PO_POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICA

CONTENIDO

1. Generales.

Aplicación de políticas.

Con el objetivo de garantizar la confidencialidad, integridad, disponibilidad y legalidad de la información propia o de terceros que ostenta nuestra organización para efecto de llevar a cabo sus operaciones, la Alta Dirección (Consejo Directivo) de Prospectiva en Tecnología e integradora de sistemas S.A. de C.V., establece las presentes Políticas de seguridad de la información y se compromete a revisar, comunicar y proveer los recursos necesarios para su correcta aplicación.
Estas medidas deberán aplicarse sin excepción por todos los usuarios internos y externos de todos los niveles, quienes tienen el deber de conocer, cumplir y hacer cumplir las mismas por el personal o tercero a su cargo.
El Representante del Sistema de Gestión Integral tiene como objetivo principal, definir, implementar, revisar y en su caso actualizar, los procesos necesarios para el cumplimiento de esta política.

Exclusiones.

Cualquier exclusión o excepción a las políticas deberá ser documentada como un incidente de seguridad y autorizada por el responsable de seguridad de la información, previo análisis de los riesgos que se deriven de la excepción.

Revisión de políticas.

Las Políticas deberán ser revisadas al menos una vez al año o a menor periodicidad siempre que se produzcan modificaciones significativas en los procesos o infraestructura y de ser necesario, actualizadas por el responsable de Seguridad de la Información, quien deberá presentar los cambios propuestos a la Consejo Directivo por medio del procedimiento **PR_Gestión de cambios**.
Durante la revisión de Políticas de seguridad de la información, el responsable deberá garantizar que estas mantienen su idoneidad, adecuación y eficacia con respecto a los riesgos identificados para el negocio.

Comunicación de políticas.

- El responsable de Seguridad de la Información deberá asegurarse de la publicación, difusión, capacitación, evaluación del conocimiento y aplicación de las Políticas de seguridad de la información por parte del personal interno.
- El personal responsable de las interacciones con terceras partes para el intercambio de información sensible propia o de terceros, deberá asegurarse de dar a conocer a los terceros las Políticas de seguridad de la información aplicables.
- La comunicación de las políticas de seguridad de la información deberá ser utilizando los medios autorizados para tal fin, pudiendo estos ser:
  - Copia física controlada
  - Copia digital controlada

- Publicación web
- Redes sociales

Autorización.

- Toda adición, modificación o supresión a las Políticas de Seguridad de la Información, deberán ser propuestas mediante el procedimiento **PR_Control de cambios** y presentadas a la alta dirección para su autorización.
- La autorización de dichas políticas podrá ser emitida por cualquiera de los siguientes métodos:
  - Firma autógrafa en copia impresa.
  - Minuta de revisión por la dirección.

Estructura.

Con la finalidad de definir, mantener y mejorar oportunamente las políticas de seguridad de la información dentro de la organización, se designan los siguientes roles y responsabilidades que podrán ser ocupados por una misma persona o bien distribuidos por medio de un Comité de Seguridad.

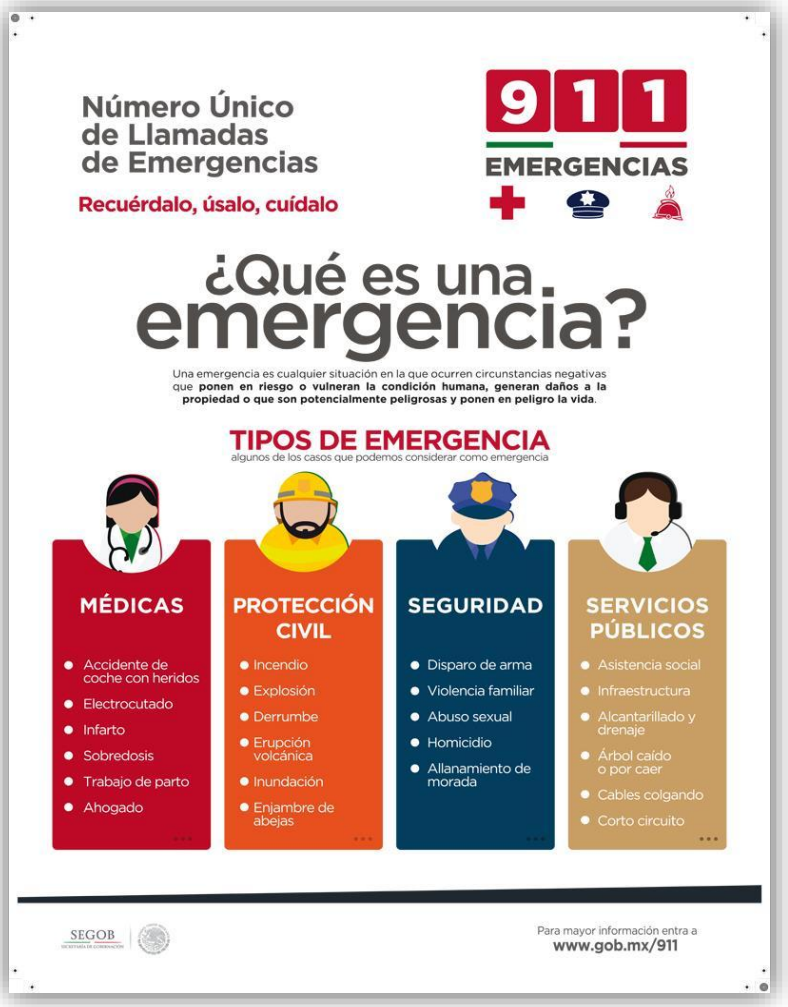
Rol	Responsabilidad	Designado
Oficial de seguridad física	Definir, mantener y mejorar las políticas, procesos y controles de seguridad aplicables a interacciones físicas de la organización.	Consultar **AN_Matriz de roles y responsabilidades** (Gestor de seguridad física).
Oficial de seguridad Informática	Definir, mantener y mejorar las políticas, procesos y controles de seguridad aplicables a infraestructura tecnológica de la organización.	Consultar **AN_Matriz de roles y responsabilidades** (responsable de la seguridad de la información)
Oficial de seguridad de la información	Definir, mantener y mejorar las políticas, procesos y controles de seguridad aplicables a la protección de datos operativos.	**AN_Matriz de roles y responsabilidades** (responsable de la seguridad de la información)
Oficial de privacidad de datos	Definir, mantener y mejorar las políticas, procesos y controles de seguridad aplicables a la protección de datos personales.	Consultar **AN_Matriz de roles y responsabilidades** (responsable de la seguridad de la información)

