UNIVERSIDAD
POLITÉCNICA DE
BACALAR

Políticas y Lineamientos de Seguridad para los Sistemas Informáticos

DRA. INGRID CITLALLI SUÁREZ MC LIBERTY, RECTORA DE LA UNIVERSIDAD POLITÉCNICA DE BACALAR; CON FUNDAMENTO POR LO DISPUESTO EN LOS ARTÍCULOS 1, 3, PÁRRAFO PRIMERO, 7 FRACCIÓN I, 30 FRACCIÓN VII, 47 Y 53, DE LA LEY ORGÁNICA DE LA ADMINISTRACIÓN PÚBLICA DEL ESTADO DE QUINTANA ROO; 2, 3, 15, 24, 29 FRACCIONES I Y II Y 64 FRACCIÓN I, DE LA LEY DE LAS ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA PARAESTATAL DEL ESTADO DE QUINTANA ROO; EN EJERCICIO DE LA FACULTAD QUE ME CONFIEREN LOS ARTÍCULOS 9, 18 FRACCIÓN XIV, 28 Y 31 FRACCIÓN X, DEL DECRETO QUE CREA EL ORGANISMO PÚBLICO DESCENTRALIZADO DE LA ADMINISTRACIÓN PÚBLICA PARAESTATAL DEL ESTADO DE QUINTANA ROO DENOMINADO "UNIVERSIDAD POLITÉCNICA DE BACALAR"; Y

CONSIDERANDO

Que la Universidad Politécnica de Bacalar es una Institución Pública de Educación Superior, con carácter de Organismo Público Descentralizado de la Administración Pública Paraestatal del Estado de Quintana Roo, con personalidad jurídica y patrimonio propios, sectorizada a la Secretaría de Educación del Estado.

Que es indispensable dotar a la Universidad de un marco jurídico flexible y ágil que, desde un enfoque académico, permita la mayor participación de los diversos sectores de la comunidad en el cumplimiento de sus funciones.

Que es prioritario para la Universidad establecer las Políticas y Lineamientos de Seguridad para los Sistemas Informáticos

Actualmente cualquier organización que cuente con activos y servicios informáticos debe contar con una guía de operación y entrega de servicios para que este pueda operar de una forma confiable en materia de seguridad informática en donde se debe definir políticas y lineamientos adecuados a buenas prácticas.

Las políticas y lineamientos de seguridad informática y de comunicaciones son un conjunto de reglas, directrices y procedimientos establecidos por una organización contra amenazas y riesgos de seguridad informática mediante la notificación de las medidas y formas que deben cumplir y utilizar para proteger los componentes de los sistemas informáticos, y que tienen como objetivo promover el buen uso y cuidado de los recursos de

tecnologías y los sistemas de información entre el personal directivo, administrativo, docentes, estudiantes y terceros.

Estas políticas definen las medidas de seguridad que se deben implementar, los roles y responsabilidades de los usuarios, los procedimientos para la gestión de incidentes y la respuesta a eventos de amenaza contra la seguridad.

Los cuales son esenciales para promover una cultura de seguridad organizacional y establecer un marco de trabajo que garantice la confiabilidad, integridad y disponibilidad de la información. Además de normar la manera de prevenir proteger y administrar los riesgos relacionados con tecnologías de información en las instalaciones, equipos, información, servicios y soluciones informáticas.

Alcance.

A todo el personal, estudiantes y terceras personas relacionadas con nuestra institución, incluyendo prestadores de servicios, proveedores que hagan uso de nuestros servicios e infraestructura de cómputo, sistemas informáticos y comunicaciones, software, documentación o información y equipos, deben de dar cumplimiento a las Políticas y Lineamientos de Seguridad Informática Institucional; tanto en el interior de las instalaciones, como en el exterior; de manera física y lógica vía internet.

Normatividad.

Los ordenamientos jurídicos administrativos vigentes que regulen la operación de las actividades o tareas específicas a normar a través de las políticas y lineamientos de seguridad informática, entre otros son:

- Ley de Responsabilidad de los Servidores Públicos del Estado de Quintana Roo;
- Decreto de Creación;
- Código de Ética y Conducta de los servidores públicos del Poder Ejecutivo del Estado de Quintana Roo;
- Código de Ética y Conducta de la Universidad Politécnica de Bacalar;
- Código de Conducta de la Universidad Politécnica de Bacalar;
- Lineamientos Generales de Uso de Infraestructura de Telecomunicaciones del gobierno del Estado de Quintana Roo;

Lineamientos.

CAPITULO I.
Seguridad informática en la institución.

