# NTT-BCD-01, Sistema de Gestión de la Continuidad del Negocio (BCMS)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Sistema de Gestión de la Continuidad del Negocio (BCMS) | | | | |
| Descripcion Control | Existen mecanismos para facilitar la implementación de controles de planificación de contingencia para ayudar a garantizar activos y servicios resilientes. | | | | |
| Pregunta | ¿La organización facilita la implementación de controles de planificación de contingencia? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias | E-NTT-AST-01 E-NTT-BCM-01 | Iniciativas | | | |

# NTT-BCD-04, Pruebas y ejercicios del plan de contingencia

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Pruebas y ejercicios del plan de contingencia | | | | |
| Descripcion Control | Existen mecanismos para realizar pruebas y/o ejercicios para evaluar la efectividad del plan de contingencia y la preparación de la organización para ejecutar el plan. | | | | |
| Pregunta | ¿La organización realiza pruebas y/o ejercicios para evaluar la efectividad del plan de contingencia y la preparación de la organización para ejecutar el plan? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias | E-NTT-BCM-06 E-NTT-BCM-07 | Iniciativas | | | |

# NTT-BCD-04.1, Pruebas coordinadas con planes relacionados

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Pruebas coordinadas con planes relacionados | | | | |
| Descripcion Control | Existen mecanismos para coordinar las pruebas del plan de contingencia con los elementos internos y externos responsables de los planes relacionados. | | | | |
| Pregunta | ¿La organización coordina las pruebas del plan de contingencia con los elementos internos y externos responsables de los planes relacionados? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias | E-NTT-AST-04 | Iniciativas | | | |

# NTT-BCD-06, Planificación de contingencia y actualizaciones

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Planificación de contingencia y actualizaciones | | | | |
| Descripcion Control | Existen mecanismos para mantener los planes de contingencia actualizados con las necesidades comerciales, los cambios tecnológicos y la retroalimentación de las actividades de prueba del plan de contingencia. | | | | |
| Pregunta | ¿La organización mantiene actualizados los planes de contingencia con las necesidades del negocio, los cambios tecnológicos y la retroalimentación de las actividades de prueba del plan de contingencia? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias | E-NTT-BCM-05 | Iniciativas | | | |

# NTT-CPL-01, Cumplimiento legal, reglamentario y contractual

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Cumplimiento legal, reglamentario y contractual | | | | |
| Descripcion Control | Existen mecanismos para facilitar la identificación e implementación de los controles legales, reglamentarios y contractuales pertinentes. | | | | |
| Pregunta | ¿Existen mecanismos aplicados por la organización para facilitar la identificación e implementación de aquellos controles legales, reglamentarios y contractuales que resulten aplicables en los casos concretos? | Respuesta | | | |
| Valoracion | noSel | Valoracion Objetivo | noSel | | |
| Evidencias | probando1-C | Iniciativas | | | |

# NTT-CPL-02, Supervisión de controles de seguridad y privacidad

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Supervisión de controles de seguridad y privacidad | | | | |
| Descripcion Control | Existen mecanismos para proporcionar una función de supervisión de los controles de seguridad y privacidad que informa al liderazgo ejecutivo de la organización. | | | | |
| Pregunta | ¿La organización supervisa los controles de seguridad y privacidad e informa a la capa ejecutiva de la organización? | Respuesta | | | |
| Valoracion | noSel | Valoracion Objetivo | noSel | | |
| Evidencias | E-NTT-CPL-07 E-NTT-GOV-04 E-NTT-GOV-05 E-NTT-GOV-06 E-NTT-GOV-13 E-NTT-RSK-03 | Iniciativas | | | |

# NTT-CPL-02.1, Función de Auditoría Interna

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Función de Auditoría Interna | | | | |
| Descripcion Control | Existen mecanismos para implementar una función de auditoría interna que sea capaz de proporcionar a la alta dirección de la organización información sobre la adecuación de la tecnología de la organización y los procesos de gobierno de la información. | | | | |
| Pregunta | ¿Realiza la organización auditorías internas que puedan proporcionar a la alta dirección de la organización, información sobre la adecuación de la tecnología que utiliza la organización como de los procesos de gobierno de la información? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-GOV-01, Programa de Gobernanza de la Seguridad Digital

