Política Específica sobre los Controles Organizacionales

1. Objetivo

Establecer los controles organizacionales necesarios para proteger la información y los activos tecnológicos de la empresa de telecomunicaciones, garantizando su confidencialidad, integridad y disponibilidad, y cumpliendo con los requisitos legales, regulatorios y contractuales aplicables.

2. Alcance

Esta política aplica a todos los empleados, contratistas, proveedores y terceros que accedan, procesen o gestionen información de la organización.

3. Principios Generales

- **Gobernanza de la Seguridad de la Información:** Se establecerá una estructura de gobernanza clara, con roles y responsabilidades definidos para la gestión de la seguridad de la información.
- **Compromiso de la Alta Dirección:** La alta dirección demostrará liderazgo y compromiso mediante la asignación de recursos, la aprobación de políticas y la supervisión del cumplimiento.
- **Gestión de Riesgos:** Se implementará un proceso continuo de identificación, evaluación y tratamiento de riesgos relacionados con la seguridad de la información.

4. Controles Organizacionales

4.1. Roles y Responsabilidades

- Se designará un Responsable de Seguridad de la Información (CISO) con autoridad para implementar y supervisar el SGSI.
- Cada área funcional deberá nombrar un Responsable de Seguridad Local para coordinar acciones específicas.

4.2. Concienciación y Formación

- Todos los empleados recibirán formación obligatoria en seguridad de la información al ingresar y de forma periódica.
- Se realizarán campañas de concienciación para reforzar buenas prácticas.

4.3. Gestión de Proveedores

- Se evaluará la seguridad de los proveedores antes de su contratación.
- Los contratos incluirán cláusulas específicas de seguridad de la información y cumplimiento normativo.

4.4. Gestión de Incidentes

- Se establecerá un proceso formal para la notificación, análisis y respuesta a incidentes de seguridad.
- Se mantendrá un registro actualizado de todos los incidentes y acciones correctivas.

4.5. Cumplimiento Legal y Regulatorio

- Se garantizará el cumplimiento de normativas como la Ley Federal de Protección de Datos Personales, normas del IFT, y otras aplicables.
- Se realizarán auditorías internas periódicas para verificar el cumplimiento.

4.6. Seguridad en Proyectos y Cambios

- Todos los proyectos tecnológicos deberán incluir una evaluación de impacto en la seguridad.
- Los cambios en sistemas críticos requerirán revisión y aprobación por el área de seguridad.

5. Revisión y Actualización

Esta política será revisada al menos una vez al año o cuando ocurran cambios significativos en el entorno tecnológico, normativo o de negocio.

6. Sanciones

El incumplimiento de esta política podrá dar lugar a medidas disciplinarias, incluyendo la terminación del contrato laboral o comercial, según la gravedad del caso.

Política Específica sobre los Controles para la Gestión del Personal

1. Objetivo
Establecer los controles necesarios para gestionar de forma segura al personal antes, durante y después de su relación laboral con la empresa, con el fin de proteger los activos de información y reducir los riesgos asociados al factor humano.

2. Alcance
Esta política aplica a todos los empleados, contratistas, consultores, proveedores y terceros que tengan acceso a los sistemas, redes o información de la organización.

3. Principios Generales
- La seguridad de la información es una responsabilidad compartida por todo el personal.
- Se establecerán controles específicos en cada etapa del ciclo de vida del empleado.
- Se promoverá una cultura de seguridad mediante formación, concienciación y supervisión continua.

4. Controles por Etapa del Ciclo de Vida del Personal

4.1. Antes de la Vinculación
- **Verificación de antecedentes:** Se realizarán verificaciones de antecedentes laborales, académicos y, cuando aplique, penales, conforme a la legislación vigente.
- **Cláusulas contractuales:** Todos los contratos incluirán cláusulas de confidencialidad, uso aceptable de la información y cumplimiento de políticas de seguridad.

4.2. Durante la Relación Laboral
- **Formación en seguridad:** Todo el personal deberá completar programas de formación inicial y continua en seguridad de la información.
- **Acceso basado en roles:** El acceso a sistemas e información será otorgado según el principio de mínimo privilegio y necesidad de conocer.
- **Supervisión y cumplimiento:** Se realizarán auditorías y revisiones periódicas para asegurar el cumplimiento de las políticas de seguridad.

4.3. Terminación o Cambio de Rol
- **Revocación de accesos:** Todos los accesos físicos y lógicos serán revocados de forma inmediata al finalizar la relación laboral o al cambiar de rol.
- **Devolución de activos:** El personal deberá devolver todos los activos de la empresa (dispositivos, credenciales, documentos, etc.).
- **Recordatorio de obligaciones:** Se recordará al empleado sus obligaciones post-empleo, especialmente en cuanto a la confidencialidad.

