Instructivo de SI Future Concept SAC

INSTRUCTIVO 1: Instrucciones para identificar y evaluar los riesgos de seguridad de la información y aplicar medidas para mitigarlos

I. Objetivo:

El objetivo de este instructivo es proporcionar un marco de trabajo para identificar y evaluar los riesgos de seguridad de la información, así como para aplicar medidas que permitan mitigarlos, con el fin de garantizar la confidencialidad, integridad y disponibilidad de los activos de información de Future Concept SAC.

II. Alcance:

Este instructivo se aplica a todas las áreas de negocio, empleados, contratistas, proveedores y terceros que manejen activos de información con Future Concept SAC., incluyendo información impresa y electrónica, dispositivos de almacenamiento y procesamiento de datos.

III. Procedimiento

1. **Identificación de activos de información:** Se debe elaborar una lista completa de todos los activos de información que se manejan en la organización, incluyendo información impresa y electrónica, así como dispositivos de almacenamiento y procesamiento de datos.

2. **Identificación de amenazas y vulnerabilidades:** Se deben identificar todas las posibles amenazas y vulnerabilidades que puedan afectar la seguridad de la información de la organización. Algunas fuentes de amenazas y vulnerabilidades incluyen la naturaleza del negocio, la ubicación física de la organización, la tecnología utilizada y el personal.

3. **Evaluación de riesgos:** Una vez identificados los activos de información, las amenazas y las vulnerabilidades, se debe evaluar el riesgo asociado con cada activo de información. Esto se realiza mediante la determinación de la probabilidad y el impacto de cada amenaza o vulnerabilidad en los activos de información.

4. **Selección de medidas de seguridad:** Después de evaluar los riesgos, se deben seleccionar medidas de seguridad apropiadas para mitigar los

riesgos identificados. Estas medidas pueden incluir controles técnicos, administrativos y físicos.

5. **Implementación de medidas de seguridad:** Una vez seleccionadas las medidas de seguridad apropiadas, se deben implementar para garantizar que la seguridad de la información se mantenga en todo momento.

6. **Monitoreo y revisión:** Se debe establecer un proceso de monitoreo y revisión continuos para garantizar que las medidas de seguridad implementadas sean efectivas y se adapten a los cambios en la organización y su entorno.

7. **Actualización de la evaluación de riesgos:** Se debe realizar una revisión periódica de la evaluación de riesgos para garantizar que los riesgos sean mitigados y que las medidas de seguridad sigan siendo efectivas.

IV. Conclusión:

Es importante que todo el personal de la organización esté consciente de la importancia de mantener la seguridad de la información y esté capacitado en los procedimientos establecidos en este instructivo. Asimismo, se debe establecer un proceso de reporte y respuesta a incidentes de seguridad de la información para poder actuar rápidamente ante cualquier eventualidad.

<u>INSTRUCTIVO 2:</u> Instrucciones para la identificación de los activos de información en Future Concept SAC

I. Objetivo:

Este instructivo tiene como objetivo guiar a los empleados, contratistas, proveedores y terceros que interactúan con Future Concept SAC en el proceso de identificación de los activos de información de la organización.

II. Alcance:

Este instructivo se aplica a todas las áreas de negocio, empleados, contratistas, proveedores y terceros que interactúen con Future Concept SAC.

III. Responsabilidades:

El personal designado por Future Concept SAC liderará el proceso de identificación de los activos de información de la organización. Los empleados, contratistas, proveedores y terceros que interactúan con Future Concept SAC tienen la responsabilidad de participar activamente en este proceso.

IV. Procedimiento:

1. **Identificación de los activos de información:** Los activos de información son elementos valiosos para la organización y deben ser protegidos. Para identificarlos, se debe hacer una lista que incluya:

    a. Información confidencial, como datos personales, información financiera, estrategias de negocio, entre otros.
    b. Sistemas de información, como aplicaciones, bases de datos, servidores, entre otros.
    c. Infraestructura de red, como routers, switches, firewalls, entre otros.
    d. Dispositivos móviles, como smartphones, tablets, laptops, entre otros.
    e. Medios de almacenamiento, como discos duros externos, unidades flash USB, CD, DVD, entre otros.
    f. Documentos físicos, como contratos, facturas, expedientes, entre otros.

2. **Categorización de los activos de información:** Una vez identificados los activos de información, se deben categorizar según su importancia y nivel

de riesgo para la organización. La categorización permitirá establecer medidas de seguridad adecuadas para protegerlos. Se pueden utilizar criterios como el impacto financiero, la relevancia estratégica, el valor de mercado, la confidencialidad, entre otros.

3. **Actualización de la lista de activos de información:** La lista de activos de información debe ser actualizada regularmente para incluir nuevos activos de información y eliminar aquellos que ya no sean necesarios. La actualización de la lista es importante para garantizar que la organización tenga una visión clara y actualizada de los activos de información que posee y debe proteger.

4. **Comunicación y concientización:** Es importante que todos los empleados, contratistas, proveedores y terceros que interactúan con Future Concept SAC estén informados sobre la lista de activos de información y su importancia para la organización. Por lo tanto, se debe realizar una campaña de comunicación y concientización para sensibilizar a todos los interesados sobre la importancia de proteger los activos de información y los riesgos asociados a su pérdida, robo o divulgación no autorizada.

V. Conclusiones:

La identificación de los activos de información es un proceso fundamental para establecer medidas de seguridad adecuadas y proteger la información de la organización. Es importante que todos los empleados, contratistas, proveedores y terceros que interactúan con Future Concept SAC participen activamente en este proceso y estén informados sobre su importancia.

<u>INSTRUCTIVO 3:</u> Instrucciones para el acceso y manejo seguro, confidencial e íntegro de la información en Future Concept SAC

I. Objetivo:

Establecer los procedimientos para el acceso y manejo seguro, confidencial e íntegro de la información en Future Concept SAC.

