correo electrónico a la dirección soporte@teledinamica.com.mx, debiendo quedar como evidencia dicha petición, justificación y en su caso la autorización o declinación de la petición.
- Como excepción a lo anterior, las subdirecciones Comercial y de Ingeniería y servicios, dirección general, operaciones, calidad, capacitación, así como la Dirección de Administración estarán exentas de solicitar la autorización de salida de información.
- La destrucción de la información que se almacene en un medio extraíble deberá realizarse de acuerdo con los lineamientos establecidos en la sección "Depuración de información" para minimizar cualquier riesgo de comprometer la información.

3.4. Uso de teléfonos inteligentes y cámaras fotográficas

- Se prohíbe de manera general la toma de fotografías o imágenes del personal, pantallas de aplicativos en equipos de cómputo y comunicaciones, así como de las instalaciones físicas de Teledinámica México S.A. de C.V. y/o de sus clientes, salvo que lo anterior se encuentre descrito dentro de un proceso o actividad específica que se encuentre plenamente documentada.

3.5. Seguridad en redes

- Todo el tráfico proveniente de redes externas deberá ser inspeccionado por el sistema de prevención de intrusos (Cisco ASA ASA 5508 NGFW with Firepower Services) y bloqueado aplicando las políticas configuradas en el firewall perimetral.
- Deberá contarse con un diagrama general de la red de comunicaciones, el cual deberá mostrar de forma lógica la conectividad de los diversos componentes de red.
- Los equipos de cómputo y servidores deberán contar con software antimalware que permita identificar, contener, bloquear y eliminar cualquier amenaza proveniente de archivos o procesos en ejecución.
- Los invitados que requieran conectividad a internet deberán utilizar la red aislada lógicamente del tráfico productivo.
- La información de carácter “confidencial” y “restringida” de Teledinámica México S.A. de C.V. o sus clientes que sea procesada o transmitida por correo electrónico a través de redes públicas, deberá contar con controles de seguridad para cifrado de transmisiones, tales como certificados TLS 1.2 o superior, o canales cifrados con algoritmos síncronos o asíncronos mayores o iguales a 128 bits por medio de la utilización de los clientes de correo Microsoft Outlook y MacMail, así como a través de los navegadores de internet Google Chrome, Mozilla Firefox, Microsoft Internet Explorer y Safari.

3.6. Circuito cerrado de Televisión (CCTV)

- La organización cuenta con un sistema de circuito cerrado de televisión, distribuido en las áreas de acceso y zonas restringidas de Teledinámica México S.A. de C.V., la visualización de las cámaras puede ser realizada a través de internet por la Dirección General y eventualmente proyectada en la pantalla colocada en el acceso principal a las oficinas.
- La modalidad de grabación es continua.

3.7. Control de accesos

- Se lleva un registro de los accesos a las instalaciones, siendo este realizado por el visitante en un "libro de visitas". En el caso de que se requiera un acceso de equipo electrónico (notebook, Tablet, entre otros) se deberá registrar marca, modelo y número de serie del equipo ingresado.
- Durante su estancia, ningún visitante podrá estar solo en cualquiera de las instalaciones, sin excepción deberá ser siempre acompañado por un responsable del área responsable de su visita.
- El acceso a las instalaciones de Teledinámica México S.A. de C.V. estará restringido por un sistema de control de acceso biométrico.

3.8. Asignación y retiro de activos

- Toda asignación y retiro de activos deberá formalizarse por medio de la "Carta Responsiva" como forma de asignación y devolución de activos.
- Cuando un usuario cambie de puesto dentro de la organización, se deberá llevar a cabo la devolución de los activos asignados y la asignación de activos de acuerdo con su nuevo rol.
- Cuando el usuario cause baja de la organización se le deberá solicitar los activos bajo su responsabilidad.

3.9. Intercambio de información

- La organización definirá y establecerá acuerdos para el intercambio de información entre personal interno.
- Se establecerán túneles seguros para intercambio de información como pueden ser VPNs basados en IPSEC, túneles SSH, así como el acceso por medio de sitios HTTPS.
- La información física que viaje fuera de las instalaciones de Teledinámica México S.A. de C.V. deberá ser enviada por algún tipo de mensajería interna o privada, utilizando sobres cerrados.