5. Responsabilidades

- **Recursos Humanos:** Coordinará los procesos de incorporación, formación y desvinculación del personal.
- **Seguridad de la Información:** Definirá los controles técnicos y realizará auditorías de cumplimiento.
- **Líderes de Área:** Supervisarán el cumplimiento de esta política en sus respectivos equipos.

6. Revisión y Actualización

Esta política será revisada anualmente o cuando se produzcan cambios significativos en la legislación, estructura organizacional o tecnología utilizada.

7. Sanciones

El incumplimiento de esta política podrá derivar en sanciones disciplinarias, incluyendo la terminación del contrato laboral o comercial, conforme a la normativa interna y legal aplicable.

Política Específica sobre los Controles para la Gestión de Activos

1. Objetivo

Establecer los lineamientos y controles necesarios para identificar, clasificar, proteger y gestionar adecuadamente los activos de información de la organización durante todo su ciclo de vida.

2. Alcance

Esta política aplica a todos los activos de información, incluyendo hardware, software, datos, documentación, servicios y recursos humanos, que sean propiedad de la empresa o estén bajo su custodia.

3. Principios Generales

- Todos los activos deben ser inventariados, clasificados y gestionados de acuerdo con su valor, criticidad y sensibilidad.
- La protección de los activos es responsabilidad de todos los usuarios que los utilicen o administren.
- Se debe garantizar la trazabilidad y control de los activos durante su adquisición, uso, mantenimiento y disposición final.

4. Controles para la Gestión de Activos

4.1. Inventario de Activos

- Se mantendrá un inventario actualizado de todos los activos relevantes para la seguridad de la información.
- Cada activo deberá tener un propietario claramente asignado, responsable de su protección y uso adecuado.

4.2. Clasificación de Activos

- Los activos serán clasificados según su nivel de sensibilidad: Público, Interno
- Confidencial y Restringido.
- La clasificación determinará los controles de acceso, almacenamiento, transmisión y eliminación.

4.3. Uso Aceptable de los Activos

- Se establecerán lineamientos claros sobre el uso aceptable de dispositivos, sistemas y redes.
- El uso indebido de activos podrá ser sancionado conforme a las políticas internas.

4.4. Protección de Activos

- Se aplicarán controles físicos y lógicos para proteger los activos contra accesos no autorizados, pérdida, daño o robo.
- Los activos críticos deberán contar con medidas de respaldo, redundancia y monitoreo.

4.5. Transferencia y Movilidad

- La transferencia de activos (física o digital) deberá realizarse bajo mecanismos seguros y autorizados.
- Los dispositivos móviles y portátiles deberán contar con cifrado y autenticación robusta.

4.6. Eliminación y Disposición Final

- Los activos que ya no sean necesarios deberán ser eliminados de forma segura, garantizando la destrucción de la información sensible.
- Se documentará el proceso de baja y destrucción de activos.

5. Responsabilidades

- **Área de TI:** Mantener el inventario de activos tecnológicos y aplicar controles técnicos.
- **Usuarios Finales:** Usar los activos conforme a las políticas y reportar cualquier anomalía.
- **Seguridad de la Información:** Supervisar la clasificación, protección y cumplimiento de esta política.

6. Revisión y Actualización

Esta política será revisada anualmente o cuando se introduzcan nuevos tipos de activos, tecnologías o amenazas relevantes.

7. Sanciones

El incumplimiento de esta política podrá derivar en sanciones disciplinarias, incluyendo la terminación del contrato laboral o comercial, conforme a la normativa interna y legal aplicable.

Política Específica sobre los Controles para la Gestión de los Accesos

1. Objetivo

Establecer los lineamientos y controles necesarios para gestionar de forma segura el acceso a los sistemas, redes, aplicaciones y datos de la organización, garantizando que solo las personas autorizadas tengan acceso a la información adecuada, en el momento adecuado y por las razones correctas.

2. Alcance

Esta política aplica a todos los empleados, contratistas, proveedores y terceros que requieran acceso a los recursos de información de la empresa, ya sea de forma local o remota.

3. Principios Generales

- El acceso a los activos de información debe estar basado en el principio de mínimo privilegio y necesidad de conocer.
- Todos los accesos deben ser autenticados, autorizados, registrados y monitoreados.
- Se deben aplicar controles diferenciados según el nivel de sensibilidad de la información o sistema.