II. Alcance:

Este instructivo se aplica a todos los empleados, contratistas, consultores y otros terceros que accedan, manejen o procesen información en nombre de Future Concept SAC.

III. Procedimientos:

1. **Acceso a la información:** El acceso a la información debe otorgarse únicamente a los empleados que necesiten la información para cumplir con sus funciones laborales. Cada empleado debe contar con credenciales de acceso únicas y confidenciales, que se asignarán según el nivel de acceso requerido.

2. **Control de acceso:** Future Concept SAC debe establecer controles de acceso físicos y lógicos para garantizar que solo se permita el acceso a la información a las personas autorizadas. Las credenciales de acceso se deben asignar de acuerdo con las políticas y procedimientos establecidos por la empresa.

3. **Protección de la información:** Se deben establecer medidas de seguridad para proteger la información contra la divulgación no autorizada, la destrucción o la alteración. Esto puede incluir el uso de contraseñas seguras, el cifrado de la información y la implementación de controles de acceso físicos y lógicos.

4. **Uso adecuado de la información:** El acceso a la información se debe utilizar únicamente para fines legítimos y autorizados. Los empleados deben respetar la confidencialidad de la información y no divulgarla a terceros no autorizados. Además, no se debe copiar, eliminar o alterar información sin la autorización correspondiente.

5. **Retiro de acceso:** El acceso a la información debe retirarse cuando el empleado ya no lo necesite para cumplir con sus funciones laborales o si el empleado deja de trabajar para Future Concept SAC. El retiro de acceso se debe realizar de manera oportuna y completa para garantizar que la información no esté expuesta a riesgos innecesarios.

6. **Capacitación y concientización:** Se debe brindar capacitación y concientización a todos los empleados sobre las políticas y procedimientos para el acceso y manejo de la información. La capacitación se debe ofrecer regularmente para garantizar que todos los empleados estén al tanto de las mejores prácticas de seguridad de la información.

IV. Cumplimiento:

Todos los empleados, contratistas, consultores y otros terceros que accedan, manejen o procesen información en nombre de Future Concept SAC deben cumplir con las políticas y procedimientos establecidos para el acceso y manejo de la información. El incumplimiento de estas políticas y procedimientos puede resultar en acciones disciplinarias y legales.

INSTRUCTIVO 4: Instrucciones para las políticas de contraseñas en Future Concept SAC:

I. Objetivo:

Establecer políticas y procedimientos para garantizar que todas las contraseñas utilizadas en la organización sean seguras y estén protegidas adecuadamente.

II. Alcance:

Estas políticas se aplican a todos los empleados, contratistas y terceros que utilizan contraseñas para acceder a los sistemas y datos de Future Concept SAC.

III. Procedimientos:

1. **Requisitos de complejidad de la contraseña:** Todas las contraseñas deben cumplir los siguientes requisitos:

    a. Tener una longitud mínima de 8 caracteres.
    b. Incluir al menos una letra mayúscula y una letra minúscula.
    c. Incluir al menos un número o un símbolo.

2. **Cambio de contraseñas:** Las contraseñas deben cambiarse cada 90 días. Los usuarios deben ser notificados con anticipación para que puedan cambiar sus contraseñas antes de que expiren.

3. **Prohibición de compartir contraseñas:** Las contraseñas nunca deben compartirse con terceros, incluyendo otros empleados o contratistas de Future Concept SAC.

4. **Almacenamiento seguro de contraseñas:** Las contraseñas nunca deben almacenarse en texto plano. Deben ser almacenadas de forma segura, utilizando técnicas de encriptación adecuadas.

5. **Uso de contraseñas fuertes para cuentas de administrador:** Las cuentas de administrador deben utilizar contraseñas especialmente fuertes para proteger los sistemas críticos de Future Concept SAC.

6. **Restricción de intentos de inicio de sesión:** El sistema debe estar configurado para bloquear automáticamente una cuenta después de un número específico de intentos de inicio de sesión fallidos.

7. **Verificación de integridad de la contraseña:** Los sistemas deben verificar la integridad de la contraseña para evitar el uso de contraseñas que hayan sido comprometidas anteriormente.

8. **Notificación de violaciones de seguridad:** Los empleados deben estar capacitados para notificar cualquier sospecha de violación de seguridad o compromiso de contraseñas a la gerencia de seguridad de la información.

IV. Conclusión

Estas políticas y procedimientos ayudarán a garantizar que las contraseñas utilizadas por Future Concept SAC sean seguras y estén protegidas adecuadamente. Todos los empleados, contratistas y terceros que utilicen contraseñas en la organización deben seguir estas políticas y procedimientos en todo momento.

INSTRUCTIVO 5: Instructivo para la política de protección de los activos de información en Future Concept SAC.

I. Objetivo:

Este instructivo tiene como objetivo establecer las medidas de protección necesarias para garantizar la seguridad de los activos de información en Future Concept SAC.

II. Alcance:

Este instructivo se aplica a todos los empleados y contratistas de Future Concept SAC que tienen acceso a los activos de información de la organización.

III. Procedimientos:

1. **Clasificación de los activos de información:** se deben clasificar todos los activos de información según su importancia y su nivel de sensibilidad. La clasificación debe basarse en factores como la confidencialidad, integridad y disponibilidad de la información.

2. **Acceso y control de los activos de información:** se deben establecer controles de acceso a los activos de información según su clasificación. Los controles pueden incluir la autenticación, autorización y supervisión de los usuarios que acceden a los activos de información.

3. **Uso adecuado de los activos de información:** se debe establecer una política clara sobre el uso adecuado de los activos de información. Los empleados y contratistas deben ser conscientes de las políticas y los procedimientos que deben seguir para utilizar los activos de información de la organización.

4. **Protección física de los activos de información:** se deben establecer medidas de protección física para los activos de información. Estas medidas pueden incluir la restricción del acceso físico a los activos de información y la protección contra robos, incendios o daños ambientales.