Es importante mencionar que para efectuar dicho intercambio de información de forma segura se requiere la colaboración e interacción con el cliente, por lo que el riesgo eventual de intercambiar información con el cliente sin lograr un cifrado depende de su disponibilidad e infraestructura.

La información podrá ser transmitida según su clasificación por los siguientes medios:

Nivel	Pública	Interna	Confidencial	Restringida
Sitios WEB	SI	NO	NO	NO
Correo electrónico	SI	SI	SI	NO
Correo electrónico con información cifrada	SI	SI	SI	SI
Por medio de VPN y conexiones seguras como SFTP/HTTPs internos y a clientes	SI	SI	SI	SI
Mensajería electrónica	SI	SI	SI	NO
Mensajería privada en sobre sellado seguro	SI	SI	SI	SI
Transmisión de palabra, incluyendo el teléfono móvil, correo de voz, contestador, equipos	SI	SI	SI	SI

Para el tipo de información confidencial y/o restringida se podrá comunicar verbalmente siempre y cuando sea un sitio seguro y entre partes involucradas.

3.10. Depuración de información

Información Física (Confidencial y Restringida)

- En el caso de que se solicite la destrucción de una determinada información en algún medio físico, se deberá realizar una petición por parte del interesado, identificando la información que desea ser destruida y el fundamento de la destrucción, para posteriormente calendarizar el evento en que la destrucción se llevará a cabo.
- De manera física se destruirá utilizando una trituradora genérica de papel.

Información Lógica

- Para la información lógica clasificada como Restringida o Confidencial, la destrucción se ejecutará de acuerdo con lo especificado en el contrato con cada cliente, a petición expresa del cliente o bien, cuando la legislación aplicable lo permita.
- Para el borrado de discos se utilizará la herramienta "DiskWipe" (http://www.diskwipe.org) y se generará una bitácora de destrucción que será firmada por el solicitante y el personal de Teledinámica que haya sido asignado para realizar la destrucción.

  *Nota: cuando se lleva la maquina de computo a valores de fabrica no es necesario utilizar esta herramienta.

- Para el borrado de archivos de las plataformas Windows se utilizará la herramienta "WipeFile" (https://www.gaijin.at/en/dlwipefile.php) y se generará una bitácora de destrucción que será firmada por el solicitante y el personal de Teledinámica que haya sido asignado para realizar la destrucción.

4. TECNOLOGIAS DE LA INFORMACIÓN

4.1. Antimalware

Los productos de software antimalware aprobados por el Responsable de la Seguridad de la Información son:

- Symantec Endpoint Protection Small Business Edition
- Cisco AMP for Endpoints
- Windows Defender
- Bit Defender
- McAfee

Se permitirá la utilización de productos de software gratuitos que acompañen a equipos de cómputo recién adquiridos, bajo las siguientes consideraciones:

- El producto de Antimalware específico deberá ser analizado y aprobado por el Responsable de la Seguridad de la Información.
- El producto de Antimalware específico deberá ser utilizado solamente durante su período de gratuidad y al final de este período ser sustituido por alguno de los productos aprobados mencionados anteriormente.

La configuración del antimalware deberá ser la siguiente:

Tareas	Cobertura	Administrador
Análisis de Correo electrónico	Cliente de correo electrónico Tiempo real	Gestor de Servicios TI
Análisis de Navegación	Navegadores Web Tiempo real	Gestor de Servicios TI
Prevención de intrusiones	Escaneo de puertos Tiempo real	Gestor de Servicios TI
Análisis del Sistema	Todos los archivos Tiempo real	Gestor de Servicios TI
Actualizaciones	Automático con revisión diaria de actualizaciones por la consola de	Gestor de Servicios TI

Tareas	Cobertura	Administrador
	administración	

En caso de detectarse alguna infección o amenaza a un equipo de cómputo se deberá proceder conforme a la sección 4.7 de la presente Política de Seguridad de la Información.

4.2. Respaldo de información

El respaldo de la información deberá realizarse periódicamente.

