**INSTRUCCIONES PARA AUTOEVALUACIÓN DE CONTROLES PRIORIZADOS DE LA NORMA NCH-ISO 27001-2013**

1. **OBJETIVO**

Entregar instrucciones para evaluar el nivel de madurez, respecto a los controles de la norma NCh-ISO 27001.2013 en los Servicios de Salud y Seremis.

1. **ALCANCE**

Servicios de Salud y Seremis.

1. **INSTRUCCIONES**
	1. **Introducción**

La evaluación del nivel de madurez de los controles priorizados por el Ministerio del Interior, se realizará en base a los controles definidos en el Anexo A de la norma NCh-ISO 27001.2013 y las directrices de implementación definidas en la Guía metodológica de la Red de expertos del Ministerio del Interior[[1]](#footnote-1), y los niveles de madurez basados en prácticas líderes como COBIT, CMMI, entre otras.

* 1. **Proceso**

El proceso de autoevaluación tendrá las siguientes etapas:



* + 1. **Revisión de instrucciones y antecedentes**

Se deberán revisar las presentes instrucciones, junto con las herramientas que se utilizan para la autoevaluación:

* Archivo Excel con el total de controles por dominio que se evaluarán
* Plataforma de encuestas de Minsal.
* Sobre el archivo Excel tiene la siguiente estructura:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **N° Control** | **Identificación del control** | **Requisito de Control NCh-ISO 27001** | **Verificación de Requisito de Control (extracto de NCH-ISO 27002 Of2013)** | **NIVEL DE MADUREZ** | **Archivos Adjuntos** |
| **0. Inexistente** | **1. Básico** | **2. Práctica Repetible** | **3. Proceso formalizado** | **4. Proceso Gestionado** | **5. Proceso resiliente** |
| A.05.01.02 | REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN | Se deben revisar las políticas de seguridad de la información a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia, y eficacia continuas | Estas políticas deberían ser revisadas a intervalos regulares o cuando ocurran cambios que pudieran afectar su idoneidad, eficiencia y efectividad. |   |   |   |   |   |   |   |

1. **AREA GRIS:** se indican los controles, junto con su identificación, requisito de la norma 27001 y las directrices de implementación de la Red de expertos del Ministerio del Interior.
2. **AREA VERDE:** niveles de madurez que deben ser identificados para cada control de la norma 27001, los distintos niveles de madurez están definidos en la siguiente tabla:

|  |  |  |  |
| --- | --- | --- | --- |
| N° | Nombre | **Nivel de Madurez** | Características del Nivel |
| 5 | Resiliente | **5 - Proceso Resiliente** | A este nivel se busca que el proceso siga estando acorde a lo que requiere la Institución, no sólo para atender los actuales requerimientos; sino que permita su proyección al mediano y largo plazo.Se agregan indicadores de Efectividad y Suficiencia, además de los de Operación y Gestión en general.Se ha maximizado la automatización de las actividades relacionadas; existen evidencias periódicas de mejora continua. Se analizan los indicadores a nivel estratégico y no sólo a nivel operativo y táctico.Dado que la Optimización última no existe; si se debe apuntar a un permanente nivel de mejora en la Calidad y Seguridad del proceso; integrando visiones estratégicas y de factibilidad futura; que permita ajustar el proceso a los cambios no sólo de la institución sino de todo su entorno, aportando a perpetuar la Institución.  |
| 4 | Gestionado | **4 - Proceso Gestionado** | Se ha implementado un Proceso de Gestión de Mejora Continua para la formalización previa, por ejemplo basada en Ciclo PDCA de DEMING; donde se reconoce que no basta el Planificar y Ejecutar; sino que se requieren instancias de control permanente que implementen acciones de monitoreo, revisión y auditoria para identificar acciones de mejora.Es posible monitorear y medir el cumplimiento de lo que se ha formalizado como proceso, incluyendo la ejecución adecuada de los procedimientos planteados. Permite identificar GAPs; Brechas; Debilidades; Atrasos; Costos y otras variables que podrían activar KPIs necesarios de vigilar en el tiempo. |
| 3 | Formalizado | **3 - Proceso Formalizado** | Existe un proceso que se puede catalogar como documentado y formalizado.El proceso posee un nombre, cierta codificación. Se identifican otros procesos relacionados, sus subprocesos, actividades y o tareas. Se detallan los recursos necesarios, así como los roles de los participantes y se designan sus responsabilidades (por ejemplo con tablas RACI).Se señalan los flujos de decisiones, así como la prioridad de las acciones.Se formalizan el quehacer concreto o práctica existente, mediante documentos oficiales, que podría incluir: Diagramas de flujo, Organigramas, Procedimientos, Instructivos y Formularios.Se mantiene la documentación del proceso como gran hito; pero no tiene mayor visibilidad sistémica para el resto de la institución; ni menos se piensa en su mejora continua u optimización. |
| 2 | Repetible | **2 - Práctica Repetible** | Existen acuerdos informales entre pares que han tenido que atender alguna situación similar, comenzando a establecer una "práctica común" para situaciones conocidas.No se ha desarrollado un análisis como proceso, no se reconocen recursos necesarios, costos, roles o responsabilidades formales.Existe un acuerdo informal de la "práctica", no existiendo una formalización del procedimiento, es más, no se reconoce como tal; sino sólo como una forma común de realizar tareas o actividades.Es muy dependiente de qué interprete cada persona distinta respecto del Qué se debe hacer, ya que no detalla el Cómo.+E7No se realizan actividades de seguimiento, no existe planificación formal, cada respuesta es propia del caso. |
| 1 | Básico | **1 - Básico** | Existe evidencia que la institución, o ciertos colaboradores en forma aislada, han reconocido que existe cierto problema o situación pendiente y se requiere alguna forma de solucionarlo.Sin embargo; no existe un proceso declarado, menos aún formal, tampoco acuerdos de actividades concretas necesarias. Lo que surge y se puede constatar es que algunas veces, se han realizado esfuerzos particulares, con un enfoques ad-hoc a la instancia a resolver y muy dependiente de quien la ejecuta.Sin un protocolo o acuerdo establecido han existido situaciones en que en forma individual y muy casuística se ha abordado el tema. |
| 0 | Inexistente | **0 - Inexistencia** | Carencia completa de cualquier proceso reconocible. No se ha generado a nivel de institución, ni de colaboradores, un reconocimiento ni acción que se señale se deba hacer algo respecto al tema.No existe visibilidad del problema a resolver. |

**Para evaluar el nivel de madurez que tiene cada control se deben revisar las siguientes variables:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nivel de Madurez** | **Cultura** | **Documentación** | **Registros** | **Roles y Responsabilidades** | **Tecnología** |
| **5 - Proceso Resiliente** | Existe criterio común de mejorar el proceso y está fuertemente arraigado en la cultura de la institución, adaptándose a los cambios del entorno. | El contenido del documento se somete a revisiones periódicas, contrastándolo con casos extremos y particulares, para hacerlo más completo y robusto. | Se registran los resultados del proceso; para mantener trazabilidad y realizar análisis de tendencias. | Además de su actualización, existe revisión de conflicto de intereses y separación de funciones en la gestión de roles y responsabilidades. Se analizan cada vez que se analiza algún cambio mayor, presente o en planificación. | La tecnología es parte integral del proceso y como tal, se proyecta su innovación junto con el análisis de nuevas tendencias y ajustes del proceso. |
| **4 - Proceso Gestionado** | La forma de ejecutar el proceso ya es parte de la cultura de la institución. | Hay evidencias concretas que el documento que referencia al proceso ha sido actualizado. Existe control y sobre las versiones y su distribución. | Se registran los resultados del proceso; para mantener trazabilidad y realizar análisis de tendencias. | Los roles y sus responsabilidades se han revisado y ajustado al menos anualmente. | Existe control de versiones, de distribución de las herramientas tecnológicas y versionamiento de sus manuales. Se controlan los pasos a producción de nuevas versiones. |
| **3 - Proceso Formalizado** | Se comparte formalmente para toda la institución la manera de desarrollar el proceso, para que todos la conozcan. | Existe un documento que referencia al proceso y sus actividades; así como roles y responsabilidades. No se identifican señales de actualización permanente. | Se registran los resultados del proceso; para mantener trazabilidad en el tiempo. | Se formalizan los roles involucrados, su jerarquía estratégica, táctica y operacional; asimismo están claramente establecidas las responsabilidades de cada uno de ellos. | Se he estandarizado una tecnología con una configuración dada y se define un procedimiento para su uso. |
| **2 - Práctica Repetible** | Se comparte sólo entre algunos usuarios involucrados la forma de hacer actividades comunes. | Si bien no se encuentra un documento asociado al proceso, diferentes personas señalan la misma forma de ejecutar las actividades consultadas. | Las acciones del proceso se registras entre los involucrados de forma estandarizada y/o centralizada; a pesar de no existir un documento formal. | Existe acuerdo informal en la distribución de las funciones y se respetan las responsabilidades asociadas; sin mayor cuestionamiento. | Se ha comenzado a usar una cierta tecnología sin un mayor cuestionamiento. |
| **1 - Básico** | Cada usuario con su propia idea | Cuando se ha preguntado, no hay documentación, cada persona involucrada responde algo distinto. | Cada persona tiene su propia forma de registras las cosas. | No existe definición. Cada persona asume el rol y responsabilidades que estime conveniente. | Cada persona busca la tecnología que más le cómoda. |
| **0 - Inexistencia** | No es un tema | No hay documentación referida al proceso. | No existe. | No existe. | No existe como un recurso pensado para el proceso. Si está presente es sólo un caso fortuito. |