5. **Protección lógica de los activos de información:** se deben establecer medidas de protección lógica para los activos de información. Estas medidas pueden incluir la protección contra virus informáticos, ataques cibernéticos y otros riesgos de seguridad.

6. **Uso de medios de almacenamiento y transporte seguros:** se deben establecer medidas para el uso seguro de medios de almacenamiento y

transporte de información, como discos duros externos, USB o correos electrónicos. Los empleados y contratistas deben utilizar solo medios autorizados y protegidos adecuadamente.

7. **Procedimientos de eliminación segura de información:** se deben establecer procedimientos para la eliminación segura de los activos de información cuando ya no sean necesarios. Estos procedimientos deben garantizar que la información se elimine de manera segura y que no se pueda recuperar.

IV. Conclusiones:

La implementación de políticas y medidas de protección adecuadas para los activos de información es esencial para garantizar la seguridad de la información en Future Concept SAC. Es importante que todos los empleados, contratistas y terceros estén comprometidos con la seguridad de la información y cumplan con las políticas y medidas establecidas.

INSTRUCTIVO 6: Instructivo para la política de seguridad de red en Future Concept SAC

I. Objetivo:

Garantizar la seguridad de la red de Future Concept SAC y la información que se transmite a través de ella.

II. Alcance:

Esta política se aplica a todos los dispositivos de red, incluidos los dispositivos móviles, que se utilizan para acceder a la red de Future Concept SAC.

III. Procedimientos:

1. **Protección de la red:** Se deben implementar medidas de seguridad técnicas, administrativas y físicas para proteger la red de Future Concept SAC. Estas medidas pueden incluir, entre otras:

    a. Firewalls.
    b. Filtro de paquetes.
    c. Antivirus y software antimalware.
    d. Actualización regular de parches y actualizaciones de seguridad.
    e. Segregación y segmentación de redes.
    f. Control de acceso a la red.
    g. Monitoreo y registro de actividades en la red.
    h. Verificación de la seguridad de los dispositivos móviles que acceden a la red de Future Concept SAC.

2. **Acceso a la red:** Solo se debe permitir el acceso a la red de Future Concept SAC a los empleados autorizados que lo necesiten para desempeñar sus funciones laborales. Los empleados deben autenticarse antes de obtener acceso a la red y se deben establecer niveles de acceso apropiados para cada empleado.

3. **Monitoreo y registro de actividades:** Se debe monitorear y registrar toda la actividad de la red de Future Concept SAC para detectar posibles amenazas y violaciones de seguridad. Se deben establecer políticas claras sobre el uso aceptable de la red y se debe capacitar a los empleados sobre estas políticas.

4. **Respuesta a incidentes:** Se debe establecer un plan de respuesta a incidentes para abordar cualquier posible violación de seguridad de la red. Este plan debe incluir la identificación de posibles amenazas, la

asignación de responsabilidades de respuesta y la definición de procesos de comunicación y notificación.

5. **Continuidad del negocio:** Se deben implementar medidas de continuidad del negocio para garantizar que la red de Future Concept SAC siga funcionando en caso de un incidente de seguridad. Estas medidas pueden incluir, entre otras, la realización de copias de seguridad regulares de la información crítica y la implementación de un plan de recuperación ante desastres.

IV. Conclusión:

La política de seguridad de la red de Future Concept SAC es fundamental para garantizar la seguridad de la información transmitida a través de la red. La protección de la red y la implementación de medidas de seguridad apropiadas son esenciales para garantizar que la red siga funcionando sin interrupciones. La autenticación de los usuarios y la implementación de niveles de acceso apropiados son importantes para proteger la información de la organización y minimizar los riesgos de seguridad. El monitoreo y registro de actividades y la implementación de medidas de continuidad del negocio son esenciales para garantizar que la red de Future Concept SAC siga funcionando en caso de un incidente de seguridad.

<u>INSTRUCTIVO 7:</u> Instrucciones para la gestión de incidentes de seguridad de la información en Future Concept SAC.

I. Objetivo:

El objetivo de estas instrucciones es establecer un proceso para la gestión de incidentes de seguridad de la información en Future Concept SAC, con el fin de minimizar los daños y restaurar los servicios afectados en caso de un incidente de seguridad de la información.

II. Alcance:

Estas instrucciones son aplicables a todos los empleados y contratistas de Future Concept SAC que trabajan con información de la organización.

III. Procedimientos:

1. **Notificación de incidentes:** Cualquier empleado o contratista que observe un incidente de seguridad de la información debe notificarlo inmediatamente a la instancia de seguridad de la información de Future Concept SAC, que está a cargo del área de operaciones.

2. **Evaluación inicial:** La instancia de seguridad de la información de Future Concept SAC debe realizar una evaluación inicial del incidente para determinar su naturaleza, alcance y posibles impactos.

3. **Contención:** Se deben tomar medidas inmediatas para contener el incidente y minimizar su impacto. Esto puede incluir la suspensión de servicios o el aislamiento de sistemas afectados.

4. **Investigación:** Se debe llevar a cabo una investigación exhaustiva del incidente para determinar su causa raíz y cómo se pudo prevenir en el futuro.

5. **Notificación y comunicación:** Se debe notificar a las partes interesadas afectadas por el incidente y comunicar los resultados de la investigación. Esto puede incluir clientes, proveedores y otras partes relacionadas.

6. **Restablecimiento:** Se deben tomar medidas para restaurar los servicios afectados y minimizar el impacto en la organización. Esto puede incluir la recuperación de datos, la restauración de sistemas y la reparación de equipos.

7. **Análisis de lecciones aprendidas:** Después del incidente, se debe realizar un análisis de lecciones aprendidas para identificar áreas de mejora y oportunidades para fortalecer las medidas de seguridad de la información en Future Concept SAC.