Los respaldos podrán realizarse a través de las siguientes opciones:

- En la IP interna asignada al NAS en sitio
- Utilizando el servicio MS OneDrive
- Utilizando el servicio Google Drive
- Utilizando cualquier otro servicio de respaldo automático a elección del usuario

4.2.1. Base de datos

Dado que los servicios de TI críticos se encuentran operativos en entornos de nube, las bases de datos de dichos servicios son respaldadas como parte del mismo servicio.

4.2.2. Verificación de integridad de respaldos

La verificación de respaldos de información de los servicios de TI críticos deberá realizarse de forma aleatoria al menos una vez al año por parte del Responsable de la Seguridad de la Información.

4.3. Control de acceso al Software

4.3.1. Equipo de cómputo

El equipo de cómputo debe cumplir los lineamientos establecidos en la política de creación de contraseñas.

4.3.2. Sistema de Gestión Integral y Mesa de Servicios

Tanto el SGI como el software OTRS para la gestión de la Mesa de Servicios deberán cumplir los lineamientos establecidos en la política de creación de contraseñas, así como la periodicidad de estas.

4.3.3. Servidores

Los servidores deben cumplir los lineamientos establecidos en la política de creación de contraseñas.

El acceso a los servidores está restringido y solo personal de la Subdirección de Ingeniería y Servicios, Operaciones y Administración tendrá acceso para uso exclusivo de sus funciones laborales y acciones de mantenimiento y/o monitoreo.

4.3.4. Otros sistemas

Si el software lo permite, se asignará una contraseña que cubra los lineamientos establecidos en la política de creación de contraseñas.

En el caso que no lo permita se documentará el software correspondiente en la tabla siguiente:

Software	Fabricante	Uso	Responsable
Control de Acceso Biométrico	ZKTime5.0	Control de Acceso Biométrico	Subdirección de servicios en la nube, calidad y gestión de servicios TI
IVMS-400	N/A	Circuito cerrado de TV	Dirección General
Web Access Buffalo	Buffalo	Repositorio	Subdirección de Ingeniería y servicios

4.3.5. Privilegios de Administración de otras áreas

La Subdirección de Ingeniería y Servicios, Soluciones de Producto y el Gestor de Servicios de TI podrán contar con privilegios administrativos en sus equipos, así como herramientas de acceso a datos y en su caso de programación para la ejecución y modificación de rutinas de manera manual, esto derivado de que todos los clientes cambian eventualmente el layout de intercambio de información, por lo que se requiere tener las herramientas para analizar los cambios requeridos.

4.4. Sistema de Detección de Intrusiones y Uso de Software

4.4.1. Software

El software utilizado deberá ser justificado para su uso en las actividades propias de la organización y el servicio brindado a los clientes.

Este software deberá estar inventariado en la siguiente tabla y autorizado por la Subdirección de servicios en la nube, calidad y gestión de servicios TI:

Software	Fabricante	Objetivo	Área
SO Windows	Microsoft	Operación de equipos de cómputo.	Toda la organización
SO MacOS	Apple	Operación de equipos de cómputo.	Toda la organización
Office Standard 2010 Office Standard 2013 Office 365 Business Premium	Microsoft	Actividades documentales de Oficina	Toda la organización
Symantec Endpoint Protection Small Business Edition	Symantec	Protección al End-Point	Toda la organización
Cisco AMP for Endpoints	Cisco	Protección al End-Point	Toda la organización
Chrome	Google	Sistema GWEB	Toda la organización
Firefox	Mozilla	Sistema GWEB	Toda la organización
Internet Explorer	Microsoft	Sistema GWEB	Toda la organización
Safari	Apple	Sistema GWEB	Toda la organización
Sales-Up	BFX	CRM	Comercial y Administración
Acrobat Reader	Adobe	Lectura de documentos PDF	Todos
Acrobat Pro	Adobe	Edición de documentos PDF	Administración
Putty	Putty.org	Cliente SSH y Terminal	SubDirección de Ingeniería y Servicios
Consolas Checkpoint	Checkpoint Technologies	Administración de seguridad perimetral	SubDirección de Ingeniería y Servicios
Aspel Bancos	Aspel de México S.A. de C.V.	Gestión de cuentas bancarias	Administración
Aspel COI	Aspel de México S.A. de C.V.	Gestión de Contabilidad	Administración
Aspel NOI	Aspel de México S.A. de C.V.	Gestión de Nómina	Administración
Aspel SAE	Aspel de México S.A. de C.V.	Gestión de administración empresarial	Administración Subdirección de Operaciones
One-X	Avaya	Comunicaciones	Toda la organización
Webex	Cisco	Comunicaciones	Toda la organización
Windows defender	Microsoft	Antimalware	Toda la organización
McAfee	McAfee	Antimalware	Toda la organización