4. Controles de Gestión de Accesos

4.1. Gestión de Identidades

- Cada usuario tendrá una identidad única para acceder a los sistemas.
- No se permitirá el uso compartido de cuentas, salvo en casos excepcionales y controlados.

4.2. Autenticación

- Se implementará autenticación multifactor (MFA) para accesos a sistemas críticos o remotos.
- Las contraseñas deberán cumplir con requisitos mínimos de complejidad y periodicidad de cambio.

4.3. Asignación y Revisión de Accesos

- Los accesos serán otorgados previa autorización formal del responsable del área.
- Se realizarán revisiones periódicas de accesos para detectar privilegios innecesarios o inadecuados.

4.4. Control de Accesos a la Red y Sistemas

- Se aplicarán listas de control de acceso (ACLs), firewalls y segmentación de red para limitar el acceso a recursos.
- Los accesos administrativos estarán restringidos y sujetos a monitoreo reforzado.

4.5. Acceso de Terceros

- Los accesos de terceros deberán estar justificados, autorizados y limitados en tiempo y alcance.
- Se utilizarán conexiones seguras (VPN, túneles cifrados) y se registrarán todas las actividades.

4.6. Desactivación de Accesos

- Los accesos serán revocados de forma inmediata al finalizar la relación laboral o contractual.
- Se mantendrá un registro de las altas, modificaciones y bajas de accesos.

5. Responsabilidades

- **Área de TI:** Administrar las plataformas de control de acceso y ejecutar las solicitudes autorizadas.
- **Responsables de Área:** Validar y aprobar los accesos requeridos por su personal.
- **Usuarios:** Usar sus credenciales de forma segura y reportar cualquier anomalía.

6. Revisión y Actualización

Esta política será revisada anualmente o cuando se introduzcan nuevos sistemas, tecnologías o amenazas relevantes.

7. Sanciones

El incumplimiento de esta política podrá derivar en sanciones disciplinarias, incluyendo la terminación del contrato laboral o comercial, conforme a la normativa interna y legal aplicable.

Política Específica sobre los Controles Físicos

1. Objetivo
Establecer los controles físicos necesarios para proteger las instalaciones, equipos y activos de información de la organización frente a accesos no autorizados, daños, robos o interferencias.

2. Alcance
Esta política aplica a todas las instalaciones físicas de la empresa, incluyendo oficinas, centros de datos, salas técnicas, almacenes y cualquier otro sitio donde se ubiquen activos de información.

3. Principios Generales
- El acceso físico a las instalaciones debe estar controlado, monitoreado y restringido según el nivel de criticidad del área.
- Se deben implementar medidas preventivas y de detección para minimizar los riesgos físicos.
- Todo el personal debe conocer y cumplir las normas de seguridad física establecidas.

4. Controles Físicos Específicos

4.1. Zonificación de Seguridad
- Las instalaciones se dividirán en zonas con distintos niveles de seguridad: públicas, restringidas y críticas.
- El acceso a zonas críticas (como centros de datos) estará limitado a personal autorizado y registrado.

4.2. Control de Acceso Físico
- Se utilizarán mecanismos de autenticación física como tarjetas de proximidad, biometría o códigos de acceso.
- Se mantendrán registros de entradas y salidas, especialmente en áreas sensibles.

4.3. Protección de Equipos
- Los equipos críticos deberán estar ubicados en áreas seguras, con protección contra incendios, humedad, temperatura extrema y sabotaje.
- Se evitará el acceso físico directo a servidores, switches, routers y otros dispositivos de red.

4.4. Supervisión y Monitoreo
- Se instalarán sistemas de videovigilancia (CCTV) en puntos estratégicos, con almacenamiento seguro de grabaciones.
- Se realizarán rondas de seguridad y auditorías físicas periódicas.

4.5. Visitantes y Terceros

- Toda visita deberá ser registrada, identificada y acompañada por personal autorizado.
- Los visitantes no podrán acceder a zonas críticas sin autorización previa y supervisión directa.

4.6. Protección contra Desastres

- Las instalaciones deberán contar con sistemas de detección y extinción de incendios, así como planes de evacuación y continuidad operativa.
- Se realizarán simulacros periódicos de emergencia.

4.7. Eliminación Segura de Equipos

Los equipos que contengan información sensible deberán ser eliminados o reciclados de forma segura, asegurando la destrucción de los datos.

5. Responsabilidades

- **Área de Seguridad Física o Infraestructura: I**mplementar y mantener los controles físicos.
- **Seguridad de la Información:** Coordinar con infraestructura para asegurar la protección de activos críticos.
- **Todo el Personal:** Cumplir con las normas de acceso y reportar cualquier anomalía.