Segregación de tareas.

- Todas las actividades o funciones de responsabilidad crítica para el negocio deberán dentro de lo posible segregarse en esquemas de "Ejecutor - Autorizador", generando al menos 2 roles, uno de ejecución y otro de autorización **(FO_Relación de Funciones Segregadas).**
- Las actividades que no sean críticas para la operación podrán ser excluidas de la segregación de tareas.

Contacto con autoridades y grupos de interés.

- El comité de seguridad deberá establecer relación con las autoridades y referentes internacionales correspondientes a su alcance con la finalidad de mantenerse al día ante cualquier actualización a las regulaciones aplicables y tendencias globales.
- La relación con dichas autoridades y referentes podrá realizarse de manera enunciativa más no limitativa por alguno de los siguientes medios:
  - Participación en foros
  - Seminarios
  - Capacitaciones
  - Redes sociales
  - Boletines
- Se recomienda que el responsable de seguridad de la información permanezca suscrito a los boletines de:
  - SANS
  - OWASP
  - UNAM-CERT
  - US-CERT



Policía cibernética al 55 55425100 extensión 5086, por correo a la dirección policía.cibernetica@scc.cdmx.gob.mx
CERT-MX en la página https://www.gob.mx/gncertmx por email cert-mx@sspc.gob.mx

Proyectos seguros.

Todos los proyectos en su fase de planificación deben contemplar la apreciación y tratamiento de riesgos (ver procedimiento **PR_Apreciación y tratamiento de riesgos**) con la finalidad de garantizar que dé así aplicar, los resultados de cada proyecto cuentan con las políticas, procesos y/o controles de seguridad pertinentes.

Movilidad.

El personal de la organización podrá utilizar para el desempeño de sus funciones, dispositivos propiedad de la empresa o de uso personal, siempre que:

- El usuario acepte por escrito el contrato de responsabilidad de uso de dispositivos
- El dispositivo cuente con el servicio de localización, bloqueo y borrado remoto
- Solicite y sea autorizado su uso al área de sistemas
- De la autorización y aceptación de realizar auditorías a su dispositivo de forma aleatoria sin previo aviso

El personal que por sus funciones así lo requiera, podrá hacer uso de canales de comunicación cifrada entre sitios, mediante herramientas de acceso remoto como:

- Enlaces privados
- Redes privadas virtuales
- Escritorios virtuales
- Administración remota
- Colaboración en línea

➢ Si el personal no tiene disponibles enlaces de comunicaciones privados, podrá hacer uso de redes públicas, siempre que considere utilizar tecnologías de cifrado para la comunicación hacia los sistemas corporativos de la organización o sus partes interesadas, por ejemplo:

- Redes privadas virtuales
- Escritorios virtuales
- Administración remota
- Colaboración en línea
- SSH
- HTTPS
- SFTP

2. Recursos Humanos.

Investigación de antecedentes.

- Durante el periodo de contratación del personal, Capital Humano deberá asegurarse mediante los procesos pertinentes la veracidad de la información provista y su idoneidad de acuerdo con el perfil de puesto al que se encuentre aplicando el postulante (**MA_Manual de Recursos Humanos SGI**), entre la información a verificar se encuentra:
  - Identificación
  - Domicilio
  - Competencias
  - Controles del puesto

Contratación.

- Toda contratación de personal deberá quedar documentada mediante un contrato de prestación de servicios entre la empresa y el empleado, estipulando en el mismo la información que ampare de acuerdo con las regulaciones vigentes, la prestación y contraprestación del servicio.

- De manera adicional, los contratos deberán establecer o hacer referencia a los roles y responsabilidades del personal para con la seguridad de la información y la protección de datos personales con base en las regulaciones aplicables y partes interesadas, buscando en todo momento preservar la confidencialidad, integridad y disponibilidad de la información.