Según el grado de cumplimiento de las variables se indicará el nivel de madurez que tiene el control en la institución. **Las variables marcadas en gris, requieren que se evidencie su implementación** mediante, políticas, procedimientos, documentos, junto con los registros que den cuenta de su operación.

1. **AREA AMARILLA:** se deben indicar los nombres de los archivos que dan cuenta de su implementación.
* Sobre la Plataforma de encuestas de Minsal, se encuentra disponible en:

<https://encuestas.minsal.cl> -> Autoevaluación ISO27001





* + 1. **Programación de la autoevaluación**

La autoevaluación, considera diferentes dominios de la norma 27001, por lo que tendrán que distintas áreas deberán revisar los diferentes dominios de la norma, según lo definido en el siguiente cuadro:

|  |  |  |
| --- | --- | --- |
| **DOMINIO** | **N° DE CONTROLES** | **RESPONSABLES** |
| 5 Políticas de seguridad de la información | 2 | Comité de Seguridad / Encargado de Seguridad |
| 6 Organización de la Seguridad de la Información | 3 | Comité de Seguridad / Encargado de Seguridad |
| 7 Seguridad de Recursos Humanos | 1 | Recursos Humanos |
| 8 Administración de Activos | 2 | Área de Administración Interna (responsable de los inventarios) – Área TIC |
| 9 Control de Acceso | 4 | Área TIC |
| 11 Seguridad Física y Ambiental | 6 | Área de Administración Interna (responsable de la Planta Física) |
| 12 Seguridad de las Operaciones | 4 | Área TIC |
| 13 Seguridad en las Comunicaciones | 1 | Área TIC |
| 14 Adquisición, desarrollo y mantenimiento de sistemas | 6 | Área TIC |
| 15 Relaciones con los proveedores | 1 | Área de Administración Interna (responsable de las compras) – Área TIC |
| 16 Administración de incidentes de seguridad de la información | 2 | Comité de Seguridad / Encargado de Seguridad / Área TIC |
| 18 Cumplimiento | 3 | Área Jurídica |
| **TOTAL DE CONTROLES** | **35** |  |

* + 1. **Revisión del nivel de madurez**

Se recomienda revisar los niveles de madurez para cada dominio, en primera instancia mediante el archivo Excel proporcionado y una vez realizada la medición e identificados los registros, realizar la carga de archivos a la plataforma de encuestas de Minsal.

* + 1. **Consolidación y recopilación de registros**

Una vez se tengan los distintos niveles de madurez para cada control, se deberá consolidad la información, en un único archivo Excel, junto con todos los registros que den cuenta del grado de madurez.

* + 1. **Revisión previa a la carga de archivos**

Antes de cargar los resultados y registros de implementación, se deberá revisar la información, para minimizar los posibles errores.

* + 1. **Carga de resultados de autoevaluación**

Cada Servicio de Salud deberá realizar la carga de los resultados de la evaluación y los registros que dan evidencia.

* + 1. **Envío de resultados al NC**

Una vez cargados los resultados y archivos se deberá hacer envío a través de la plataforma al nivel central, además se deberá enviar el archivo Excel consolidado con la medición de los niveles de madurez.

1. Para mayores antecedentes visitar <http://www.dipres.gob.cl/594/w3-propertyvalue-16887.html> [↑](#footnote-ref-1)