6. Revisión y Actualización

Esta política será revisada anualmente o cuando se realicen cambios significativos en las instalaciones o en el entorno de amenazas.

7. Sanciones

El incumplimiento de esta política podrá derivar en sanciones disciplinarias, incluyendo la terminación del contrato laboral o comercial, conforme a la normativa interna y legal aplicable.

Política Específica sobre los Controles para la Seguridad Operativa

1. Objetivo
Establecer los controles necesarios para garantizar la operación segura, confiable y eficiente de los sistemas de información, minimizando el riesgo de interrupciones, errores, accesos no autorizados y pérdida de datos.

2. Alcance
Esta política aplica a todos los procesos operativos relacionados con la gestión de sistemas, redes, aplicaciones, bases de datos y servicios tecnológicos de la organización.

3. Principios Generales
- La operación de los sistemas debe estar documentada, controlada y monitoreada.
- Se deben aplicar controles preventivos, detectivos y correctivos para asegurar la continuidad y seguridad de las operaciones.
- Todo cambio en el entorno operativo debe ser gestionado de forma controlada.

4. Controles de Seguridad Operativa

4.1. Gestión de Cambios
- Todo cambio en sistemas, aplicaciones o infraestructura debe ser evaluado, aprobado, probado y documentado antes de su implementación.
- Se mantendrá un registro de cambios con su justificación, impacto y responsables.

4.2. Gestión de la Capacidad
- Se monitoreará el uso de recursos tecnológicos para anticipar necesidades de capacidad y evitar interrupciones.
- Se realizarán análisis de tendencias y planificación de crecimiento.

4.3. Protección contra Malware
- Se implementarán soluciones de protección contra malware en todos los dispositivos y servidores.
- Se actualizarán regularmente las firmas y se realizarán escaneos automáticos.

4.4. Copias de Seguridad
- Se realizarán respaldos periódicos de la información crítica, con pruebas regulares de restauración.
- Las copias de seguridad estarán protegidas contra accesos no autorizados y almacenadas en ubicaciones seguras.

4.5. Monitoreo y Registro

- Se habilitará el registro de eventos relevantes (logs) en sistemas críticos.
- Se implementarán herramientas de monitoreo para detectar anomalías, accesos indebidos o fallos operativos.

4.6. Segregación de Ambientes

- Se mantendrán separados los entornos de desarrollo, pruebas y producción para evitar interferencias y riesgos de seguridad.
- El acceso entre entornos estará controlado y justificado.

4.7. Gestión de Vulnerabilidades

- Se realizarán escaneos periódicos de vulnerabilidades y se aplicarán parches de seguridad conforme a un calendario definido.
- Las vulnerabilidades críticas deberán ser atendidas de forma inmediata.

5. Responsabilidades

- **Área de Operaciones de TI:** Ejecutar y mantener los controles operativos definidos.
- **Seguridad de la Información:** Supervisar la correcta implementación de los controles y realizar auditorías.
- **Usuarios Técnicos:** Cumplir con los procedimientos establecidos y reportar cualquier desviación.

6. Revisión y Actualización

Esta política será revisada anualmente o cuando se introduzcan nuevas tecnologías, procesos o amenazas relevantes.

7. Sanciones

El incumplimiento de esta política podrá derivar en sanciones disciplinarias, incluyendo la terminación del contrato laboral o comercial, conforme a la normativa interna y legal aplicable.

Política Específica sobre los Controles en las Telecomunicaciones

1. Objetivo
Establecer los controles necesarios para proteger la infraestructura de telecomunicaciones de la organización, garantizando la confidencialidad, integridad y disponibilidad de la información transmitida a través de redes internas y externas.

2. Alcance
Esta política aplica a todas las redes de telecomunicaciones utilizadas por la empresa, incluyendo redes LAN, WAN, VPN, enlaces inalámbricos, redes móviles, enlaces satelitales y cualquier otro medio de transmisión de datos.

3. Principios Generales
- Las telecomunicaciones deben estar protegidas contra accesos no autorizados, interceptaciones, alteraciones y pérdidas de servicio.
- Se deben implementar controles técnicos y administrativos para asegurar la transmisión segura de la información.
- Toda conexión con redes externas debe estar debidamente autorizada, controlada y monitoreada.