Responsabilidades.

Es responsabilidad del personal el conocer, cumplir y hacer cumplir, las políticas y procesos que permitan garantizar la seguridad de la información definidas por la organización y es el deber de esta última, exigir el cumplimiento de estas mediante la definición, comunicación y ejecución a través del procedimiento **MA_Manual de Recursos Humanos SGI** en caso de incumplimientos.

- La organización tiene la obligación de impartir al menos una vez al año a todo el personal y cuando sea necesario a terceras partes, sesiones de capacitación y/o concientización en materia de seguridad de la información según corresponda a su puesto de trabajo.
- Ante la terminación de un empleo, la organización deberá notificar como recordatorio a la salida del personal, las obligaciones de confidencialidad o no divulgación, así como, los derechos de acceso, rectificación, oposición y cancelación sobre sus datos personales.

3. Activos.

Para conocer el uso y manejo de información y otros activos, consulte el documento **PL_políticas de uso aceptable de la información y otros activos.**

Clasificación de la información.

- La organización en su compromiso por mantener la confidencialidad, integridad y disponibilidad de la información define a continuación las clasificaciones a ser utilizadas para la clasificación y etiquetado de la información.

Nivel	Facultades
Confidencial	Información acerca de clientes, empleados y/o negocios de la Organización que la misma está obligada a proteger y que, si es divulgada a entidades no autorizadas, podría tener un impacto en obligaciones legales, resultados financieros o clientes. Ejemplo: • Contratos • Expedientes de personal • Estrategias corporativas • Diagramas de red • Memorias técnicas • Configuraciones • Contraseñas • Nóminas

Nivel	Facultades
	• Análisis de riesgos • Planes de continuidad del negocio • Planes de continuidad del servicio • Planes de recuperación en caso de desastres
Restringida	Información que la alta Dirección de la organización o el responsable de la misma, determina, tiene potencial para proporcionar una ventaja competitiva u ocasionar un impacto significante en el negocio si es divulgada a entidades no autorizadas. Ejemplo: • Evidencia de procesos • Informes de desempeño • Informes de auditoría • Estados de resultados
Interna	La información que se comparte común y libremente dentro de la Organización y que no esté clasificado como restringida o confidencial Ejemplo: • Procedimientos • Instrucciones de Trabajo • Políticas • Formatos • Comunicados
Pública	Información que es libremente disponible al exterior de la Organización y que se ha elaborado para ser de uso público. Ejemplo: • Folletos • Anuncios de productos y/o servicios • Solicitud de vacantes • Página web • Redes sociales

Etiquetado de la información.

Los documentos oficiales que sean generados al interior de la organización deben tener controles descritos en el procedimiento **PR_ Elaboración y control de documentos y registros**, indicando en el campo "clasificación", la clasificación correspondiente de acuerdo con las definiciones provistas en la sección de clasificación de la información de la presente política.

Tratamiento de la información.

Con base en los criterios definidos por la organización podrá hacerse uso de los siguientes medios autorizados para el tratamiento de información de acuerdo con la clasificación de la información.

Medio autorizado	Pública	Interna	Confidencial	Restringida
Sitio web y redes sociales	SI	NO	NO	NO
Correo electrónico	SI	SI	NO	NO
Correo electrónico con información cifrada	SI	SI	SI	SI
Mensajería y conferencia electrónica pública	SI	SI	NO	NO
Mensajería y conferencia electrónica corporativa	SI	SI	SI	SI
CDs, DVDs y Medios de Almacenamiento Extraíbles	SI	SI	NO	NO
CDs, DVDs y Medios de Almacenamiento Extraíbles CIFRADOS	SI	SI	SI	SI
Por medio de VPN y conexiones seguras como SFTP/HTTPS internos y a clientes	SI	SI	SI	SI
Fax, servicio postal	SI	SI	NO	NO
Mensajería privada o interna en sobre sellado o empaque de seguridad*	SI	SI	SI	SI
Transmisión de palabra, incluyendo el teléfono móvil, correo de voz, contestador, equipos.	SI	NO	NO	NO

*Al hacer uso de un servicio de mensajería pública, privada o interna para el envío de medios físicos de información, el personal deberá asegurarse de que la información enviada haya sido recibida por el destinatario autorizado de manera íntegra y sin violaciones a los sobres y/o empaques de seguridad.

Eliminación de la información.

- Una vez que la información ha cumplido con el ciclo de vida definido para la misma y que ya no será requerida por el negocio, debe eliminarse la información mediante el uso de las técnicas de eliminación definidas por la organización o bien la que ha sido acordada por contrato con el cliente y de acuerdo con la clasificación que le corresponda.
- En la siguiente tabla se muestra las técnicas de eliminación requeridas por cada tipo de información con base en su clasificación.