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Programa de Gobernanza de la Seguridad Digital | | | | |
| Descripcion Control | Existen mecanismos para facilitar la implementación de controles de ciberseguridad y privacidad. | | | | |
| Pregunta | ¿Tiene el personal de la organización una función para gobernar centralmente los controles de ciberseguridad y privacidad? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-GOV-02, Publicación de documentación sobre ciberseguridad y privacidad

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Publicación de documentación sobre ciberseguridad y privacidad | | | | |
| Descripcion Control | Existen mecanismos para establecer, mantener y difundir políticas, normas y procedimientos de ciberseguridad y privacidad. | | | | |
| Pregunta | ¿La organización establece, mantiene y difunde políticas, estándares y procedimientos de ciberseguridad y privacidad? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-GOV-04, Responsabilidades asignadas de ciberseguridad y privacidad

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Responsabilidades asignadas de ciberseguridad y privacidad | | | | |
| Descripcion Control | Existen mecanismos para asignar a una persona calificada con la misión y los recursos para administrar, coordinar, desarrollar, implementar y mantener de manera centralizada un programa de ciberseguridad y privacidad en toda la empresa. | | | | |
| Pregunta | ¿La organización asigna a una persona calificada con la misión y los recursos para administrar, coordinar, desarrollar, implementar y mantener de manera centralizada un programa de ciberseguridad y privacidad en toda la empresa? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-GOV-05, Medidas de Desempeño

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Medidas de Desempeño | | | | |
| Descripcion Control | Existen mecanismos para desarrollar, informar y monitorizar las medidas de desempeño del programa de seguridad cibernética y privacidad. | | | | |
| Pregunta | ¿La organización desarrolla, informa y monitorea las medidas de rendimiento del programa de seguridad cibernética y privacidad? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-GOV-08, Definición del contexto empresarial y la misión

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Definición del contexto empresarial y la misión | | | | |
| Descripcion Control | Existen mecanismos para definir el contexto de su modelo de negocio y documentar la misión de la organización. | | | | |
| Pregunta | ¿La organización define el contexto de su modelo de negocio y documenta la misión de la organización? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-HRS-01, Gestión de la seguridad de los recursos humanos

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Gestión de la seguridad de los recursos humanos | | | | |
| Descripcion Control | Existen mecanismos para facilitar la implementación de controles de seguridad del personal, tales como, la Política de seguridad de la información referente a los recurosos humanos. | | | | |
| Pregunta | ¿La organización dispone de una Política de seguridad de la información referente a los recursos humanos? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-HRS-03, Roles y responsabilidades

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Roles y responsabilidades | | | | |
| Descripcion Control | Existen mecanismos para definir las responsabilidades de ciberseguridad de todo el personal, tales como la Política de roles y responsabilidades relativos a ciberseguridad | | | | |
| Pregunta | ¿Existe una política o procedimiento que describa los roles y responsabilidades relativos a ciberseguridad? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-HRS-03.2, Requisitos de competencia para puestos relacionados con la seguridad

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Requisitos de competencia para puestos relacionados con la seguridad | | | | |
| Descripcion Control | Existen mecanismos para garantizar que todos los puestos relacionados con la seguridad estén ocupados por personas formadas que tengan las habilidades necesarias. | | | | |
| Pregunta | ¿Se asegura la organización de que todos los puestos relacionados con la seguridad estén ocupados por personas formadas que tengan las habilidades necesarias? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-IRO-10, Notificación de incidentes a las partes interesadas

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Notificación de incidentes a las partes interesadas | | | | |
| Descripcion Control | Existen mecanismos para reportar oportunamente los incidentes a las partes interesadas pertinentes:  ▪ Partes interesadas internas,  ▪ Clientes y terceros afectados y  ▪ Autoridades reguladoras. | | | | |
| Pregunta | ¿La organización notifica los incidentes:  ▪ Internamente al personal de respuesta a incidentes de la organización dentro de los plazos definidos por ésta; y  ▪ Externamente a las autoridades reguladoras y a las partes afectadas, según sea necesario? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-OPS-01, Seguridad de Operaciones

