SEYCEX, organización dedicada a *Consultoría y Asistencia Técnica. Redacción de Proyectos. Dirección de Obra. Prevención de Riesgos. Coordinación de Seguridad* tiene el convencimiento de que la Seguridad de la Información es un factor clave para el correcto desarrollo de la organización. Considera que, junto con la dotación de formación y recursos necesarios para el desarrollo de la actividad, son los principales pilares para ofrecer a los clientes servicios con la calidad adecuada.

Por ello, desde la Dirección de Seycex declaramos la implantación, el mantenimiento y la mejora del Sistema de Gestión como objetivo estratégico y prioritario, donde dicho sistema tiene como objetivos:

- Asegurar el cumplimiento de la legislación, reglamentación y normativas aplicables, así como todos aquellos requisitos que la organización considere oportuno para conseguir una mejora continua.
- Ofrecer servicios con un nivel de seguridad que satisfaga y supere las necesidades de nuestros clientes.
- La formación del personal conforme a los cambios técnicos e innovaciones tecnológicas a los que la actividad de la organización se vea sometida.
- La asignación eficaz de funciones y responsabilidades en el ámbito de la seguridad.
- La prevención de posibles defectos e incidentes de Seguridad de la Información antes de que ocurran, trabajando orientados hacia la “mejora continua” y la comunicación.
- La evolución continua del Sistema de Gestión de Seguridad de la Información, con el fin de adecuarnos a las exigencias de nuestros clientes.
- La concienciación y motivación del personal de SEYCEX sobre la importancia de la implantación y desarrollo de un Sistema de Gestión de Seguridad de la Información.

La Dirección establece y revisa objetivos y metas, teniendo como marco de referencia la política definida, fijando las responsabilidades en su consecución y estableciendo criterios de actuación.

La Dirección se compromete a la implantación, mantenimiento y mejora del SGSI dotándolo de aquellos medios y recursos que sean necesarios e instando a todo el personal para que asuma este compromiso.

Fdo:

Juana María Carranza. Responsable del SIG

José Marcos López-Palomo. Dirección

POLÍTICA DE EQUIPOS HARDWARE

Para garantizar la seguridad de la información en **Seycex**, es esencial mantener una disciplina con los equipos hardware de la empresa, tanto para su mantenimiento como para la prevención de accesos no autorizados a los mismos.

PROTECCIÓN DEL EQUIPO.

Se divide en tres secciones:

- Equipos portátiles: Los equipos portátiles deben estar siempre vigilados en entornos públicos, y si es preciso dejarlo en un punto desatendido, siempre que se pueda se deberá utilizar un candando de seguridad. Si se trabaja en lugares públicos, se ha de tener la precaución de no tener a la vista datos sensibles, bien de la empresa, bien de clientes y/o usuarios.
- Equipos sobremesa: Los equipos de sobremesa deben estar ubicados en una localización segura, la cual, mediante controles de acceso permita evitar el hurto de estos equipos. Dichos equipos no se podrán cambiar de localización sin autorización previa de la dirección.
- Otros dispositivos: Se aplicarán las reglas generales indicadas para los equipos portátiles y sobremesa, garantizando la seguridad de la ubicación y la protección contra accesos no autorizados

Equipo desatendido

Siempre que se vaya a dejar el equipo desatendido (siempre cumpliendo la normativa de protección del equipo), éste debe estar bloqueado para evitar accesos no autorizados. Es irrelevante la duración de la ausencia, **siempre que no estemos delante del equipo, éste debe estar bloqueado**.

Mesa y pantalla limpia

Es importante mantener el puesto de trabajo limpio y ordenador. Para evitar fugas de información, toda documentación física con la que se trabaje deberá ser guardada al finalizar. Al final de la jornada no debe quedar ningún tipo de documento sobre la mesa. Los post-it o similares con contraseñas apuntadas quedan **totalmente prohibidos**.

Al dejar el equipo bloqueado, debemos asegurarnos de que en la pantalla de bloqueo no aparece informaciónsensible.

