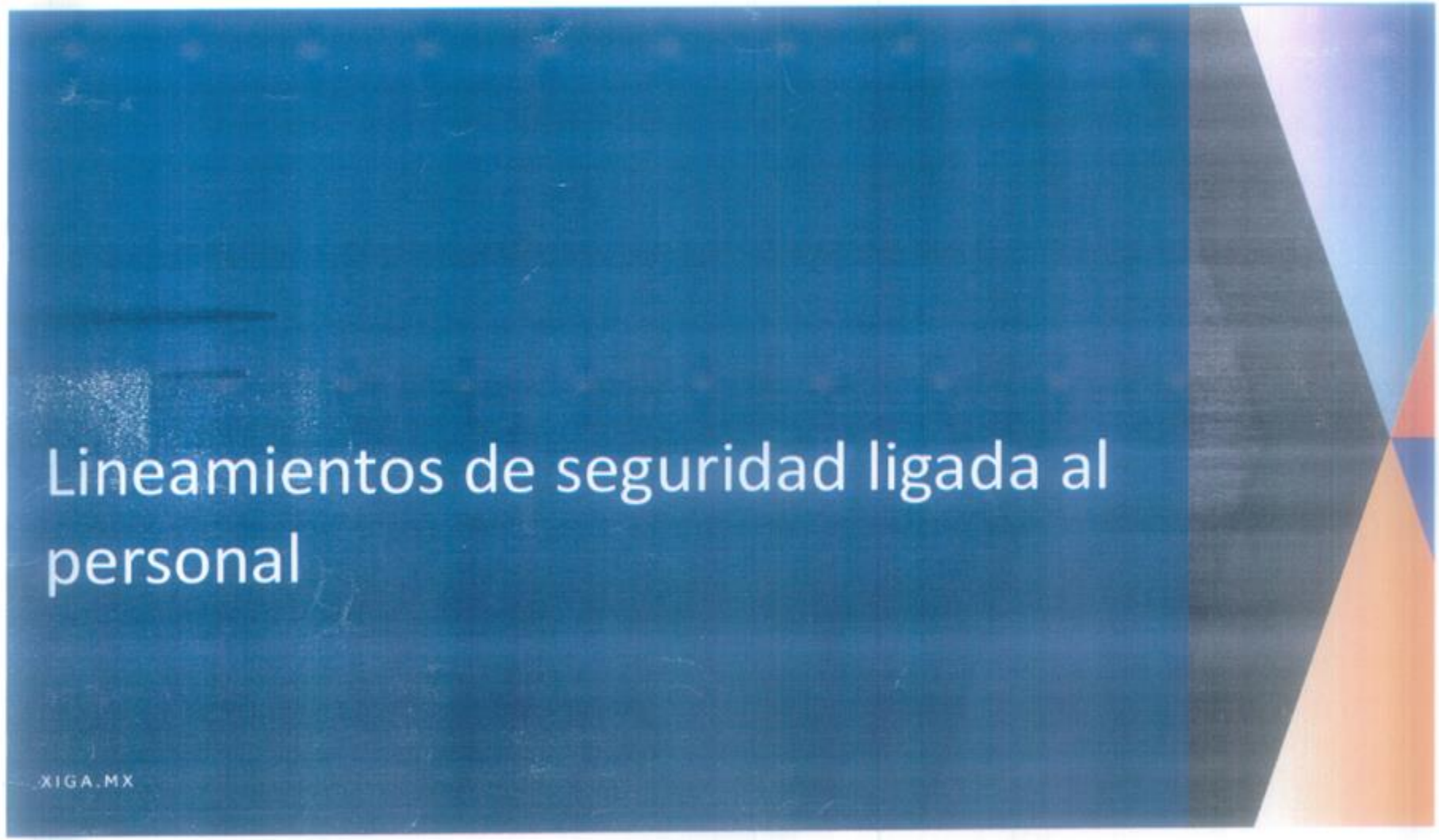
Lineamientos de seguridad ligada al personal
XIGA.MX

Alcance

Las Políticas y Estándares de Seguridad aplican de manera obligatoria todos los usuarios en XIGA, con el fin de lograr el uso seguro de equipos, aplicaciones, instalaciones y servicios de Tecnologías de Información.