4. Controles en las Telecomunicaciones

4.1. Seguridad de la Infraestructura de Red
- Se utilizarán firewalls, sistemas de detección y prevención de intrusos (IDS/IPS), y segmentación de red para proteger los perímetros.
- Las redes críticas estarán separadas lógicamente mediante VLANs o físicamente cuando sea necesario.
-

4.2. Cifrado de Comunicaciones
- Toda transmisión de información sensible deberá realizarse mediante protocolos seguros (por ejemplo, TLS, IPsec, SSH, VPN).
- Se utilizarán certificados digitales válidos y actualizados para garantizar la autenticidad de las conexiones.

4.3. Gestión de Conexiones Remotas
- El acceso remoto a la red corporativa deberá realizarse exclusivamente mediante VPNs seguras y autenticación multifactor.
- Se registrarán y monitorearán todas las sesiones remotas.

4.4. Supervisión y Monitoreo de Redes

- Se implementarán herramientas de monitoreo de tráfico y análisis de comportamiento para detectar actividades anómalas.
- Se mantendrán registros de eventos de red para auditoría y respuesta a incidentes.

4.5. Protección contra Interferencias y Sabotaje

- Las instalaciones de telecomunicaciones deberán estar protegidas físicamente contra accesos no autorizados y condiciones ambientales adversas.
- Se aplicarán controles de redundancia y tolerancia a fallos en enlaces críticos.

4.6. Gestión de Proveedores de Telecomunicaciones

- Los proveedores de servicios de red deberán cumplir con los requisitos de seguridad establecidos por la organización.
- Se evaluará periódicamente el desempeño y cumplimiento de los acuerdos de nivel de servicio (SLA).

5. Responsabilidades

- **Área de Redes y Telecomunicaciones:** Implementar y mantener los controles técnicos definidos.
- **Seguridad de la Información:** Supervisar el cumplimiento de esta política y coordinar auditorías.
- **Usuarios:** Utilizar los servicios de red conforme a las políticas y reportar cualquier anomalía.

6. Revisión y Actualización

Esta política será revisada anualmente o cuando se introduzcan nuevas tecnologías, amenazas o cambios en la infraestructura de red.

7. Sanciones

El incumplimiento de esta política podrá derivar en sanciones disciplinarias, incluyendo la terminación del contrato laboral o comercial, conforme a la normativa interna y legal aplicable.

Política Específica sobre los Controles para la Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

1. Objetivo

Establecer los controles necesarios para garantizar que los sistemas de información adquiridos, desarrollados o modificados por la organización cumplan con los requisitos de seguridad desde su concepción hasta su retiro, minimizando riesgos y asegurando la continuidad operativa.

2. Alcance

Esta política aplica a todos los proyectos de adquisición, desarrollo interno, mantenimiento o mejora de sistemas de información, incluyendo software, aplicaciones, bases de datos y componentes tecnológicos utilizados por la empresa.

3. Principios Generales

- La seguridad debe integrarse desde las etapas iniciales del ciclo de vida del sistema.
- Todo sistema debe cumplir con los requisitos de seguridad, privacidad, cumplimiento normativo y continuidad del negocio.
- Se deben aplicar prácticas de desarrollo seguro y pruebas rigurosas antes de la puesta en producción.

4. Controles para Adquisición, Desarrollo y Mantenimiento

4.1. Requisitos de Seguridad

- Los requisitos de seguridad deben definirse y documentarse desde la fase de análisis del sistema.
- Se deben considerar aspectos como autenticación, autorización, cifrado, trazabilidad y protección de datos personales.

4.2. Evaluación de Proveedores y Soluciones

- Toda solución adquirida externamente debe ser evaluada en términos de seguridad, cumplimiento y compatibilidad.
- Los contratos con proveedores deben incluir cláusulas de seguridad, auditoría y soporte.

4.3. Desarrollo Seguro

- Se adoptarán metodologías de desarrollo seguro (como DevSecOps) y se capacitará al personal técnico en prácticas seguras de codificación.
- Se utilizarán herramientas de análisis estático y dinámico de código para detectar vulnerabilidades.

4.4. Pruebas de Seguridad

- Antes de la implementación, los sistemas deben someterse a pruebas de penetración, análisis de vulnerabilidades y validación de controles.
- Se documentarán los resultados y se corregirán las debilidades detectadas.

4.5. Gestión de Cambios

- Toda modificación a sistemas existentes deberá seguir un proceso formal de gestión de cambios, con evaluación de impacto en la seguridad.
- Se mantendrá un historial de versiones y cambios aplicados.

4.6. Protección de Datos en Desarrollo y Pruebas

- No se utilizarán datos reales de clientes en entornos de desarrollo o pruebas, salvo que estén debidamente anonimizados o cifrados.
- El acceso a estos entornos estará restringido y monitoreado.