Mantenimiento de equipos

Es responsabilidad del empleado mantener su equipo en pleno funcionamiento, dándole un correcto uso. En caso de fallos, el empleado deberá avisar al departamento de tecnología para obtener asistencia.

Mérida, 01 de enero de 2023

Dirección

POLÍTICA DE GESTIÓN DE CAMBIOS

Es esencial definir como se controlan los cambios en el sistema de información.

Cualquier cambio sobre sistemas operativos o de producción, debe ser realizado de la siguiente forma:

- Los cambios pueden ser propuestos por Dirección o por cualquier responsable de departamento
- Los cambios deben ser autorizados por Dirección que debe evaluar su justificación para el negocio y las potenciales consecuencias negativas sobre la seguridad.
- Los cambios deben ser implementados por el personal que designe Dirección.
- El Resp. de Seguridad de la información es el responsable de verificar que los cambios se han implementado de acuerdo con los requerimientos.
- La Dirección es la responsable de probar y verificar la estabilidad del sistema; el sistema no debe ser puesto en producción antes de haber realizado pruebas exhaustivas.

Los registros sobre los cambios son llevados en el Registro de Control de Cambios de cada documento.

Mérida, 01 de enero de 2023

Dirección

POLÍTICA SOBRE DISPOSITIVOS MÓVILES Y TELETRABAJO

Para evitar el acceso no autorizado a dispositivos ubicados tanto dentro como fuera de las instalaciones de la organización, **Seycex**, ha implementado la siguiente política sobre dispositivos móviles y el teletrabajo.

Como dispositivo móvil se entiende todo tipo de ordenadores portátiles, teléfonos móviles, tarjetas de memoria y demás equipamientos móviles utilizados para almacenamiento, procesamientos y transferencia de datos. El equipamiento mencionado precedentemente puede ser llevado fuera de las instalaciones solamente conautorización de la dirección y el departamento de tecnología.

Se debe tener especial cuidado cuando los equipos de computación móvil se encuentran en vehículos,espacios públicos, habitaciones de hotel o salas de reunión.

La persona que se lleva equipos de computación móvil fuera de las instalaciones debe cumplir las siguientesreglas:

- El equipamiento de computación móvil que contiene información importante, sensible o crítica no debe ser desatendido y, en lo posible, debe quedar resguardado bajo llave o se deben utilizar trabas especiales para asegurarlo.
- Cuando se utiliza un equipamiento de computación móvil en lugares públicos, el usuario debe tener la precaución de que los datos no pueden ser leídos por personas no autorizadas.
- Las actualizaciones de parches y demás configuraciones del sistema son realizadas solo por el personal autorizado.
- La protección contra código malicioso se instala y actualiza solo por el personal autorizado.
- La persona que utiliza el equipamiento de computación móvil fuera de las instalaciones es responsable de realizar periódicamente controles de seguridad de datos.
- La información que se encuentra en ordenadores portátiles debe estar encriptada.

Mérida, 01 de enero de 2023

Dirección

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES

Para garantizar la seguridad de la información frente a la relación con los proveedores y socios, **Seycex**, ha implementado la siguiente política de seguridad de seguridad para proveedores.

La tercerización siempre implicará un riesgo. Para ello siempre que sea necesario por el tipo de relación que se tenga con el proveedor, habrá que incluir una serie de cláusulas en el contrato, presupuesto, acuerdo de colaboración, contrato de UTE… que regule nuestra relación y que nos garanticen la trazabilidad de la seguridad de la información.