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Seguridad de Operaciones | | | | |
| Descripcion Control | Existen mecanismos para facilitar la implementación de controles de seguridad operacional. | | | | |
| Pregunta | ¿La organización facilita la implementación de controles de seguridad operacional? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-OPS-01.1, Procedimientos operativos estandarizados (POE)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Procedimientos operativos estandarizados (POE) | | | | |
| Descripcion Control | Existen mecanismos para identificar y documentar los Procedimientos Operativos Estandarizados (POE), o documentación similar, para permitir la ejecución adecuada de las tareas diarias/asignadas. | | | | |
| Pregunta | ¿La organización utiliza Procedimientos Operativos Estandarizados (POE), o mecanismos similares, para identificar y documentar los procedimientos diarios para permitir la ejecución adecuada de las tareas asignadas? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-OPS-02, Concepto de seguridad de las operaciones (CONOPS)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Concepto de seguridad de las operaciones (CONOPS) | | | | |
| Descripcion Control | Existen mecanismos para desarrollar un Concepto de operaciones de seguridad (CONOPS), o un plan definido de manera similar para lograr los objetivos de seguridad cibernética. Se documenta las medidas técnicas, operativas y de gestión implementadas para aplicar una defensa en profundidad que se comunican a todas las partes interesadas apropiadas. | | | | |
| Pregunta | ¿La organización desarrolla un Concepto de Operaciones de seguridad (CONOPS) que documente las medidas de gestión, operativas y técnicas implementadas para aplicar una defensa en profundidad? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-OPS-03, Prestación de servicios (Apoyo a Procesos de Negocio)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Prestación de servicios  (Apoyo a Procesos de Negocio) | | | | |
| Descripcion Control | Existen mecanismos para definir los procesos comerciales de apoyo. Se implementa la gestión adecuada de los servicios y el gobierno para garantizar la planificación, la entrega y el soporte adecuados de las capacidades tecnológicas de la organización. Se respaldan las funciones comerciales, la fuerza laboral y/o los clientes en función de los estándares reconocidos de la industria para lograr los objetivos específicos de la área de proceso. | | | | |
| Pregunta | ¿La organización define los procesos comerciales de apoyo? ¿Se implementa la gestión de servicios y el gobierno adecuados para garantizar la planificación, la entrega y el soporte adecuados de las capacidades tecnológicas de la organización?  ¿ Se respaldan las funciones comerciales, la fuerza laboral y/o los clientes con base en estándares reconocidos por la industria? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-PRM-01, Gestión de la cartera de seguridad

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Gestión de la cartera de seguridad | | | | |
| Descripcion Control | Existen mecanismos para facilitar la implementación de controles de planificación de recursos relacionados con la ciberseguridad y la privacidad que definen un plan viable para lograr los objetivos de ciberseguridad y privacidad. | | | | |
| Pregunta | ¿Facilita la organización la implementación de controles de planificación de recursos relacionados con la ciberseguridad y la privacidad? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-PRM-02, Gestión de recursos de seguridad y privacidad

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Gestión de recursos de seguridad y privacidad | | | | |
| Descripcion Control | Existen mecanismos para abordar todas las solicitudes de inversión y planificación de capital, incluidos los recursos necesarios para implementar los programas de seguridad y privacidad y documentar todas las excepciones a este requisito. | | | | |
| Pregunta | ¿La organización aborda todas las solicitudes de inversión y planificación de capital, incluidos los recursos necesarios para implementar los programas de seguridad y privacidad, y documenta todas las excepciones a este requisito? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-PRM-03, Asignación de recursos

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Asignación de recursos | | | | |
| Descripcion Control | Existen mecanismos para identificar y asignar recursos para requisitos de gestión, operativos, técnicos y de privacidad dentro de la planificación de procesos comerciales para proyectos/iniciativas. | | | | |
| Pregunta | ¿La organización identifica y asigna recursos para los requisitos de gestión, operativos, técnicos y de privacidad dentro de la planificación de procesos comerciales para proyectos/iniciativas? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-PRM-05, Definición de requisitos de seguridad y privacidad