Tipo de información	Borrado estándar	Borrado seguro	Destrucción de medios
Pública	Opcional	No	No
Interna	Opcional	Opcional	No
Restringida	No	Si	Opcional

Tipo de información	Borrado estándar	Borrado seguro	Destrucción de medios
Confidencial	No	Si	Opcional

Una vez que los medios o dispositivos que contenían información confidencial o restringida ha sido borrados de manera segura (**FO_Acta de borrado seguro**), la organización podrá disponer de los mismos de la forma que más convenga a sus intereses, acorde al procedimiento **FO_Eliminación y disposición de activos y medios** pudiendo llevar a cabo alguna de las siguientes actividades:

- Destrucción
- Resguardo
- Reciclaje electrónico
- Subasta
- Venta
- Donación

4. Control de Acceso.

Tomando como referencia el procedimiento **PR_ Apreciación y Tratamiento de Riesgos** y los requisitos de negocio, la organización debe establecer mecanismos de control para acceder a la infraestructura tecnológica y sus diversos componentes, dichos mecanismos de control deberán ser revisados de forma periódica en función de los cambios que haya presentado la organización y de ser necesario, deberán realizarse los ajustes pertinentes para cumplir con las necesidades y requisitos de seguridad.

Perfil de acceso.

Dentro de lo posible, toda infraestructura tecnológica o sistema de información deberá contar con un sistema de control de accesos basado en roles, mismo que deberá estar configurado tomando como referencia la matriz de accesos y privilegios y las funciones designadas para el perfil de puesto en cuestión.
Cuando la infraestructura tecnológica no tenga la capacidad de contar con un sistema de control de accesos basado en roles, deberá únicamente dar acceso a usuarios personalizados con privilegios homologados tomando como referencia la matriz de accesos y privilegios y las funciones designadas para el perfil de puesto en cuestión.
Los perfiles de acceso por defecto no deberán contar con privilegios de administración que permitan a los usuarios instalar, desinstalar o invalidar de alguna forma los controles de seguridad activos en los equipos.

Solicitud.

Toda solicitud de privilegios de acceso deberá ser requerida por el personal correspondiente al generarse un ingreso o modificación de puesto a la organización, dicha solicitud deberá llegar por escrito mediante una solicitud de servicio.
La solicitud de privilegios de acceso deberá contar al menos con la siguiente información:

- Fecha de solicitud
- Fecha de aplicación
- Descripción de solicitud
- Nombre completo de alta
- Perfil de acceso requerido

Asignación.

El personal que configure las credenciales de acceso en el sistema deberá mantener una codificación homologada para usuarios, así como, la descripción de los roles y nombres del personal, buscando en todo momento que cada usuario sea identificable en sus operaciones dentro de la infraestructura tecnológica.
Los privilegios de acceso a redes y los servicios existentes, deberán ser otorgados única y exclusivamente a los colaboradores que por sus funciones así lo requieran de acuerdo con la matriz de accesos y privilegios.
Los usuarios asignados, deberán ser personales e intransferibles, no deberán existir usuarios genéricos o de grupo que sean utilizados por más de una persona.

Provisión.

Una vez creadas las credenciales de acceso, estas deberán ser proporcionadas de forma directa en 2 o más tantos al propietario de estas, debiendo transmitir de forma segura y por separado, usuario y contraseña.

Revisión.

El personal responsable de la administración de accesos y privilegios deberá al menos una vez al año, realizar una revisión sobre los accesos a infraestructura tecnológica, teniendo como objetivo, identificar cuentas de usuarios inactivas o que deban ser deshabilitadas por terminación o cambio de puesto del personal en cuestión, informando las desviaciones y correcciones del proceso.

Retiro.

Al presentarse una terminación o cambio de relación laboral con socios, empleados o terceras partes deberá ser solicitada la baja o modificación de los privilegios de acceso de forma anticipada o bien de forma inmediata al momento de presentarse la baja.

Acceso a la información.

Los aplicativos o componentes tecnológicos de la organización que contengan información confidencial o restringida, deberán solicitar la identificación y autenticación del usuario previo a su acceso a la información por medio de algún control de seguridad que solicite al menos usuario y contraseña.

Los controles de acceso y perfiles de usuario deberán limitar el acceso a código fuente únicamente al personal autorizado por sus funciones para tal fin.

Contraseñas.

Las contraseñas que sean configuradas en la infraestructura de la organización o sus clientes deberán incluir las siguientes características de así permitirse por el sistema en cuestión.

1. Longitud mínima de 10 caracteres alfanuméricos.
2. Al menos un carácter en mayúscula.
3. Al menos un carácter en minúscula.
4. Al menos un número.
5. La contraseña de usuarios deberá ser cambiada como máximo cada 90 días.
6. Las contraseñas provistas por el administrador del sistema deberán ser cambiadas por el usuario en su primer ingreso, ya sea por alta o restauración de contraseña.
7. La contraseña solo podrá ser restaurada por el personal que administre los accesos de sistema y deberá ser solicitada por el usuario responsable mediante una solicitud de servicio o correo electrónico.
8. Las contraseñas no podrán ni serán almacenadas en archivos no cifrados.
9. Los usuarios emplearan alguna herramienta de almacenamiento que posibilite el cifrado de la información y el uso de al menos una contraseña segura.

5. Cifrado.

Controles criptográficos.

La información de carácter confidencial o restringido deberá de contar con controles de cifrado a lo largo de su ciclo de vida, buscando en todo momento mantener la confidencialidad, integridad y disponibilidad de la información.