Artículo 1. El presente documento deberá ser revisado anualmente por el Departamento de Desarrollo de Sistemas de la UPB. Será actualizado cuando sea necesario y todo cambio debe ser autorizado por la persona titular del Despacho de Rectoría.

Los términos y definiciones utilizados en el presente documento son:

Acceso. - Es el privilegio que se le otorga a una persona para utilizar un objeto, infraestructura o sistemas informáticos.

Activo informático. - Son recursos de sistemas informáticos o relacionados con este, que son necesarios para el desempeño de las funciones del usuario, tales como equipos de cómputo, impresoras, video proyectores, pantallas LED, teléfonos, teléfonos inteligentes, laptops, tabletas, equipo de telecomunicaciones, software, información, entre otros.

Antivirus. – Software especializado diseñado para detectar, eliminar y prevenir eventualmente los virus informáticos que puede haber en los dispositivos de la red, medios o activos informáticos.

Base de datos. - Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

Confidencialidad: Divulgar información solo a personas y procesos autorizados

Contraseña. – o clave es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso, aplicación, plataforma, archivo informático o sistema de información.

Correo electrónico. – Servicio de la Red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente mediante sistemas de comunicación electrónicos.

Disponibilidad: Asegurar el acceso y la utilización oportuna de la información y los sistemas de información como se requiera y la protección de los equipos, software y demás activos de tecnología informática.

DDS. – Departamento de Desarrollo de Sistemas de la UPB.

Equipo de cómputo. – Dispositivo electrónico de uso personal capaz de almacenar información, procesar datos y entregarle al usuario los resultados de la información procesada.

Firewall. – Software especializado de protección, también llamado cortafuegos, sistema cuya función es prevenir y proteger a la red privada, de intrusiones o ataques de otras redes, incluyendo malware y virus, bloqueando el acceso no autorizado.

Hardware. – Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

Información reservada y/o Confidencial. – La información clasificada como reservada es aquella que se encuentra temporalmente fuera del acceso público, debido al daño que su divulgación causaría a un asunto de interés público o seguridad nacional.

Infraestructura. – Conjunto de bienes informáticos, cableado, equipos de cómputo, dispositivos de red, servidores y otros equipos de naturaleza tecnológica.

Integridad: Garantiza la exactitud e integridad de la información.

Internet. – Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.

Malware. – Cualquier tipo de software malicioso deseñado para infiltrarse en su dispositivo sin su conocimiento.

Medio de almacenamiento removible. - Medio externo al equipo de cómputo en el que se almacena información, como CD, DVD, memorias (USB, SD, otras), cartuchos de respaldo, discos externos y otros.

Persona usuaria. – Toda persona que haga uso de los activos o servicios informáticos de la institución para el desempeño de sus funciones, consulta o servicio.

Privilegio. – Derecho de un usuario a realizar una tarea específica, que suele afectar a un sistema completo en lugar de un objeto determinado. Los privilegios los asignan los administradores a usuarios individuales o grupos de usuarios, como parte de la configuración de seguridad del equipo.

Servidor. – Equipo de cómputo de altas prestaciones, que forman parte de una red y provee servicios a otros equipos denominados clientes.

Servicio informático. – Bien tangible que se proporciona para satisfacer los requerimientos de los usuarios, relacionado con el uso del activo informático.

Sistema operativo. – Programa o conjunto de programas informáticos que gestiona los recursos de Hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto a los restantes.

Software. – Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

Software institucional. – Aplicación o programa informático con licenciamiento de uso propietario que puede ser instalado y utilizado por los usuarios para el desempeño de sus actividades o funciones, o para la gestión de un servicio informático otorgado por la institución.

Software libre. – También conocido como freeware, shareware, software demo. Software gratuito proveniente de internet o cualquier otro medio que no requiere la compra de una licencia para su uso.

UPB. – Universidad Politécnica de Bacalar.

Virus. – Software creado para producir daño en un equipo informático.

Web. – Es una convergencia de conceptos computacionales para presentar y enlazar información que se encuentra dispersa a través de internet en una forma fácilmente accesible.

CAPITULO II.
Buen uso de los activos informáticos.

Artículo 2. Todas las personas usuarias de bienes y servicios informáticos de los servicios de la universidad deberán conducirse conforme a los principios de legalidad, consentimiento, calidad de datos, confidencialidad, seguridad, disponibilidad, temporalidad y uso de los recursos informáticos y de información.