4.7. Mantenimiento Seguro

- Las actualizaciones, parches y mejoras deberán ser evaluadas y aplicadas de forma controlada.
- Se establecerán ventanas de mantenimiento y procedimientos de respaldo antes de cualquier intervención.

5. Responsabilidades

- **Área de Desarrollo y Tecnología:** Aplicar los controles definidos en cada fase del ciclo de vida del sistema.
- **Seguridad de la Información:** Validar los requisitos de seguridad, realizar auditorías y pruebas de cumplimiento.
- **Usuarios Funcionales:** Participar en la definición de requisitos y pruebas de aceptación.

6. Revisión y Actualización

Esta política será revisada anualmente o cuando se introduzcan nuevas tecnologías, metodologías o amenazas relevantes.

7. Sanciones

El incumplimiento de esta política podrá derivar en sanciones disciplinarias, incluyendo la terminación del contrato laboral o comercial, conforme a la normativa interna y legal aplicable.

Política Específica sobre los Controles para la Gestión de Proveedores

1. Objetivo

Establecer los controles necesarios para gestionar de forma segura y eficaz la relación con proveedores y terceros que tengan acceso a los activos de información, sistemas o servicios críticos de la organización, asegurando el cumplimiento de los requisitos de seguridad, legales y contractuales.

2. Alcance

Esta política aplica a todos los proveedores, contratistas, socios tecnológicos y terceros que presten servicios, desarrollen soluciones o tengan acceso a información o infraestructura de la empresa.

3. Principios Generales

- La seguridad de la información debe ser considerada desde la selección del proveedor hasta la finalización del contrato.
- Los proveedores deben cumplir con los estándares de seguridad definidos por la organización.
- Se deben establecer mecanismos de evaluación, monitoreo y control continuo de los riesgos asociados a terceros.

4. Controles para la Gestión de Proveedores

4.1. Evaluación y Selección de Proveedores

- Antes de su contratación, los proveedores serán evaluados en función de su capacidad técnica, cumplimiento normativo y madurez en seguridad de la información.
- Se priorizarán proveedores que cuenten con certificaciones reconocidas (ISO 27001, SOC 2, etc.).

4.2. Contratos con Cláusulas de Seguridad

- Todos los contratos deberán incluir cláusulas específicas sobre: Confidencialidad y protección de datos.
- Cumplimiento de políticas de seguridad.
- Derechos de auditoría.
- Notificación de incidentes de seguridad.
- Responsabilidades legales y contractuales.

4.3. Clasificación de Proveedores

- Los proveedores serán clasificados según el nivel de riesgo que representan para la organización (alto, medio, bajo).
- Esta clasificación determinará la frecuencia y profundidad de las evaluaciones de seguridad.

4.4. Monitoreo y Revisión Continua

- Se realizarán revisiones periódicas del desempeño y cumplimiento de los proveedores críticos.
- Se podrán aplicar auditorías, revisiones de seguridad y análisis de cumplimiento contractual.

4.5. Gestión de Accesos de Terceros

- El acceso de proveedores a sistemas o información deberá ser autorizado, limitado en tiempo y alcance, y monitoreado.
- Al finalizar la relación contractual, se revocarán todos los accesos y se recuperarán los activos entregados.

4.6. Gestión de Incidentes con Proveedores

Los proveedores deberán notificar de inmediato cualquier incidente de seguridad que pueda afectar a la organización.
Se establecerán procedimientos conjuntos de respuesta y mitigación.

5. Responsabilidades

- **Área de Compras o Contratación:** Coordinar la evaluación y formalización de contratos con proveedores.
- **Seguridad de la Información:** Definir requisitos de seguridad, evaluar riesgos y realizar auditorías.
- **Áreas Usuarias:** Supervisar el cumplimiento de los acuerdos y reportar desviaciones.

6. Revisión y Actualización

Esta política será revisada anualmente o cuando se introduzcan nuevos tipos de servicios, proveedores o cambios regulatorios relevantes.

7. Sanciones

El incumplimiento de esta política podrá derivar en sanciones contractuales, suspensión de servicios o terminación de la relación comercial, conforme a lo establecido en los acuerdos firmados.

Política Específica sobre los Controles para la Gestión de Incidentes de Seguridad de la Información

1. Objetivo

Establecer los lineamientos y controles necesarios para la detección, reporte, análisis, respuesta, documentación y aprendizaje de los incidentes de seguridad de la información, con el fin de minimizar su impacto y prevenir su recurrencia.