- Algunos controles sugeridos para el cifrado de información dependiendo de su momento en el ciclo de vida de la información son:

Cifrado de información	
En tránsito	**En reposo**
• Compresión con contraseña • VPN site to site • VPN client to site • TLS 1.2 o superior	• Compresión con contraseña • Cifrado de disco • Cifrado de archivo • Cifrado de BD • Cifrado de respaldos

- Las llaves de tipo simétrico deberán ser modificadas con regularidad, contemplando los índices de rotación del personal, la confidencialidad de la información que resguardan y los riesgos de la gestión de llaves.
- Las llaves de tipo asimétrico deberán ser modificadas tras su expiración, contemplando los índices de rotación del personal, la confidencialidad de la información que resguardan y los riesgos de la gestión de llaves, teniendo una vigencia mínima de 1 año y máxima de 3 años.
- Los componentes de cifrado deberán contar con algoritmos superiores a los 128 bits y los certificados digitales de nueva adquisición deberán ser del tipo TLS 1.2 o superior, certificados digitales SSL en sus versiones 1, 2 o 3 deberán ser migrados al tipo TLS 1.2 o superior con algoritmos superiores a los 1024 bits al momento de su expiración.

6. Seguridad física.

Áreas seguras.

- La organización deberá definir e implementar perímetros de seguridad y áreas seguras para sus oficinas, despachos y recursos, que tenga como finalidad la protección de las áreas que contienen información sensible o datos personales, así como los diversos recursos de tratamiento de información, permitiendo únicamente el acceso al personal autorizado para tal fin (ver **MA_Seguridad física**).
- Dichos perímetros podrán ser asegurados de acuerdo con los niveles de confidencialidad de la información y garantizando una protección física contra desastres naturales, ataques provocados por el hombre o accidentes, utilizando diversos mecanismos de control como pueden ser:
  - Controles de acceso de presencia
  - Controles de acceso biométrico
  - Controles de acceso mecánico
  - Puertas de acceso
  - Distribución de espacios físicos
  - Circuito Cerrado de TV
  - Áreas de carga y descarga
  - Áreas restringidas
  - Pasillos de servicio
- Debe adoptarse una cultura de puesto de trabajo limpio, despejado de papeles y medios de almacenamiento extraíbles, así como una pantalla limpia para los recursos de tratamiento de información.

Seguridad en equipos.

Los equipos de procesamiento, almacenamiento y transmisión de información deberán situarse o protegerse de manera que se reduzcan los riesgos de daño o pérdida, así como las oportunidades de un acceso no autorizado a la información sensible pudiendo aplicar alguno de los siguientes controles:

- Supervisión permanente
- Bloqueo por inactividad
- Acceso controlado

- Debe asegurarse la protección de los equipos contra fallas de alimentación u otras alteraciones causadas por fallos en las instalaciones de suministro eléctrico.

El cableado eléctrico y de comunicaciones deberá ser identificado y protegido frente a intercepciones, interferencias o daños por medio de tuberías, canaletas o escalerillas.

Los equipos que deban ser retirados de las instalaciones, deberán de contar con la autorización expresa por parte del responsable de los activos.

- De requerirse trabajar fuera de las instalaciones de la organización, el responsable del equipo deberá tomar en consideración los controles y las medidas necesarias para mitigar el riesgo que conlleve el operar fuera de las instalaciones, tales como:
  - Supervisión permanente
  - Uso de candados
  - Cifrado de discos
  - Bloqueo por inactividad

7. Seguridad Operativa.

Procedimientos.

- Debe contar con procesos operativos documentados que permitan a los diversos usuarios identificar sus responsabilidades y alcances dentro de la operación, mismos que deberán ser comunicados y puestos al alcance de todo el personal que por sus funciones lo requiera.
- Debe controlarse por medio del procedimiento **PR_Control de Cambios** cualquier modificación deseada sobre la organización, sus procesos de negocio, instalaciones de tratamiento de información o sistemas que pudiesen impactar la seguridad de la información.
- Debe llevarse a cabo el monitoreo periódico de los recursos requeridos para la generación de productos o servicios, realizando una proyección de los requisitos futuros de capacidad para garantizar el rendimiento requerido para el ofrecimiento continuo de los productos o servicios.
- Los ambientes de desarrollo, prueba y producción deberán permanecer segregados en todo momento al menos virtualmente en servidores distintos, de forma que los datos productivos no puedan ser alcanzados desde los ambientes de desarrollo y pruebas.

(ver procedimiento **PR_Adquisición, desarrollo y mantenimiento**).

Malware.

- Se deberá contar con una solución antimalware que proteja los equipos de la organización, independientemente del sistema operativo que se utilice, dicha solución podrá ser centralizada o local.
- La solución antimalware deberá ser actualizada de forma diaria, contar con revisiones rápidas programadas al menos 1 semanal y revisiones completas al menos 1 mensual.
- Los hallazgos encontrados solo serán tratados como eventos, y no es necesario la atención inmediata ya que son contenidos por la solución.

Respaldos.

- Deberá establecerse un esquema de respaldos **FO_Esquema de respaldos** y dentro de lo posible configurarse su ejecución automática a intervalos planificados, tomando como referencia la criticidad de la información y registrando las ejecuciones en la bitácora de respaldos.
- Una muestra de la información respaldada deberá ser validada mediante pruebas de integridad y restauración al menos una vez al año registrando los resultados en el **FO_Informe de pruebas de respaldo**.