NORMA ISO 27001

Introducción

Entre otros estándares, conocer la norma ISO 27001 ayuda a comprender como gestionar la seguridad de la información en la organización.

Cláusulas ISO/IEC 27001:2022

0. INTRODUCCIÓN
0 Introducción
0.1 Generalidades
0.2 Compatibilidad con otros Sistemas de Gestión

1. OBJETO Y CAMPO DE APLICACIÓN
Norma aplicable a cualquier organización, cualquiera que sea su actividad y cualquiera que sea su tamaño.

2. NORMAS PARA CONSULTA
ISO 27000:2014

3. TÉRMINOS Y DEFINICIONES
Recogidos en la Norma ISO 27000

4. CONTEXTO DE LA ORGANIZACIÓN
4.1 COMPRENSIÓN DE LA ORGANIZACIÓN Y DE SU CONTEXTO
4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS
4.3 DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)
4.4 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

5. LIDERAZGO
5.1 Liderazgo y compromiso
5.2 Política
5.3 Roles, responsabilidades y autoridades en la organización

6. PLANIFICACIÓN (PLAN)
6.1 ACCIONES PARA TRATAR LOS RIESGOS Y OPORTUNIDADES
6.1.1 Consideraciones Generales
6.1.2 Apreciación de riesgos de seguridad de la información
6.1.3 Tratamiento de los Riesgos de Seguridad de la Información
6.2 Objetivos de seguridad de la información y planificación para su consecución
6.3 Planificación de los cambios

7. SOPORTE
7.1 Recursos
7.2 Competencia
7.3 Concienciación
7.4 Comunicación
7.5 Información documentada
7.5.1 Consideraciones generales
7.5.2 Creación y actualización
7.5.3 Control de la información documentada

8. OPERACIÓN (DO)
8.1 Planificación y control operacional
8.2 Apreciación de los riesgos de seguridad de la información
8.3 Tratamiento de los riesgos de la seguridad de la información

9. EVALUACIÓN DEL DESEMPEÑO
9.1 Seguimiento, medición, análisis y evaluación
9.2 Auditoría Interna
9.2.1 General
9.2.2 Programa de auditoría interna
9.3 Revisión por la Dirección
9.3.1 General
9.3.2 Aportaciones a la Revisión por Dirección
9.3.3 Resultados de la Revisión por Dirección

10. MEJORA
10.1 Mejora continua
10.2 No conformidad y acciones correctivas

XIGA

ESTANDAR ISO 27001

Introducción

ISO 27001 norma internacional que se ha preparado para proporcionar los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información.

El objetivo principal de esta norma es la defensa, protección y gestión de la información como uno de los activos más importantes de la empresa

TEMAS	Nº CONTROLES
CONTROLES ORGANIZATIVOS	37
CONTROLES SOBRE LAS PERSONAS	8
CONTROLES FÍSICOS	14
CONTROLES TECNOLÓGICOS	34
TOTAL: **93 CONTROLES**	

El Anexo A es común y permite una completa integración con otros sistemas de Gestión basados en Normas ISO (Ej: Norma ISO 9001:2015; Norma ISO 14001:2015, etc.).