8. **Actualización de políticas y procedimientos:** Las políticas y procedimientos de seguridad de la información de Future Concept SAC deben actualizarse según corresponda para abordar las áreas de mejora identificadas en el análisis de lecciones aprendidas.

IV. Actualización:

Estas instrucciones para la gestión de incidentes de seguridad de la información en Future Concept SAC deben revisarse y actualizarse regularmente para asegurar su eficacia y relevancia.

INSTRUCTIVO 8: Instrucciones para el manejo de copias de seguridad y restauración en Future Concept SAC

I. **Objetivo:**

El presente instructivo tiene como finalidad establecer los procedimientos y medidas necesarios para garantizar la realización adecuada de las copias de seguridad de la información y su correspondiente restauración en caso de interrupción del servicio.

II. **Alcance:**

Este instructivo es aplicable a todos los empleados y contratistas de Future Concept SAC que manejan y/o administran información en sistemas y dispositivos informáticos, así como también a los equipos de TI responsables de la gestión de copias de seguridad y restauración.

III. Procedimientos:

1. **Planificación de la copia de seguridad:** Se debe realizar una planificación adecuada para la realización de copias de seguridad, la cual debe incluir la frecuencia de realización de copias, el tipo de copia de seguridad que se realizará y el medio de almacenamiento a utilizar. Además, se deben definir los procedimientos de recuperación y las pruebas para verificar la efectividad de las copias de seguridad.

2. **Selección del medio de almacenamiento:** Se debe seleccionar un medio de almacenamiento confiable y seguro para almacenar las copias de seguridad, tales como discos duros externos, dispositivos de almacenamiento en red (NAS) o servicios de almacenamiento en la nube.

3. **Realización de copias de seguridad:** Las copias de seguridad deben ser realizadas de manera regular, de acuerdo con la planificación previamente establecida. Para ello, se debe utilizar software de copia de seguridad o herramientas específicas para realizar copias de seguridad en línea de comandos.

4. **Verificación de las copias de seguridad:** Se deben realizar pruebas regulares para verificar la integridad y calidad de las copias de seguridad realizadas. Además, se deben verificar las copias de seguridad con regularidad para asegurar que se hayan realizado correctamente y que se puedan restaurar sin problemas.

5. **Protección de las copias de seguridad:** Se deben tomar medidas adecuadas para proteger las copias de seguridad, como la utilización de contraseñas seguras y la implementación de medidas de seguridad físicas para evitar su pérdida, robo o daño.

6. **Procedimientos de restauración:** Se deben establecer procedimientos claros para la restauración de copias de seguridad en caso de una interrupción del servicio o pérdida de datos. Estos procedimientos deben ser conocidos por todo el personal involucrado en la gestión de copias de seguridad y restauración.

7. **Pruebas de restauración:** Se deben realizar pruebas regulares para verificar la efectividad de las copias de seguridad y los procedimientos de restauración. Estas pruebas deben ser realizadas por personal capacitado y deben documentarse adecuadamente.

8. **Actualización de las copias de seguridad:** Las copias de seguridad deben actualizarse regularmente para garantizar que se incluyan los datos más recientes. Se deben establecer procedimientos claros para la actualización de las copias de seguridad y se deben seguir rigurosamente para garantizar la integridad de la información.

IV. Conclusión

El manejo adecuado de las copias de seguridad y su correspondiente restauración son fundamentales para garantizar la continuidad del negocio en caso de una interrupción del servicio o pérdida de datos. Por lo tanto, es importante seguir los procedimientos establecidos y realizar pruebas regulares para garantizar la efectividad de las copias de seguridad y los procedimientos

INSTRUCTIVO 9: Instrucciones para el análisis y monitoreo de la seguridad de la información en Future Concept SAC

I. Objetivo:

Este instructivo tiene como objetivo establecer los procedimientos para el análisis y monitoreo de la seguridad de la información en Future Concept SAC, con el fin de detectar y prevenir posibles incidentes de seguridad y mejorar continuamente los controles de seguridad.

II. Alcance:

Este instructivo se aplica a todas las áreas y usuarios de Future Concept SAC que manejen información de la organización.

III. Procedimientos:

1. **Identificación de los puntos críticos:** Identificar los puntos críticos en la infraestructura de la organización, como servidores, bases de datos y aplicaciones, que requieran un monitoreo constante para detectar posibles amenazas y vulnerabilidades.

2. **Selección de herramientas de monitoreo:** Seleccionar herramientas de monitoreo adecuadas para cada punto crítico que permitan recopilar y analizar información relevante para la seguridad de la información.

3. **Establecimiento de umbrales de alerta:** Establecer umbrales de alerta para cada herramienta de monitoreo, de modo que se active una alerta cuando se detecte una actividad inusual o sospechosa en los puntos críticos.

4. **Análisis de las alertas:** Cuando se reciba una alerta, se debe analizar la información recopilada para determinar si se trata de una amenaza real o de una falsa alarma.

5. **Acciones ante incidentes:** En caso de confirmar un incidente de seguridad, se deben tomar las medidas necesarias para mitigar los efectos del incidente y prevenir su propagación. Se debe establecer un procedimiento específico para cada tipo de incidente, que contemple la notificación a las personas involucradas y la recuperación de los datos afectados.

6. **Monitoreo constante:** Se debe monitorear constantemente la seguridad de la información de la organización, realizando revisiones periódicas de

los controles de seguridad y actualizando los procedimientos de monitoreo y análisis en función de las nuevas amenazas y vulnerabilidades.

7. **Registro de incidentes:** Mantener un registro detallado de todos los incidentes de seguridad detectados y las acciones tomadas para resolverlos, con el fin de realizar un seguimiento y evaluación de la efectividad de las medidas implementadas.