Monitoreo y registro.

- La infraestructura crítica de la organización deberá contar con sistemas automatizados para el registro de eventos generados por usuarios, administradores e incidentes estándar o de seguridad.
- Los registros generados por la infraestructura tecnológica deberán permanecer protegidos contra intentos de modificación o eliminación.
- La infraestructura tecnológica deberá mantener sincronizados los husos horarios en todo momento mediante protocolos NTP (Network Time Protocol).

Parches y actualizaciones.

- A intervalos planificados, la organización deberá llevar a cabo la identificación e implementación de parches y actualizaciones que sean requeridas por la infraestructura tecnológica existente.
- La aplicación de parches y actualizaciones en ambientes productivos deberá llevarse a cabo mediante el procedimiento **PR_Gestión de cambios** buscando en todo momento mantener la disponibilidad y continuidad del servicio.

Vulnerabilidades.

- Los desarrollos en SAP quedan exluidos de realizar analisis de vulnerabilidades de OWASP.
- La organización deberá identificar al menos una vez al año las vulnerabilidades de la infraestructura tecnológica utilizada y evaluar la exposición de las configuraciones a dichas vulnerabilidades mediante alguna de las siguientes actividades.
  - Análisis de vulnerabilidades
  - Pruebas de penetración
  - Análisis de código fuente
- Las actividades de auditoría sobre sistemas informáticos deberán ser cuidadosamente planificadas, acordadas y notificadas a los involucrados para minimizar el riesgo de interrupciones en los procesos de negocio, preferentemente fuera de horarios de oficina.
- Los riesgos derivados de las vulnerabilidades identificadas deberán ser tratados tomando como referencia el procedimiento **PR_Apreciación y tratamiento de riesgos** y notificados a la alta dirección mediante el procedimiento **PR_ Revisión por la dirección.**
- Con la finalidad de controlar los riesgos a los que la organización se encuentra expuesta, derivado del software que utiliza, los usuarios no podrán realizar la instalación de ningún tipo de software en los

equipos de cómputo, cualquier instalación deberá ser realizada únicamente por el personal administrador de los mismos.

8. Seguridad en las Comunicaciones

Redes.

- Las redes de telecomunicaciones utilizadas por la organización deberán contar con controles tecnológicos de seguridad que permitan identificar, contener y atender los eventos de seguridad a los que la organización se encuentre expuesta, protegiendo así la información y los sistemas.
  - De así requerirse por las partes interesadas, la organización deberá documentar mediante acuerdos contractuales o niveles de servicio los requisitos de seguridad de los servicios de red provistos internamente o bien subcontratados con terceras partes.
- Las redes de telecomunicaciones deberán mantener una segregación entre usuarios y sistemas de información con base en las funciones y requisitos de seguridad de la información por medio de VLAN's, listas de acceso o seguridad en capas por medio de segregaciones físicas o lógicas.

Transferencia.

- El personal que tenga acceso a información privilegiada que pueda ser clasificada como restringida o confidencial propiedad de la organización o sus clientes deberá contar con acuerdos de confidencialidad debidamente firmados y revisar su vigencia y aplicabilidad al menos una vez al año.
- La organización deberá acordar con terceras partes los protocolos autorizados para la transferencia segura de información. De requerirse, dichos acuerdos podrán quedar establecidos contractualmente y de lo contrario deberán apegarse a las presentes políticas de seguridad de la información para clasificación, tratamiento, eliminación y cifrado.
- La información que requiera ser enviada por mensajería electrónica y que por su clasificación sea considerada restringida o confidencial, deberá hacer uso de los controles mencionados en el apartado de cifrado de información en tránsito en las presentes políticas.

9. Sistemas de Información.

Requisitos de seguridad.

- Todo nuevo sistema o liberación sobre sistemas existentes deberá haber contemplado durante su generación los requisitos de seguridad pertinentes para garantizar la confidencialidad, integridad y disponibilidad de la información.
- La información deberá contar con los controles de seguridad en tránsito o reposo sugeridos de acuerdo con el momento en el que se encuentre dentro de su ciclo de vida.
- Previo a su liberación, la infraestructura expuesta deberá pasar por un proceso de robustecimiento de controles de seguridad, debiendo realizar al menos las siguientes actividades:
  1. Eliminación de software no utilizado

2. Actualización de versiones
3. Integración al proceso de administración de vulnerabilidades
4. Aplicación de políticas de grupo
5. Aplicación de políticas de seguridad
6. Aplicación de configuraciones predefinidas por plataforma

- De ser necesario, la infraestructura crítica podrá ser analizada mediante pruebas de penetración o análisis de vulnerabilidades. Dichas pruebas podrán ser realizadas de forma interna o por un tercero, debiendo dar el debido tratamiento a los riesgos críticos y altos que sean identificados.

Desarrollo seguro.