ISO/IEC 27001:2013 Anexo A Dominios de control

A5 – Políticas de seguridad de la información (2 controles)
A6 – Organización de la seguridad de la información (7 Controles)
A7 – Seguridad de los recursos humanos (6 controles)
A8 – Gestión de activos (10 controles)
A9 – Control de acceso (14 controles)
A10 – Criptografía (2 controles)
A11 – Seguridad física y ambiental (15 controles)
A12 – Seguridad de las operaciones (14 controles)
A13 – Seguridad de las comunicaciones (7 controles)
A14 – Adquisición, desarrollo y mantenimiento de sistemas (13 Controles)
A15 – Relaciones con proveedores (5 controles)
A16 – Gestión de incidentes de seguridad de la información (7 controles)
A17 – Aspectos de seguridad de la información en la gestión de la continuidad del negocio (4 controles)
A18 – Cumplimiento (8 controles)

JUSTIFICACIÓN

Las nuevas plataformas tecnológicas y la disponibilidad de interconectarse a través de redes, ha abierto nuevos horizontes para la protección los sistemas e instalaciones tecnológicas.

Por lo que es necesario establecer acuerdos y procesos para la protección de los activos tecnológicos e información. A continuación, se mencionan los principales procesos y políticas de seguridad.

POLÍTICA DE SERVICIOS TI

La política de Servicios TI establece las funciones y responsabilidades del prestador de servicios de TI. Entre las cuales se encuentran:

- Establecer procedimientos e implementar herramientas para asegurar su cumplimiento.
- Brindar apoyo cuando el personal requiera alguna nueva aplicación o funcionalidad para realizar sus actividades laborales.
- Mantener los equipos con antivirus activo y actualizado.
- Generar copias de seguridad periódicas de toda la información de la organización.

XIGA

POLÍTICA DE SERVICIOS TI

A su vez, en Política de Servicios podrás encontrar lineamientos sobre el uso de los recursos informáticos. Por ejemplo:

- La asignación de los recursos informáticos al usuario, es por medio de una Carta Responsiva, la cual al firmarla se compromete a vigilar que se conserven en óptimas condiciones físicas, para que su desgaste sea sólo el generado por su uso normal de trabajo.
    - No alterará ninguna componente (ya sea hardware o software) de los recursos informáticos.
    - En caso de alguna falla en los recursos informáticos se canalizará con el departamento de Sistemas a través de los mecanismos que se hayan establecido.
- Seguridad periódicas de toda la información de la organización.

POLÍTICA DE SERVICIOS TI

Uso de los medios de comunicación

Están destinado única y exclusivamente a las actividades laborales relacionadas con la organización.

El servicio de acceso a internet está configurado para restringir el acceso a ciertos sitios (redes sociales, transmisiones de música y videos, juegos, pornografía, etc.) El usuario final está obligado a respetar dichos filtros.

El usuario final tiene prohibido el uso de cualquier tipo de herramienta, ya sea vía hardware y/o software, para saltarse los filtros de contenido y obtener acceso a sitios restringidos.

.

XIGA

POLÍTICA DE SERVICIOS TI

... Continuación: Uso de los medios de comunicación.

El usuario no debe compartir su contraseña con cualquier otro colaborador o externo, a excepción de posible mantenimiento que se deba hacer a su equipo, a lo que solo deberá compartir sus credenciales de acceso, con el departamento de Sistemas.

En los correos electrónicos, el usuario únicamente puede adjuntar archivos con extensiones del tipo de archivos permitidos en las definiciones.

Los archivos con extensión: .exe | .pif | .scr| .vbs | .cmd | .com | .bat | .hta serán eliminados automáticamente por el servicio de correo electrónico sin previo aviso, debido a que este tipo de extensiones son propensas a ser utilizadas para propagación de virus.

XIGA

POLÍTICA DE SERVICIOS TI

Uso de los medios de almacenamiento

Para garantizar la seguridad de la información, todas las computadoras de escritorio y laptops tendrán bloqueados los puertos USB. La transmisión de archivos electrónicos, sólo se podrán realizar por medio del servicio institucional One Drive.

En caso excepcional que se requiera desbloquear puertos USB, por ejemplo: a petición de información por auditores, proveedores, personal interno, entre otros se aplicará procedimiento de "XIGA-A28-P06 Autorización y Revocación de Medios Removibles".