IV. Conclusiones

El análisis y monitoreo de la seguridad de la información es un proceso fundamental para detectar y prevenir posibles incidentes de seguridad en Future Concept SAC. La implementación de herramientas de monitoreo adecuadas y el establecimiento de procedimientos claros para el análisis y gestión de incidentes permitirán mejorar la seguridad de la información y garantizar la continuidad del negocio. Es importante recordar la importancia de mantenerse actualizado ante las nuevas amenazas y vulnerabilidades y adaptar continuamente los controles de seguridad para proteger la información de la organización.

INSTRUCTIVO 10: Instructivo para realizar pruebas de seguridad en Future Concept SAC

I. Objetivo:

El presente instructivo tiene como objetivo establecer los procedimientos necesarios para llevar a cabo pruebas de seguridad en Future Concept SAC, con el fin de identificar posibles vulnerabilidades y riesgos en los sistemas y aplicaciones utilizados por la organización.

II. Alcance:

Este instructivo es aplicable a todos los sistemas y aplicaciones utilizados en Future Concept SAC y a cualquier persona que realice pruebas de seguridad en la organización.

III. Procedimientos:

1. **Planificación de la prueba de seguridad:**

    a. Identificar los sistemas y aplicaciones que se someterán a prueba.
    b. Definir el alcance de la prueba y los objetivos específicos a lograr.
    c. Establecer un cronograma para la realización de la prueba de seguridad.
    d. Identificar al personal encargado de llevar a cabo las pruebas y definir sus roles y responsabilidades.

2. **Recopilación de información:**

    a. Obtener información sobre los sistemas y aplicaciones que se someterán a prueba, como la arquitectura, configuración, software y hardware utilizados.
    b. Realizar una evaluación de los sistemas y aplicaciones para identificar posibles vulnerabilidades.

3. **Análisis de vulnerabilidades:**

    a. Utilizar herramientas de análisis de vulnerabilidades para identificar posibles vulnerabilidades en los sistemas y aplicaciones.
    b. Realizar pruebas de penetración para verificar la explotabilidad de las vulnerabilidades identificadas.

4. **Evaluación de riesgos:**

a. Evaluar el riesgo asociado con cada vulnerabilidad identificada.
b. Priorizar las vulnerabilidades de acuerdo con su criticidad y el impacto potencial en la organización.

5. **Reporte de resultados:**

a. Documentar los resultados de las pruebas de seguridad, incluyendo las vulnerabilidades identificadas y las recomendaciones para mitigar los riesgos.
b. Presentar los resultados a la dirección de la organización y a los responsables de los sistemas y aplicaciones evaluados.
c. Establecer un plan de acción para abordar las vulnerabilidades identificadas y mitigar los riesgos asociados.

6. **Monitoreo y seguimiento:**

a. Realizar monitoreo continuo de los sistemas y aplicaciones para detectar posibles vulnerabilidades y riesgos.
b. Realizar pruebas de seguridad periódicas para verificar que las medidas de mitigación implementadas sean efectivas y adecuadas.

IV. Conclusiones:

La realización de pruebas de seguridad es fundamental para garantizar la protección de los sistemas y aplicaciones utilizados en la organización. Siguiendo este instructivo, Future Concept SAC podrá identificar vulnerabilidades y riesgos potenciales en sus sistemas y aplicaciones, así como establecer medidas de mitigación para garantizar la seguridad de la información en todo momento.

<u>INSTRUCTIVO 11</u>: Instrucciones para el cumplimiento legal y contractual en Future Concept SAC

I. Objetivo:

El objetivo de estas instrucciones es garantizar que Future Concept SAC cumpla con todas las leyes, regulaciones y acuerdos contractuales que se aplican a la empresa y a la información que maneja.

II. Alcance:

Estas instrucciones se aplican a todas las áreas de la empresa que manejan información, incluyendo el personal, los sistemas y los procesos.

III. Procedimientos:

1. **Identificación de los requisitos legales y contractuales:** se debe realizar una lista completa de todas las leyes, regulaciones y acuerdos contractuales que se aplican a la empresa y a la información que maneja.

2. **Evaluación del cumplimiento:** una vez identificados los requisitos, se debe realizar una evaluación para determinar si se están cumpliendo. Esta evaluación debe ser realizada de forma periódica.

3. **Implementación de medidas para cumplir con los requisitos:** en caso de que se identifiquen áreas en las que no se está cumpliendo con los requisitos, se deben implementar medidas para garantizar el cumplimiento. Estas medidas pueden incluir cambios en los procesos, sistemas y políticas, así como capacitación del personal.

4. **Revisión de los contratos y acuerdos:** se debe realizar una revisión periódica de los contratos y acuerdos que se tienen con terceros, para garantizar que se estén cumpliendo los requisitos contractuales en términos de seguridad de la información.

5. **Actualización de las políticas y procedimientos:** en caso de que se identifiquen cambios en las leyes y regulaciones que afecten a la empresa y a la información que maneja, se deben actualizar las políticas y procedimientos para garantizar el cumplimiento.

6. **Establecimiento de controles:** Se deben establecer los siguientes controles:

a. **Documentación de las políticas y procedimientos:** se debe mantener una documentación actualizada de todas las políticas y procedimientos que se aplican al cumplimiento legal y contractual.
b. **Capacitación del personal:** se debe capacitar al personal para que comprenda los requisitos legales y contractuales que se aplican a la empresa y a la información que maneja.
c. **Supervisión y monitoreo:** se deben establecer mecanismos de supervisión y monitoreo para garantizar que se cumplan los requisitos legales y contractuales.

IV. Conclusión:

El cumplimiento legal y contractual es esencial para garantizar la seguridad de la información y la continuidad del negocio. Future Concept SAC debe implementar medidas para garantizar el cumplimiento de todas las leyes, regulaciones y acuerdos contractuales que se aplican a la empresa y a la información que maneja.