- Las aplicaciones o recursos informáticos que sean desarrollados por la organización o sus terceras partes a excepcion de los desarrollados en SAP, deberán seguir metodologías de desarrollo seguro y dentro del ciclo de vida del desarrollo validar al menos el Top 10 de OWASP como parte de las pruebas funcionales de seguridad previo a su liberación. Se debe genrar un informe correspondiente a la validadción realizada y se debe entregar al Gestor de Adquisición, mantenimiento y desarrollo de sistemas.
    1. Broken Access Control
    2. Cryptographic Failures
    3. Injection
    4. Insecure Design
    5. Security Misconfiguration
    6. Vulnerable and Outdated Components
    7. Identification and Authentication Failures
    8. Software and Data Integrity Failures
    9. Security Logging and Monitoring Failures
    10. Server-Side Request Forgery

- Los desarrollos que sean subcontratados a un tercero deberán ser supervisados y controlados por la organización, debiendo cubrir los mismos requisitos que los desarrollos internos.
- Cualquier cambio que vaya a ser aplicado a lo largo del ciclo de vida del desarrollo deberá controlarse mediante el procedimiento **PR_Gestión de cambios** y deberá estar limitado a los cambios rigurosamente necesarios.
- Tras aplicar cambios en los sistemas operativos de infraestructura crítica, deberá realizarse una verificación sobre las aplicaciones de negocio, garantizando así la no existencia de efectos adversos en las operaciones o la seguridad de la organización.
- La organización debe de mantener protegidos y restringidos los ambientes de desarrollo, así como los componentes generados en el mismo durante todo el ciclo de vida del desarrollo.
- La organización deberá contar con criterios y pruebas de aceptación documentadas para nuevos sistemas de información, actualizaciones o nuevas versiones desarrolladas internamente o por terceros subcontratados.

Datos de prueba.

- Los datos utilizados por la organización en ambientes de pruebas o desarrollo deberán en medida de lo posible ser ficticios o no permitir la identificación o trazabilidad del propietario de los datos.
- Los datos utilizados por los clientes deberán cubrir las necesidades y requisitos de seguridad estipulados por el mismo cliente.
- Para ambientes de prueba que así lo requieran, podrá utilizarse información real bajo escenarios controlados que protejan los datos sensibles de los propietarios de la información.
- Las modificaciones a los datos productivos para ser utilizados en ambientes de pruebas o desarrollo deberán ser registrados dentro de la bitácora de data scrambling.

10. Proveedores.

- La organización deberá establecer contratos de servicio y acuerdos de confidencialidad con los terceros subcontratados que por sus funciones requieran de acceso a información o infraestructura de la organización o de los clientes.
- Con la finalidad de homologar terminología y procesos con los terceros subcontratados, la organización deberá difundir a sus proveedores, las políticas de seguridad de la información aplicables de acuerdo con los servicios contratados y asegurarse de que el tercero subcontratado y su personal tienen conocimiento de las mismas.
- Los proveedores serán responsables de definir, implementar, mantener y revisar a intervalos planificados los controles de seguridad que permitan a la organización mitigar los riesgos derivados de la interacción entre la organización y el tercero en cuestión.
- Los proveedores deberán hacer uso de las políticas de clasificación de la información para identificar, etiquetar y tratar la información de forma correcta mismas que se les deberán compartir para su conocimiento. Consultar **MA_Seguridad para proveedores del SGI.**

11. Incidentes de Seguridad de la Información.

Procedimiento.

- La organización debe definir y documentar incidentes de seguridad a través del procedimiento **MA_Respuesta a Incidentes**, con la finalidad de garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información, mismo que deberá contar con las siguientes fases.
  1. Prevención
  2. Identificación
  3. Contención
  4. Solución
  5. Recuperación
  6. Lecciones aprendidas
- Dicho proceso deberá contar los criterios de decisión para determinar la existencia de un incidente de seguridad de la información.

Responsabilidades.

- Se debe establecer los roles y responsabilidades del personal involucrado durante un incidente de seguridad de la información y dichas responsabilidades deben ser conocidas y entendidas por los responsables.
- Todo el personal interno o externo que identifique cualquier evento de seguridad de la información debe notificar a través de un ticket el incidente. (consultar el procedimiento PR-IT-001 Gestión de tickets).
- Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información son responsables de documentar y notificar mediante un incidente cualquier punto débil que observen o sospechen que exista, en los sistemas o servicios.
- El responsable de Seguridad de la información estará encargado de dar seguimiento del incidente hasta su cierre.

Notificación.

- Los eventos de seguridad o puntos débiles que se presenten en infraestructura de terceros o que sean identificados por terceros deberán ser notificados al responsable de Seguridad de la información de la organización mediante un correo electrónico, o bien, a través de los canales de comunicación disponibles en el momento.

Resguardo de evidencias.

- La organización es responsable de recolectar y preservar de forma íntegra las evidencias generadas durante un evento de seguridad de la información.

12. Continuidad del Negocio.

Planificación.

- La organización debe definir planes de continuidad del servicio o negocio que le permitan determinar sus necesidades y requisitos de disponibilidad y continuidad para la seguridad de la información durante una contingencia.
- Dichos planes deberán determinar los criterios de activación, desactivación, requisitos de disponibilidad, objetivos de recuperación, roles, responsabilidades, sedes, recursos de tratamiento de información, redundancias, actividades y protocolos de comunicación y notificación con las partes interesadas.

Implementación.