Inclusión de cláusulas en los contratos con los proveedores:

- Derechos a auditoría: Garantiza a la organización contratante, el derecho a evaluar y auditar los controles de seguridad implementados por el proveedor, en forma periódica o cuando se presenten cambios significativos en los controles o en la relación contractual entre ambas partes.
- Notificaciones sobre infracciones en la seguridad: esta cláusula obliga al proveedor a informar a la organización contratante sobre cualquier violación a la seguridad de la información que afecte sus operaciones o sus negocios.
- Aceptación de las prácticas de seguridad: con esta cláusula el proveedor declara que conoce y acepta sin restricciones las prácticas de seguridad de la información propuestas por el contratante, y que comunicará en forma oportuna, su imposibilidad de adherirse a alguna, algunas o todas ellas en un momento determinado.
- Tiempo de respuesta ante una violación: el proveedor debe comunicar al contratante los planes de tratamiento que contempla ante posibles violaciones de la seguridad, y los tiempos en que tendrán efecto esas acciones.
- Demostración de cumplimiento: el proveedor debe demostrar con evidencia irrefutable, que los controles que ha implementado y las acciones correctivas que ha diseñado cumplen con los requisitos contractuales. Es probable que esta demostración de cumplimiento requiera una auditoría o una verificación de algún tercero.
- Control sobre la cadena de suministro: el proveedor puede tener la necesidad de aplicar a otras organizaciones con las que suscriba acuerdos, las mismas políticas y condiciones que a él le ha impuesto la organización contratante, en la medida en la que se conforme una cadena de suministro.
- Comunicación sobre cambios: el proveedor debe informar a la organización contratante, todos los cambios en su entorno que afecten el negocio o la operación de su cliente, en forma oportuna.

Mérida, 01 de enero de 2023

Dirección

POLÍTICA DE CLASIFICACIÓN Y USO DE LA INFORMACIÓN

Para garantizar que se proteja la información en un nivel adecuado se ha creado dicha política que será aplicable a todo el personal de la empresa y de obligado cumplimiento.

Información clasificada

- Clasificación de la información

Toda la información debe ser clasificada en niveles de confidencialidad. Actualmente se clasifica la información de la siguiente manera:

Nivel de confidencialidad	Etiquetado	Criterios de clasificación	Restricción de acceso
Pública	(sin etiquetar)	Hacer pública la información no puede dañar al Grupo de ninguna forma cumpliendo con la legalidad vigente.	La información está disponible para todo el público.
Uso interno	(sin etiquetar)	El acceso no autorizado a la información podría ocasionar daño y/o inconvenientes menores al Grupo.	La información está disponible para todos los empleados y terceros seleccionados
Restringida	(sin etiquetar)	El acceso no autorizado a la información podría dañar considerablemente el negocio y/o reputación del Grupo.	La información está disponible solamente para grupos específicos de empleados y de terceros autorizados
Confidencial	(sin etiquetar)	El acceso no autorizado a la	La información está disponible

		información podría dañar de forma catastrófica (irreparable) el negocio y/o reputación de Seycex.	solamente para un grupo reducido de personas de Seycex.

La regla básica es utilizar el nivel de confidencialidad más bajo garantizando un adecuado nivel de protección para evitar gastos de protección innecesarios.

En caso de no tener etiqueta identificativa se considera información clasificada como de uso interno.

Personas autorizadas

La información clasificada como "Restringida" y "Confidencial" debe estar acompañada de una Lista de personas autorizadas en la que el propietario de la información específica los nombres o los cargos de las personas que tienen derechos de acceso para esa información.

La misma regla aplica para el nivel de confidencialidad "Uso interno" si las personas externas a la organización tendrán acceso a esos documentos.

Mérida, 01 de enero de 2023

Dirección

POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

1. Introducción

Este procedimiento es un mecanismo para identificar vulnerabilidades, detectar amenazas y responder a incidentes de seguridad minimizando los efectos o daños causados por estos. Este documento se centrará en la capacidad de respuesta que se debe tener cuando ocurra un incidente urgente independientemente su categoría:

- Cortes eléctricos
- Ataques delincuentes cibernéticos
- Accesos indebidos
- Suplantación de identidad
- Fraude
- Etc.

Con el fin de garantizar la información y el buen funcionamiento de los sistemas de SEYCEX, se designa a los responsables del Sistema de seguridad de la información para hacer frente a cualquier tipo de brecha o emergencia, pudiendo delegar la función en la persona o personas que puedan hacer frente al incidente de la forma más rápida y eficaz posible.

La incidencia puede producirse fuera del horario laboral por lo que los responsables deben de estar disponibles para actuar, en cualquier caso.