<u>LINEAMIENTOS CONTRACTUALES 1:</u> Cláusulas Contractuales para Colaboradores Terceros y Contratistas en torno los de Softwares a Service (SaaS) que desarrolla Future Concept SAC

En caso de que el contratista, tercero o colaborador utilice algún Software as a Service proporcionado por Future Concept SAC, se compromete a cumplir con las siguientes cláusulas:

I. **CLÁUSULA 1: USO DEL SOFTWARE.** El contratista, tercero o colaborador se compromete a usar el software proporcionado por Future Concept SAC conforme a las siguientes directrices:

1. Utilizar el software únicamente para los fines establecidos en el contrato y en cumplimiento de la política y reglamento de seguridad de información de Future Concept SAC.
2. No transferir, ceder o sublicenciar el uso del software a terceros sin la autorización previa y por escrito de Future Concept SAC.
3. Informar de inmediato a Future Concept SAC cualquier incidente de seguridad relacionado con el software as a Service, proporcionando toda la información necesaria para su análisis y solución.
4. Cumplir con las políticas de privacidad y protección de datos del software as a Service proporcionado por Future Concept SAC.
5. Utilizar contraseñas seguras y robustas para el acceso al software, evitando compartirlas con terceros y notificando de inmediato cualquier sospecha de compromiso de sus credenciales.

II. **CLÁUSULA 2: DURACIÓN DEL CONTRATO.** El contratista, tercero o colaborador se compromete a cumplir con las cláusulas establecidas en este documento durante toda la vigencia del contrato, incluyendo los periodos de prórroga o renovación de este.

III. **CLÁUSULA 3: INCUMPLIMIENTO DE LAS CLÁUSULAS.** En caso de que el contratista, tercero o colaborador incumpla con alguna de las cláusulas establecidas en este documento, Future Concept SAC se reserva el derecho de tomar las medidas necesarias para proteger sus activos de información y garantizar el cumplimiento de la política y reglamento de seguridad de información, incluyendo la terminación anticipada del contrato.

IV. **CLÁUSULA 4: JURISDICCIÓN Y LEY APLICABLE.** Este contrato estará regido e interpretado de acuerdo con las leyes de la jurisdicción correspondiente a la ubicación de Future Concept SAC, y las partes se someten a la jurisdicción exclusiva de los tribunales de dicha jurisdicción.

Este documento forma parte integrante del contrato entre Future Concept SAC y el contratista, tercero o colaborador, y debe ser firmado por ambas partes como anexo al contrato principal.

<u>LINEAMIENTOS CONTRACTUALES 2:</u> Cláusulas para incluir en el contrato del Colaborador

I. **CLÁUSULA 1: CUMPLIMIENTO.** El colaborador se compromete a cumplir con la política y reglamento de seguridad de información de Future Concept SAC en todo momento durante la vigencia del contrato. Asimismo, se compromete a seguir todos los procesos y procedimientos establecidos por Future Concept SAC para garantizar la seguridad de la información y la privacidad de los datos.

II. **CLÁUSULA 2: USO DE LA INFORMACIÓN.** El colaborador se compromete a utilizar la información proporcionada por Future Concept SAC única y exclusivamente para los fines establecidos en el contrato. Asimismo, se compromete a mantener la confidencialidad y privacidad de la información, así como a no revelarla, transferirla o utilizarla para fines distintos a los acordados.

III. **CLÁUSULA 3: PROTECCIÓN DE LOS ACTIVOS.** El colaborador se compromete a proteger los activos de información de Future Concept SAC, tanto físicos como electrónicos, que se encuentren bajo su custodia, evitando su pérdida, robo, modificación, divulgación o destrucción no autorizada. Asimismo, se compromete a reportar cualquier incidente de seguridad de información que ocurra en el desarrollo de sus actividades.

IV. **CLÁUSULA 4: USO DE CONTRASEÑAS.** El colaborador se compromete a utilizar contraseñas seguras y robustas para el acceso a los sistemas y aplicaciones de Future Concept SAC, evitando compartir sus credenciales de acceso con terceros. Asimismo, se compromete a cambiar regularmente sus contraseñas y a notificar de inmediato cualquier sospecha de compromiso de sus credenciales.

V. **CLÁUSULA 5: USO DE REDES Y SISTEMAS.** El colaborador se compromete a utilizar las redes y sistemas de Future Concept SAC únicamente para los fines establecidos en el contrato, evitando el acceso no autorizado, la introducción de virus, malware o cualquier otro código malicioso en los sistemas de Future Concept SAC. Asimismo, se compromete a reportar cualquier incidente de seguridad de red que detecte.

VI. **CLÁUSULA 6: NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD.** El colaborador se compromete a notificar de inmediato a Future Concept SAC cualquier incidente de seguridad de información que detecte durante el desarrollo de sus actividades, proporcionando toda la información necesaria para su análisis y solución.

VII. **CLÁUSULA 7. SEGUIMIENTO.** El colaborador se compromete a cooperar plenamente con Future Concept SAC en cualquier investigación o auditoría relacionada con la seguridad de la información, proporcionando toda la información requerida y colaborando en la implementación de cualquier acción correctiva que se requiera.

VIII. **CLÁUSULA 8: INCUMPLIMIENTO DE CLÁUSULAS.** El colaborador reconoce y acepta que el incumplimiento de cualquier cláusula de seguridad de información establecida en este contrato puede ser causa de rescisión del contrato y puede tener consecuencias legales y financieras adversas tanto para el colaborador como para Future Concept SAC.

IX. **CLÁUSULA 9: DEVOLUCIÓN DE ACTIVOS DE INFORMACIÓN.** El colaborador reconoce y acepta que, en caso de rescisión del contrato, debe devolver a Future Concept SAC toda la información, materiales y activos de información bajo su custodia, así como cualquier copia o registro de esta.