Se prohíbe el uso de software que no haya sido evaluado y autorizado por los antimalware autorizados para minimizar cualquier posible riesgo que comprometa la continuidad del negocio.

4.5. Robustecimiento de Sistemas

El robustecimiento de seguridad a nivel infraestructura se aplicará según el criterio correspondiente en cada punto siguiente:

4.5.1. Servidores

Las acciones que seguir para el robustecimiento de la seguridad en servidores son:

- Desactivar/Eliminar usuarios por defecto
- Configuración de usuarios personalizados
- Evitar el uso de contraseñas genéricas
- Instalar actualizaciones y parches de seguridad
- Robustecer contraseñas según Política de Control de Acceso a Software
- Instalación de herramientas antimalware y de seguridad perimetral

4.5.2. Equipo de cómputo

Las acciones que seguir para el robustecimiento de la seguridad en estaciones de trabajo son:

- Desactivar/Eliminar usuarios por defecto o genéricos
- Configuración de usuarios personalizados
- Evitar el uso de contraseñas genéricas
- Restringir los usuarios al software y servicios requeridos
- Instalación de actualizaciones y parches de seguridad
- Robustecimiento de contraseñas según Política de Control de Acceso a Software
- Uso de antimalware en Sistemas Operativos
- Uso de Software de Cifrado autorizado por la empresa, revisar política de cifrado de información, salvo ejecución de la política de manejo de excepciones

4.5.3. Otros equipos e infraestructura

Las acciones que seguir para el robustecimiento de la seguridad en equipos de comunicación y seguridad son:

- Desactivar/Eliminar usuarios por defecto o genéricos
- Configuración de usuarios personalizados
- Cambio inmediato de contraseñas genéricas
- Instalación de actualizaciones y parches de seguridad
- Robustecimiento de contraseñas según Política de Control de Acceso a Software

4.6. Gestión de incidentes de Seguridad de la Información

Los Incidentes asociados a la seguridad de la información se gestionarán por medio del subproceso “Gestión de Incidentes y Solicitudes del Servicio”.

4.6.1. Definición de incidentes de Seguridad

Cualquier evento no planificado que interrumpa la provisión de un servicio de TI y que amenace la integridad, disponibilidad o autenticidad de la información será considerado un incidente de seguridad.

La lista que se presenta a continuación es de carácter ilustrativo y deberá considerarse su contenido de forma enunciativa más no limitativa.

Incidente	Clasificación
Acceso no autorizado	Ataque de red
Incumplimiento de políticas	Cumplimiento
Intento de intrusión	Ataque de Red
Falla en respaldos	Continuidad
Ataques de denegación de servicios	Disponibilidad
Ataque de intrusión por fuerza bruta	Ataque de red
Fotografía en áreas restringidas	Confidencialidad

Los intentos de intrusión que sean atajados por parte del software de protección antimalware no se considerarán incidentes de seguridad.

4.6.2. Definición de roles y responsabilidades

El equipo involucrado en la administración de incidentes se compone de personal de, de las Subdirecciones de Ingeniería y eventualmente personal de los proveedores externos de servicio.

Puesto	Rol	Responsabilidad
Responsable de Seguridad de la Información	Propietario y gestor del proceso	Definición y operación del proceso.
Gestor de Servicios de TI	Gestor de Incidentes	Registro, análisis, evaluación y resolución de incidentes.
Subdirección de Ingeniería y Servicios	2ª. Línea de soporte	Análisis, evaluación y resolución de incidentes.
Dirección General	Gestor de Aplicación GSuite	Análisis, evaluación y resolución de incidentes.
Gerente de Desarrollo de Producto	Gestor de Aplicación SalesUp	Análisis, evaluación y resolución de incidentes.
Gerente de Servicios	Gestor de Aplicación OTRS	Análisis, evaluación y resolución de incidentes.