2. Notificación Incidencia

La incidencia puede ser detectada por los servicios de monitorización que dispone la organización o puede ser transmitida por algún trabajador del grupo.

Indistintamente de la forma de comunicación o detención de la incidencia, se trasladará inmediatamente al **responsable de Seguridad.**

3. Etapas

3.1. Acción inmediata para detener o minimizar el incidente

Mediante sistemas que permiten implementar alertas inmediatas y controles de protección que identifiquen ciertas situaciones como sospechosas; SEYCEX invierte recursos técnicos y humanos en esta primera fase porque la capacidad de reacción es el factor que te permitirá reducir los daños.

3.2. Investigación del incidente

Una vez detectado el incidente, se tienen mecanismos de análisis que te permiten clasificar, de manera rápida y certera, la incidencia y poner en alerta a los equipos especializados o descartarla por no representar un verdadero riesgo para la organización.

3.3. Restauración de los recursos afectados

Ya habiendo acciones concretas para hacer frente a la incidencia, se comienza a evaluar los daños generados y se busca la manera de hacer frente a estas consecuencias, dando prioridad a restaurar los recursos más urgentes para el funcionamiento de la empresa, para después ya ir solucionando los demás.

3.4. Reporte del incidente a los canales apropiados

Finalmente, se generan reportes detallados del incidente que son compartidos con las áreas apropiadas para generar manuales de acción que ayuden a hacer frente a próximas amenazas con características similares.

3.5. Pérdida de información o brecha de seguridad

Si la incidencia o ataque ha supuesto una pérdida de información o brecha de seguridad habrá que evaluar los daños generados de una manera mucho más específica, haciendo hincapié en la recuperación de la misma lo antes posible, además se debe dar prioridad a restaurar los recursos más urgentes para el funcionamiento de la empresa e ir después solucionando los demás.

Además se debe realizar denuncia ante la Policía, la Guardia Civil o el Juzgado. Actualmente tanto la Guardia Civil con el Grupo de Delitos Telemáticos y la Policía con la Brigada de Investigación Tecnológica perteneciente a la UDEF, disponen de equipos de trabajo, especialmente formados para la investigación de estos ciberdelitos, incluso disponen de grupos de trabajo que investigan y focalizan su trabajo, únicamente a delitos informáticos cometidos en el seno de empresas.

Los contactos a los que comunicar incidencias son los siguientes:

- Comunicación de brechas de comunicaciones de datos:
  - Agencia Española de Protección de Datos (AEPD)
    - https://sedeagpd.gob.es/sede-electronica-web/
    - En un plazo máximo de 72 horas.
  - Grupo de Delitos Telemáticos Unidad Central Operativa Guardia Civil (062)
    - https://www.gdt.guardiacivil.es/webgdt/home_alerta.php
  - Policía Nacional BRIGADA CENTRAL DE INVESTIGACIÓN TECNOLÓGICA (B.C.I.T.)
    - https://www.policia.es/_es/denuncias.php
  - Instituto Nacional de Ciberseguridad (INCIBE)
    - https://www.incibe-cert.es/
    - Buzón de correos: incidencias@incibe-cert.es
  - Centro criptológico nacional (CCN)
    - https://www.ccn-cert.cni.es/

4. Continua evolución

Los ataques e incidencias cambian o evolucionan con el paso del tiempo, es por ello por lo que periódicamente se deberá revisar el procedimiento de respuesta y también se tendrá en cuenta:

- Creación de manuales con los pasos a seguir ante una incidencia para dar una respuesta exacta a la amplia variedad de situaciones, reduciendo significativamente los errores debido al estrés de hacer frente a la amenaza. Todos estos manuales deben estar en constante revisión porque siempre hay situaciones que enriquecen o replantean las estrategias.
- La creación o actualización de manuales y políticas establecidas por la organización adaptándose a los cambios con el fin de minimizar las incidencias.
- Suscripción a plataformas de seguridad para estar informado (INCIBE, OSI...).

- Formación continua relacionada con la materia.