2. Alcance

Esta política aplica a todos los empleados, contratistas, proveedores y terceros que utilicen, administren o tengan acceso a los sistemas de información, redes, datos o servicios tecnológicos de la organización.

3. Principios Generales

- Todo incidente de seguridad debe ser reportado de forma inmediata y gestionado conforme a procedimientos establecidos.
- La organización debe contar con un equipo especializado para la gestión de incidentes (CSIRT o equivalente).
- Se debe fomentar una cultura de reporte proactivo y sin represalias.

4. Controles para la Gestión de Incidentes

4.1. Clasificación de Incidentes

- Los incidentes se clasificarán según su naturaleza, impacto y urgencia (por ejemplo: acceso no autorizado, malware, fuga de información, denegación de servicio, etc.).
- Se establecerán niveles de severidad para priorizar la respuesta.

4.2. Detección y Reporte

- Se implementarán mecanismos automáticos y manuales para la detección de incidentes (SIEM, IDS/IPS, monitoreo de logs).
- Todo el personal deberá reportar incidentes al canal designado (correo, sistema de tickets, línea directa).

4.3. Respuesta y Contención

- El equipo de respuesta a incidentes deberá actuar de forma inmediata para contener, mitigar y erradicar el incidente.
- Se documentarán todas las acciones tomadas y se preservará la evidencia digital cuando sea necesario.

4.4. Análisis y Recuperación

- Se realizará un análisis técnico y forense del incidente para determinar su causa raíz.
- Se restaurarán los servicios afectados de forma segura y controlada.

4.5. Comunicación y Escalamiento

- Se establecerán protocolos de comunicación interna y externa, incluyendo notificación a autoridades regulatorias si aplica.
- Los incidentes críticos deberán ser escalados a la alta dirección y al Comité de Seguridad.

4.6. Lecciones Aprendidas y Mejora Continua

- Después de cada incidente, se realizará una reunión de revisión post-mortem.
- Se actualizarán los controles, procedimientos y políticas según las lecciones aprendidas.

5. Responsabilidades

- **Usuarios Finales:** Reportar cualquier incidente o comportamiento sospechoso.
- **Equipo de Seguridad de la Información:** Coordinar la gestión de incidentes, análisis, respuesta y documentación.
- **Áreas Técnicas:** Apoyar en la contención, recuperación y mejora de controles.
- **Alta Dirección:** Tomar decisiones estratégicas en incidentes de alto impacto.

6. Revisión y Actualización

Esta política será revisada anualmente o cuando se produzcan incidentes significativos que requieran ajustes en los controles establecidos.

7. Sanciones

El incumplimiento de esta política, incluyendo la omisión de reporte de incidentes, podrá derivar en sanciones disciplinarias conforme a la normativa interna y legal aplicable.

Política Específica sobre los Controles para la Gestión de la Continuidad del Negocio

1. Objetivo

Establecer los controles necesarios para garantizar la continuidad de las operaciones críticas de la organización ante eventos disruptivos, minimizando el impacto en los servicios, la reputación y el cumplimiento normativo.

2. Alcance

Esta política aplica a todas las áreas, procesos, sistemas y recursos críticos de la organización, incluyendo personal, infraestructura, tecnología, proveedores y servicios esenciales.

3. Principios Generales

- La continuidad del negocio es responsabilidad de toda la organización, con liderazgo desde la alta dirección.
- Se deben identificar los procesos críticos y establecer planes de continuidad y recuperación.
- La preparación, respuesta y recuperación deben ser probadas y mejoradas de forma continua.

4. Controles para la Gestión de la Continuidad del Negocio

4.1. Análisis de Impacto al Negocio (BIA)

- Se realizará un análisis de impacto para identificar procesos críticos, dependencias, tiempos máximos de interrupción tolerables (RTO) y niveles mínimos aceptables de operación (RPO).
- El BIA será revisado periódicamente o ante cambios significativos.

4.2. Evaluación de Riesgos

- Se identificarán amenazas que puedan afectar la continuidad del negocio (desastres naturales, fallas tecnológicas, ciberataques, etc.).
- Se establecerán medidas de mitigación y contingencia.

4.3. Planes de Continuidad del Negocio (BCP)

- Se desarrollarán y mantendrán planes documentados que incluyan procedimientos de respuesta, recuperación y restauración de operaciones.
- Los planes deberán estar disponibles, actualizados y accesibles para los responsables.

4.4. Planes de Recuperación ante Desastres (DRP)

- Se establecerán planes específicos para la recuperación de sistemas de TI, incluyendo respaldos, sitios alternos y procedimientos técnicos.
- Se definirán roles, responsabilidades y tiempos de recuperación.