X. **CLÁUSULA 10. DERECHO DE MODIFICACIÓN Y ACTUALIZACIÓN.** El colaborador reconoce y acepta que Future Concept SAC se reserva el derecho de modificar y actualizar las cláusulas de seguridad de información establecidas en este contrato en cualquier momento, y que es responsabilidad del colaborador estar al tanto de cualquier cambio y cumplir con las nuevas disposiciones establecidas.

<u>LINEAMIENTOS CONTRACTUALES 3:</u> Cláusulas de Future Concept SAC para contratos con terceros

I. **CLÁUSULA 1: CONFIDENCIALIDAD.** El tercero se compromete a mantener la confidencialidad y privacidad de toda la información a la que tenga acceso en virtud del contrato, ya sea de forma verbal, escrita, electrónica o en cualquier otro formato.

II. **CLÁUSULA 2: PROTECCIÓN DE LA INFORMACIÓN.** El tercero se compromete a proteger los activos de información de Future Concept SAC, tanto físicos como electrónicos, que se encuentren bajo su custodia, evitando su pérdida, robo, modificación, divulgación o destrucción no autorizada.

III. **CLÁUSULA 3: USO DE LA INFORMACIÓN.** El tercero se compromete a utilizar la información proporcionada por Future Concept SAC única y exclusivamente para los fines establecidos en el contrato y no para ningún otro fin, sin la autorización expresa y por escrito de Future Concept SAC.

IV. **CLÁUSULA 4: ACCESO A LA INFORMACIÓN.** El tercero se compromete a utilizar la información y los sistemas de Future Concept SAC únicamente para los fines establecidos en el contrato y a no acceder a ninguna otra información o sistema sin la autorización expresa y por escrito de Future Concept SAC.

V. **CLÁUSULA 5: POLÍTICA DE CONTRASEÑAS.** El tercero se compromete a utilizar contraseñas seguras y robustas para el acceso a los sistemas y aplicaciones de Future Concept SAC, evitando compartir sus credenciales de acceso con terceros. Asimismo, se compromete a cambiar regularmente sus contraseñas y a notificar de inmediato cualquier sospecha de compromiso de sus credenciales.

VI. **CLÁUSULA 6: GESTIÓN DE INCIDENTES.** El tercero se compromete a notificar de inmediato a Future Concept SAC cualquier incidente de seguridad de información que detecte durante el desarrollo de sus actividades, proporcionando toda la información necesaria para su análisis y solución.

VII. **CLÁUSULA 7: CUMPLIMIENTO NORMATIVO.** El tercero se compromete a cumplir con todas las leyes y regulaciones aplicables en relación con la seguridad de la información, incluyendo, sin limitación, la normativa de protección de datos personales.

VIII. **CLÁUSULA 8: AUDITORÍA.** Future Concept SAC se reserva el derecho a auditar la seguridad de la información del tercero en cualquier momento durante la vigencia del contrato, con el fin de asegurarse de que el tercero está cumpliendo con las obligaciones establecidas en el contrato.

IX. **CLÁUSULA 9: DURACIÓN DEL COMPROMISO.** Las obligaciones establecidas en el contrato se mantendrán vigentes mientras el tercero tenga acceso a la

información o sistemas de Future Concept SAC, incluso después de la finalización del contrato.

<u>LINEAMIENTOS CONTRACTUALES 4:</u> Cláusulas de Seguridad de Información para Contratistas de Future Concept SAC

Este documento tiene como objetivo establecer las cláusulas que deben ser incluidas en los contratos con contratistas que trabajen con Future Concept SAC, para garantizar el cumplimiento de la política y reglamento de seguridad de información, así como las especificaciones relacionadas con el uso de software y hardware propiedad de la empresa.

I. **CLÁUSULA 1: POLÍTICA Y REGLAMENTO DE SEGURIDAD DE INFORMACIÓN.** El contratista se compromete a cumplir con la política y reglamento de seguridad de información de Future Concept SAC, en todo momento durante la vigencia del contrato.

II. **CLÁUSULA 2: ACCESO A LA INFORMACIÓN.** El contratista debe comprometerse a utilizar la información proporcionada por Future Concept SAC única y exclusivamente para los fines establecidos en el contrato. Asimismo, se compromete a mantener la confidencialidad y privacidad de la información, así como a no revelarla, transferirla o utilizarla para fines distintos a los acordados.

III. **CLÁUSULA 3: PROTECCIÓN DE LOS ACTIVOS DE INFORMACIÓN.** El contratista se compromete a proteger los activos de información de Future Concept SAC, tanto físicos como electrónicos, que se encuentren bajo su custodia, evitando su pérdida, robo, modificación, divulgación o destrucción no autorizada. Asimismo, se compromete a reportar cualquier incidente de seguridad de información que ocurra en el desarrollo de sus actividades.

IV. **CLÁUSULA 4: POLÍTICA DE CONTRASEÑAS.** El contratista se compromete a utilizar contraseñas seguras y robustas para el acceso a los sistemas y aplicaciones de Future Concept SAC, evitando compartir sus credenciales de acceso con terceros. Asimismo, se compromete a cambiar regularmente sus contraseñas y a notificar de inmediato cualquier sospecha de compromiso de sus credenciales.

V. **CLÁUSULA 5: SEGURIDAD DE LA RED.** El contratista se compromete a utilizar las redes y sistemas de Future Concept SAC únicamente para los fines establecidos en el contrato, evitando el acceso no autorizado, la introducción de virus, malware o cualquier otro código malicioso en los sistemas de Future Concept SAC. Asimismo, se compromete a reportar cualquier incidente de seguridad de red que detecte.

VI. **CLÁUSULA 6: GESTIÓN DE INCIDENTES DE SEGURIDAD DE INFORMACIÓN.** El contratista se compromete a notificar de inmediato a Future Concept SAC cualquier incidente de seguridad de información que detecte durante el desarrollo de sus actividades, proporcionando toda la información necesaria para su análisis y solución.