- La organización deberá determinar escenarios de amenaza que pudiesen afectar los objetivos de disponibilidad y continuidad para definir una estrategia que haga frente a los mismos.

- La organización debe establecer, documentar, implementar y mantener los procesos y controles que garanticen la continuidad del negocio con base en los objetivos de disponibilidad y continuidad.
- La documentación de los planes de continuidad deberá contar con las matrices de contacto y actividades necesarias para mantener la operación del negocio a los niveles mínimos requeridos por las partes interesadas.

Pruebas.

- La organización deberá ejecutar al menos una vez al año, de forma independiente la prueba de los escenarios de contingencia, dichas pruebas deberán ser previamente documentadas para conocer los pasos a seguir, así como, los responsables de su ejecución.
- Durante las pruebas es necesario llevar un registro de las actividades que se realizan y los resultados obtenidos de las mismas, así como las desviaciones de lo planificado.

Lecciones aprendidas.

- Una vez que han sido concluidas las pruebas de continuidad correspondientes, es necesario que el responsable de la continuidad del negocio genere el informe de pruebas de continuidad con los resultados obtenidos durante las pruebas del plan de continuidad y disponibilidad. Posteriormente, el comité de gestión de crisis deberá analizar los resultados y determinar las acciones preventivas, correctivas o de mejora que apliquen.
- Cualquier modificación a los planes de continuidad deberá ser solicitada mediante el procedimiento **PR_Gestion de cambios.**

13. Cumplimiento.

Regulaciones aplicables.

- La organización debe determinar todos los requisitos legales, regulatorios, contractuales, estatutarios o contractuales aplicables, así como, las medidas o controles pertinentes para cumplirlos, dichos requisitos deberán ser tomados en cuenta para analizar el contexto de la organización y determinar los riesgos inherentes del negocio (ver **AN_Leyes aplicales).**
- Dichos requisitos deberán mantenerse actualizados y vigentes para cada servicio y sistema de información de la organización.

Propiedad intelectual.

- La organización deberá mantenerse informada y en cumplimiento sobre el uso de materiales, licenciamiento de software, código fuente o cualquier tipo de medio que pudiese infringir algún derecho de propiedad intelectual.
- Así mismo, la organización deberá mantener bajo registro de propiedad intelectual cualquier material o idea que así lo amerite con la finalidad de proteger los activos de la organización ante cualquier intento de uso mal intencionado.

Protección de registros.

- La organización debe tomar en cuenta los requisitos legales, regulatorios, contractuales y de negocio para llevar a cabo el correcto resguardo y protección de los registros resultado de su operación.
- Por defecto los registros que sean resguardados por la organización deberán ser almacenados por 10 años, sin embargo, podrá definirse un ciclo de vida de la información distinto por cada registro existente con base en los acuerdos establecidos con cada cliente, proveedor o personal de la organización.
- En caso de requerirse la eliminación de los registros, esto deberá ser atendido mediante el procedimiento **PR_Manual de respuesta a incidentes** y deberá seguir las políticas de seguridad de la información de la organización.

Privacidad de datos personales.

- La organización deberá atender y cumplir los requisitos enunciados por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y sus respectivos reglamentos vigentes.
- Debe definirse, documentarse y publicarse un aviso de privacidad integral en la página web de la organización, indicando los procesos para tratar la información con base en lo previsto por la LFPDPPP que deberá contemplar al menos los siguientes puntos:
  - Finalidad
  - Datos recabados
  - Acceso
  - Rectificación
  - Cancelación
  - Oposición
  - Contacto
  - Consentimiento
  - Modificaciones
- En la recepción de la organización deberá mostrarse el aviso de privacidad en su versión corta o simplificada, haciendo referencia a la liga del aviso de privacidad integral.
- Debe colocarse en el acceso a la organización, señalítica plenamente visible que indique la existencia de un sistema de grabación de CCTV.

Controles criptográficos.

La organización debe tomar en cuenta los requisitos legales, regulatorios, contractuales y de negocio para llevar a cabo la implementación de controles criptográficos para el intercambio o almacenamiento de información, así como, lo estipulado en las políticas de seguridad de la información para determinar los requisitos mínimos indispensables de seguridad de la información.

Auditoría de seguridad de la información.

Al menos una vez al año, o bien, cada que se produzca una modificación significativa en la organización, se deberá someter a revisiones independientes el sistema de gestión de seguridad de la información, con la finalidad de identificar desviaciones a los procesos y oportunidades de mejora, mismas que deberán ser tratadas mediante el procedimiento **PR_ Acciones correctivas y de mejora.**

Controles documentales.

Es responsabilidad de los directivos de la organización el cumplir y hacer cumplir los controles documentales de seguridad, tales como políticas, procesos, procedimientos, instructivos, formatos, al igual que cualquier otro requisito aplicable.

Controles tecnológicos.

La organización deberá comprobar al menos una vez al año y con base en la rotación de personal y uso de los controles, la debida aplicación de los controles tecnológicos en los sistemas de tratamiento de información, generando el informe de controles tecnológicos correspondiente.

14. Control de cambios.

Versión	Cambios realizados	Fecha
11	Actualización de formato y procesos citados.	16 Sep 24

FIN DEL DOCUMENTO.