4.5. Pruebas y Ejercicios

- Se realizarán pruebas periódicas de los planes de continuidad y recuperación, incluyendo simulacros y ejercicios de escritorio.
- Se documentarán los resultados y se aplicarán mejoras según las lecciones aprendidas.

4.6. Capacitación y Concienciación

- El personal clave será capacitado en sus roles dentro del BCP y DRP.
- Se promoverá una cultura organizacional orientada a la resiliencia operativa.

4.7. Gestión de Proveedores Críticos

- Se evaluará la capacidad de los proveedores estratégicos para mantener la continuidad de sus servicios.
- Los contratos deberán incluir cláusulas de continuidad y recuperación.

5. Responsabilidades

- **Alta Dirección**: Aprobar y respaldar el programa de continuidad del negocio.
- **Oficial de Continuidad del Negocio:** Coordinar el desarrollo, mantenimiento y pruebas de los planes.
- **Responsables de Área:** Identificar procesos críticos y participar en la implementación de los planes.
- **Todo el Personal:** Conocer los procedimientos básicos de respuesta ante incidentes y emergencias.

6. Revisión y Actualización

Esta política será revisada anualmente o cuando se produzcan cambios significativos en los procesos, estructura organizacional o entorno de amenazas.

7. Sanciones

El incumplimiento de esta política podrá derivar en sanciones disciplinarias, conforme a la normativa interna y legal aplicable.

Política Específica sobre los Controles para la Gestión de Cumplimiento

1. Objetivo

Establecer los controles necesarios para asegurar que la organización cumpla con todas las obligaciones legales, regulatorias, contractuales y normativas relacionadas con la seguridad de la información, la protección de datos y la operación del negocio.

2. Alcance

Esta política aplica a todas las áreas, procesos, empleados, contratistas y terceros que participen en actividades que puedan estar sujetas a requisitos de cumplimiento en el contexto de la organización.

3. Principios Generales

- El cumplimiento es una responsabilidad compartida que debe integrarse en todos los niveles de la organización.
- Se deben identificar, documentar y monitorear todas las obligaciones aplicables.
- El incumplimiento puede generar riesgos legales, financieros y reputacionales significativos.

4. Controles para la Gestión de Cumplimiento

4.1. Identificación de Requisitos

- Se mantendrá un inventario actualizado de leyes, regulaciones, normas y contratos aplicables a la organización (por ejemplo: Ley Federal de Protección de Datos Personales, regulaciones del IFT, ISO/IEC 27001).
- Se asignarán responsables para cada tipo de obligación.

4.2. Evaluación de Cumplimiento

- Se realizarán evaluaciones periódicas para verificar el cumplimiento de los requisitos identificados.
- Se documentarán los hallazgos y se establecerán planes de acción correctiva.

4.3. Auditorías Internas y Externas

- Se llevarán a cabo auditorías internas de seguridad de la información y cumplimiento normativo al menos una vez al año.
- Se facilitará la realización de auditorías externas por parte de autoridades o certificadores cuando corresponda.

4.4. Gestión de Incumplimientos

- Todo incumplimiento detectado será registrado, analizado y tratado mediante acciones correctivas y preventivas.
- Se notificará a las autoridades competentes cuando así lo exija la normativa aplicable.

4.5. Concienciación y Capacitación

- El personal será capacitado regularmente en temas de cumplimiento, incluyendo protección de datos, ética, seguridad de la información y normativas sectoriales.
- Se promoverá una cultura de cumplimiento mediante campañas internas.

4.6. Supervisión y Reportes

- Se establecerán mecanismos de monitoreo continuo y reportes periódicos a la alta dirección sobre el estado del cumplimiento.
- Se utilizarán indicadores clave de cumplimiento (KPIs) para evaluar el desempeño.

5. Responsabilidades

- Oficial de Cumplimiento o Legal: Coordinar la identificación y seguimiento de obligaciones legales y regulatorias.
- Seguridad de la Información: Asegurar el cumplimiento de normas técnicas y políticas internas.
- Responsables de Área: Implementar controles específicos y colaborar en auditorías.
- Todo el Personal: Cumplir con las políticas y reportar cualquier posible incumplimiento.

6. Revisión y Actualización

Esta política será revisada anualmente o cuando se produzcan cambios en el marco legal, regulatorio o contractual que afecten a la organización.

7. Sanciones

El incumplimiento de esta política podrá derivar en sanciones disciplinarias, contractuales o legales, conforme a la normativa interna y externa aplicable.