VII. **CLÁUSULA 7: AUDITORÍAS DE SEGURIDAD DE INFORMACIÓN.** Future Concept SAC se reserva el derecho de realizar auditorías de seguridad de información al contratista durante la vigencia del contrato, con el fin de verificar el cumplimiento de las cláusulas de seguridad de información establecidas en este documento. El contratista se compromete a colaborar activamente en las auditorías y a proporcionar toda la información necesaria.

VIII. **CLÁUSULA 8: CONFIDENCIALIDAD.** El contratista se compromete a mantener la confidencialidad de toda la información confidencial de Future Concept SAC a la que tenga acceso durante el desarrollo del contrato, y no revelarla, transferirla o utilizarla para fines distintos a los acordados.

IX. **CLÁUSULA 9: PROPIEDAD.** El contratista reconoce que todo el software y hardware propiedad de Future Concept SAC y utilizado en el desarrollo del contrato, sigue siendo propiedad exclusiva de Future Concept SAC y no adquiere ningún derecho de propiedad sobre el mismo.

X. **CLÁUSULA 10: TERMINACIÓN DEL CONTRATO.** Este contrato podrá ser terminado por cualquiera de las partes mediante notificación por escrito a la otra parte con una anticipación mínima de treinta (30) días calendario. Al terminar el contrato se deben seguir las siguientes directrices

1. Si este contrato es terminado por cualquiera de las partes, el contratista deberá entregar a Future Concept SAC toda la información, documentación y materiales proporcionados por Future Concept SAC, así como cualquier otro activo de propiedad de Future Concept SAC en su poder, en un plazo máximo de cinco (5) días hábiles contados a partir de la fecha de terminación del contrato.

2. El contratista reconoce que la terminación del contrato no le exime de las obligaciones de confidencialidad, seguridad de la información y protección de los activos de Future Concept SAC que haya adquirido durante la vigencia del contrato, y que seguirá siendo responsable de cualquier incumplimiento de dichas obligaciones.

3. La terminación del contrato no eximirá al contratista de cualquier responsabilidad que haya contraído con Future Concept SAC antes de la fecha de terminación, y será responsable por cualquier daño, pérdida o perjuicio causado por el incumplimiento de sus obligaciones contractuales hasta el momento de la terminación del contrato.

XI. **CLÁUSULA 11: LEY APLICABLE.** Este contrato se regirá e interpretará de acuerdo con las leyes de la República del Perú, sin consideración a sus principios de conflicto de leyes.

XII. **CLÁUSULA 12: RESOLUCIÓN DE CONTROVERSIAS.** Cualquier controversia, conflicto o reclamación que surja de o en relación con este contrato, incluyendo

cualquier cuestión relativa a su existencia, validez, interpretación, ejecución, incumplimiento o resolución, será sometida a arbitraje de acuerdo con las normas del Centro de Arbitraje de la Cámara de Comercio de Lima, y se resolverá definitivamente de acuerdo con el laudo arbitral emitido en el procedimiento arbitral. La sede del arbitraje será en la ciudad de Lima, Perú, y el idioma de arbitraje será el español.

XIII. **CLÁUSULA 13: COMPENSACIÓN.** Las partes acuerdan renunciar a cualquier derecho a reclamar o buscar cualquier compensación o indemnización en relación con cualquier daño indirecto, especial, incidental o consecuencial, incluyendo, sin limitación, la pérdida de beneficios o ingresos, o el costo de reemplazo o reparación de cualquier equipo, propiedad o información, que surja de o en relación con este contrato. La renuncia a estos derechos no limita la capacidad de las partes para buscar compensación por cualquier daño directo que puedan sufrir.

LINEAMIENTOS CONTRACTUALES 5: Cláusulas para empresas consultoras de sostenibilidad que actúan como proveedor de servicios para un tercero, brindando sus servicios de generación de reportes de sostenibilidad haciendo uso del software Autonomouz Sostenible

I. **CLÁUSULA 1: CONFIDENCIALIDAD.** La empresa consultora de sostenibilidad que utiliza la modalidad máster de Autonomouz Sostenible para la gestión de portafolio de cuentas corporativas, se compromete a mantener la confidencialidad de la información proporcionada por sus clientes, incluyendo la información contenida en el software Autonomouz Sostenible. Además, deberá asegurar que sus consultores responsables de cada cuenta y demás personal involucrado en la generación de reportes de sostenibilidad, mantengan la confidencialidad de la información y sólo utilicen la información para fines relacionados con la generación de reportes de sostenibilidad.

II. **CLÁUSULA 2: PROTECCIÓN DE DATOS.** La empresa consultora de sostenibilidad se compromete a cumplir con todas las leyes y regulaciones aplicables en materia de protección de datos, incluyendo la Ley de Protección de Datos Personales y la Ley de Protección de Datos Personales en el Ámbito de las Telecomunicaciones. La empresa consultora de sostenibilidad deberá tomar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales contenidos en el software Autonomouz Sostenible y en los informes de sostenibilidad generados.

III. **CLÁUSULA 3: ACCESO AL SOFTWARE.** FUTURE CONCEPT SAC brinda a la empresa consultora una cuenta Máster para acceder y utilizar el software Autonomouz Sostenible. La empresa consultora deberá asegurar que sus consultores responsables de cada cuenta accedan sólo a la información necesaria para la generación de los reportes de sostenibilidad. Asimismo, la empresa consultora deberá asegurar que el acceso a la cuenta Master sea limitado y controlado, y que se tomen medidas para evitar el acceso no autorizado.

IV. **CLÁUSULA 4: RESPONSABILIDAD.** La empresa consultora será responsable ante FUTURE CONCEPT SAC y sus clientes por cualquier incumplimiento de las obligaciones establecidas en el contrato y por cualquier daño o perjuicio que cause a FUTURE CONCEPT SAC o sus clientes en relación con el uso del software Autonomouz Sostenible y la generación de reportes de sostenibilidad.

Lima, 01 de octubre de 2022.