4.7. Seguridad física y ambiental

4.7.1. Centro de Datos

El centro de datos, cuyo objetivo es el resguardo, procesamiento y protección de la información, contará con control de acceso físico estrictamente restringido a las personas cuya necesidad amerite el ingreso al mismo.

El centro de datos tendrá un servicio de aire acondicionado para mantener la temperatura estable.

Se encuentra estrictamente prohibido ingresar con alimentos y bebidas al centro de datos.

4.7.2. Control de acceso.

La organización cuenta con control de acceso físico, basado en lectores biométricos de huella digital, permitiendo la identificación del personal que ingresa a las zonas de operación, áreas seguras y de procesamiento de información.

4.8. Plan de riesgos inducidos por terceros

4.8.1. Plan de riesgos sobre la información

En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta que se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

Ningún visitante deberá permanecer solo en ningún área de las instalaciones, independientemente del motivo de su visita estará acompañado por la persona responsable de su visita o en su caso por alguien designado para esta actividad.

Cuando exista la necesidad de otorgar acceso a terceras partes a la información deberá ser autorizado por el Responsable de Seguridad de la información y el Propietario de la Información de que se trate.

4.8.2. Seguridad de la Información en proveedores

El Responsable de la Seguridad de la Información deberá participar en los procesos de Evaluación y Selección de Proveedores, así como realizar revisiones periódicas a la Seguridad de la Información de los proveedores.

Se comunicará esta Política de Seguridad a los proveedores críticos y se firmará entre ambas partes un convenio de confidencialidad.

4.9. Plan de control de cambios de software

4.9.1. Detección del requerimiento.

Cuando se detecte que existe una necesidad, esta deberá ser solicitada vía correo electrónico a la dirección soporte@teledinamica.com.mx y de ser necesario, realizando una reunión para el análisis de los requerimientos y justificación de la necesidad, debiendo quedar documentado en una minuta.

4.9.2. Evaluación de necesidades

Se gestionará con el SubProceso Gestión de Cambios.

4.9.3. Plan de instalación y actualizaciones

Se gestionará por el SubProceso Liberación y Despliegue.

5. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Los controles de Seguridad de la Información aplicables a la organización son:

- Aprobación, publicación y sensibilización de la Política de Seguridad de la Información
- Control de visitas
- Control de Acceso Físico Restringido a las instalaciones generales
- Control de Acceso Físico Restringido al Centro de Datos
- Segmentación lógica de la red
- Definición de roles y responsabilidades inherentes a la seguridad de la información
- Definición de tipos de incidentes de seguridad
- Existencia de diagrama de red
- Funcionamiento del circuito cerrado de televisión
- Existencia de Carta Responsiva de Activos
- Acuerdos de Confidencialidad
- Definición de Comité de Gestión de Crisis
- Pruebas de continuidad

Los controles específicos de Seguridad de la Información que serán aplicables a computadoras y determinados elementos de configuración de servicios serán:

- Establecimiento de contraseñas y bloqueo de equipo de cómputo
- Instalación y configuración de antimalware con escaneo automático y estado de equipo
- Respaldo de Información
- Licenciamiento de Office y otros programas de software autorizados
- Ausencia de software no autorizado
- Depuración de información

5.1. Auditoría de la Política de la Seguridad de la Información

Se deberá realizar una auditoría aleatoria del cumplimiento de la presente política para asegurar el cumplimiento de los controles de seguridad de la información.

Esta auditoría deberá de contener los siguientes elementos

- Fecha de la revisión.
- Responsable de la revisión.
- Periodo de revisión.
- Validador de la revisión.
- Activos revisados y/o controles
- Remediaciones a aplicar

La auditoría deberá ser efectuada por el personal de la Subdirección de Servicios en la Nube, Calidad y Gestión de Servicios TI y eventualmente apoyadas por personal de terceros.

La auditoría será llevada a cabo al menos una vez al año.

La validación de las auditorias serán efectuadas por el Responsable de la Seguridad de la Información.