El uso de las distintas carpetas compartidas estará limitado de acuerdo al departamento en el que el colaborador se encuentre, en caso de requerir el acceso a una carpeta de otro departamento, el gerente de este último deberá solicitar el acceso al departamento de Sistemas por medio de correo electrónico, en el cual deberá copiar al jefe inmediato del colaborador.

POLÍTICA DE SERVICIOS TI

Sobre el acceso remoto.

Sólo los usuarios previamente autorizados podrán utilizar los beneficios de la conexión remota, quienes serán responsables del correcto uso del servicio.

Es responsabilidad del usuario con privilegios de acceso a la conexión remota asegurarse que ninguna persona utilice su cuenta, ya que es de uso personal.

Cuando algún usuario requiera el acceso para la conexión remota se deberá llenar el formato Acceso a los aplicativos, el cual deberá estar firmado por el gerente o director del área.

Cuando el permiso de acceso a la conexión remota corresponda a un proveedor externo, la solicitud de acceso a la conexión remota deberá ser solicitada por el personal interno que reciba al proveedor, así mismo se asegurara que este firme el Contrato Acuerdo de Confidencialidad (NDA), el cual resguardara hasta enviarlo al departamento jurídico.

Todas las solicitudes de acceso remoto, deberán ser enviadas al departamento de Sistemas con los formatos establecidos, justificación y periodo de aprovisionamiento, dicha solicitud se canaliza a la Coordinación de Infraestructura y/o Gerencia de TI, quienes autorizarán o denegarán la solicitud.

XIGA

POLÍTICA DE SERVICIOS TI

Acuerdo de Confidencialidad

Acuerdo donde el colaborador o proveedor se compromete a guardar estricta reserva y secreto con relación a la información confidencial de la Organización:

- La información es confidencial será exclusiva y únicamente utilizada para los fines para los cuales fue suministrada y no podrá ser revelada a terceros salvo autorización expresada de la Empresa.

- Cualquier proceso de producción, software, maquinaria, políticas, estrategias de venta y publicidad, cartera de clientes y proveedores, y demás objetos de trabajo, durante el tiempo que dure la relación de trabajo y hasta por un período de tres años, posterior a la terminación de la relación laboral.

XIGA

POLÍTICA DE SERVICIOS TI

Control de Accesos

Todo el personal debe conocer tanto las líneas generales de los procedimientos de seguridad como las implicaciones d su trabajo en el mantenimiento de la seguridad global.

En el documento de Seguridad Física y del Entorno se establece cuales son los accesos Físicos y Lógicos que posee l organización:

Controles de Acceso Físico.

- Entrada y salida de visitas.
- Control de accesos a instalaciones.
- Control de accesos a centro de computo.
- Seguridad de oficinas, recintos e instalaciones.

Cualquier persona que ingrese a las instalaciones debe contar con su gafete de visitante o colaborador, con el fin d identificarse ante los demás y evitar posibles intrusiones.

El acceso a las instalaciones por medio de la huella, así como el registro en el reloj checador, se hace por medio d una solicitud al departamento de Recursos Humanos, los cuales autorizan o deniegan dichos permisos.

XIGA

PROCESOS DE VERIFICACIÓN TI

El departamento de Sistemas tiene facultad para correr Procesos de Verificación como medida para detectar comportamiento de usuarios que no estén en completo apego con estas políticas.

Los resultados obtenidos de dicha verificación quedaran a disposición del departamento de Recursos Humanos y si se detectan incumplimientos con lo dispuesto, se podrán tomar medidas disciplinarias y/o legales de acuerdo a lo estipulado en el Reglamento Interior de Trabajo , Ley Federal del Trabajo y demás normativas aplicables


Información de Contacto:
Mesa de Ayuda
Correo: helpdesk@xiga.com.mx
Telefono Corto: 334(María Elena) 499 (Eduardo Cazares) 790(Valeria)
Extension: 5083(María Elena),5070 (Valeria)
XIGA.MX