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Definición de requisitos de seguridad y privacidad | | | | |
| Descripcion Control | Existen mecanismos para identificar funciones y componentes críticos del sistema mediante la realización de un análisis de criticidad para sistemas críticos, componentes del sistema o servicios en puntos de decisión predefinidos en el ciclo de vida de desarrollo seguro (SDLC). | | | | |
| Pregunta | ¿La organización identifica los componentes y funciones críticos del sistema mediante la realización de un análisis de criticidad para sistemas críticos, componentes del sistema o servicios en puntos de decisión predefinidos en el ciclo de vida de desarrollo seguro (SDLC)? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-PRM-06, Definición de proceso de negocio

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Definición de proceso de negocio | | | | |
| Descripcion Control | Existen mecanismos para definir los procesos de negocio teniendo en cuenta la ciberseguridad y la privacidad que determina:   ▪ El riesgo resultante para las operaciones de la organización, los activos, las personas y otras organizaciones; y  ▪ Las necesidades de protección de la información derivadas de los procesos de negocio definidos y revisa los procesos según sea necesario, hasta obtener un conjunto alcanzable de necesidades de protección. | | | | |
| Pregunta | ¿La organización define los procesos comerciales teniendo en cuenta la ciberseguridad y la privacidad ? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-RSK-01, Programa de Gestión de Riesgos

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Programa de Gestión de Riesgos | | | | |
| Descripcion Control | Existen mecanismos para facilitar la aplicación de los controles de gestión de riesgos. | | | | |
| Pregunta | ¿Facilita la organización la implementación de controles de gestión de riesgos? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-RSK-04, Evaluación de riesgos

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Evaluación de riesgos | | | | |
| Descripcion Control | Existen mecanismos para realizar evaluaciones recurrentes de riesgo. Estos estudios incluyen la probabilidad y la magnitud del daño por: - acceso no autorizado - uso - divulgación  -interrupción - modificación o destrucción de los sistemas y datos de la organización. | | | | |
| Pregunta | ¿La organización lleva a cabo una evaluación anual del riesgo que incluye:  - acceso no autorizado - uso - divulgación  -interrupción - modificación o destrucción de los sistemas y datos de la organización.? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-RSK-08, Análisis de impacto comercial (BIA)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Análisis de impacto comercial (BIA) | | | | |
| Descripcion Control | Existen mecanismos para realizar un análisis de impacto comercial (BIA) para identificar y evaluar los riesgos de ciberseguridad y protección de datos. | | | | |
| Pregunta | ¿La organización realiza un análisis de impacto comercial (BIA) para identificar y evaluar los riesgos de ciberseguridad y protección de datos? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-SAT-01, Fuerza laboral preocupada por la seguridad y la privacidad

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Fuerza laboral preocupada por la seguridad y la privacidad | | | | |
| Descripcion Control | Existen mecanismos para facilitar la implementación de controles de concienciación de la criticidad de la seguridad. | | | | |
| Pregunta | ¿Facilita la organización la implementación de controles de concienciación de seguridad? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-SAT-02, Conciencia de seguridad y privacidad

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Conciencia de seguridad y privacidad | | | | |
| Descripcion Control | Existen mecanismos para brindar a todos los empleados y contratistas la educación adecuadas que sean relevantes para su función laboral. | | | | |
| Pregunta | ¿Proporciona la organización a todos los empleados y contratistas educación y capacitación apropiadas que sean relevantes para su función laboral? | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |

# NTT-SAT-03, Capacitación en seguridad y privacidad basada en roles

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nombre Control | Capacitación en seguridad y privacidad basada en roles | | | | |
| Descripcion Control | Existen mecanismos para proporcionar capacitación relacionada con la seguridad basada en roles:   ▪ Antes de autorizar el acceso al sistema o realizar las funciones asignadas;   ▪ Cuando sea requerido por cambios en el sistema; y   ▪ Anualmente a partir de entonces. | | | | |
| Pregunta | ¿La organización brinda formación relacionada con la seguridad basada en funciones:  ▪ Antes de autorizar el acceso al sistema o realizar las funciones asignadas;  ▪ Cuando sea requerido por cambios en el sistema; y  ▪ Anualmente a partir de entonces | Respuesta | | | |
| Valoracion |  | Valoracion Objetivo |  | | |
| Evidencias |  | Iniciativas | | | |