Artículo 3. Las personas usuarias que tengan activo informático o equipo móvil asignado de acuerdo a sus funciones, son las únicas responsables de su utilización, así como también de la información contenida en los mismos, por lo que debe evitar compartirlos. En caso de requerir

compartirlo o prestar el activo informático, será solamente para cuestiones laborales y sin liberarlo de su responsabilidad.

Únicamente el personal adscrito a la institución podrá ser responsable de activos informáticos, misma que deberá quedar por escrito.

Artículo 4. Toda movilización de activo informático dentro o fuera de las instalaciones de la institución es responsabilidad de las personas usuarias resguardante.

Para el caso de equipos de telecomunicaciones entre ellos switches, puntos de acceso, ruteadores, deberá ser bajo supervisión del DDS.

Artículo 5. Los resguardantes de cada activo informático serán los responsables de gestionar el buen funcionamiento del mismo.

CAPITULO III.
Clasificación de la información.

Artículo 6. La persona usuaria de un servicio informático ofrecido por la institución es responsable de la información que este servicio genera y procesa.

Artículo 7. Las personas titulares de cada unidad responsable, área, coordinación o departamento deben informar a sus colaboradores de la clasificación de la información a su cargo para su adecuado tratamiento.

Artículo 8. Toda persona servidora pública es responsable del resguardo de información, debe asegurar que la información esté protegida para asegurar su integridad y confidencialidad, acorde a su clasificación. La información puede estar disponible de manera electrónica, impresa en papel, magnética, o bien, en algún otro medio de almacenamiento removible y dispositivos portátiles.

Artículo 9. Toda persona usuaria deberá hacer uso de la información a la que tenga acceso, únicamente para propósitos relacionados con el cumplimiento de sus funciones, debiendo resguardar principalmente la relativa a datos personales, absteniéndose de comunicarlos a terceros, sin el consentimiento expreso de la persona a la que se refieren.

Artículo 10. Todas las personas usuarias que hacen uso de información clasificada como restringida confidencial, evitarán que sea accedida por personas no autorizadas y se debe asegurar que se solicite un medio de autentificación para su acceso.

CAPITULO IV.
Intercambio de información.

Artículo 11. Las personas usuarias que intercambien información que haya sido declarada reservada y/o confidencial de la Universidad, con personal de la misma o con terceras personas, deberán asegurarse de dejar el registro correspondiente de la entrega de la información que sea proporcionada, ya sea por medio físico o electrónico, dejando constancia que es procedente la entrega de información.

Artículo 12. Todo convenio de la institución con empresas, dependencias, o terceras personas para compartir información reservada y/o confidencial, deberá apegarse a las disposiciones de las leyes, reglamentos y demás instrumentos normativos relacionados con el acceso a la información pública y protección de datos personales. Se deberá asegurar que en el convenio se agreguen cláusulas de confidencialidad de la información.

CAPITULO V.
Prestación de servicios por terceros.

Artículo 13. Todo proveedor que proporcione servicios y/o equipamiento informático a la institución y que tenga acceso a información reservada y/o confidencial, deberá apegarse a las disposiciones de las leyes, reglamentos y demás instrumentos normativos relacionados con acceso a la información pública y protección de datos personales y contar con acuerdos de no divulgación ni uso que perjudique a la universidad.

Artículo 14. Todo servicio y/o equipo informático otorgado por terceros debe ser monitoreado y revisado por la persona responsable de su contratación, para asegurar que se cumplan con los términos estipulados en los acuerdos o contratos.

CAPITULO VI.
Protección contra código malicioso (virus y malware).

Artículo 15. Los equipos de cómputo institucional deben contar con software antivirus y antimalware, así como estar protegidos por el Firewall. Si el software antivirus no cubre a la plataforma utilizada, el personal deberá notificar al DDS para buscar una alternativa de solución.

Artículo 16. Toda persona usuaria que identifique o sospeche de alguna anomalía en su equipo de cómputo deberá reportarla de inmediato al DDS para su inmediata atención.

Artículo 17. Las personas usuarias no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus en programas tales como: antivirus, correo electrónico, paquetería Office, o navegadores u otros programas.

Artículo 18. Las personas usuarias deberán utilizar los mecanismos institucionales para proteger la información que resguardan, de igual forma, deberán proteger la información reservada y/o confidencial que por necesidades institucionales deba ser almacenada o trasmitida, ya sea dentro de la red interna o hacia redes externas.

CAPITULO VII.
Servicios informáticos en la red.

Artículo 19. Todo el personal, alumnado y terceros son responsables del buen uso de los servicios informáticos alojados en nuestras instalaciones y en la nube, asignados para realizar sus funciones administrativas y académicas.

Artículo 20. Sólo el personal del DDS queda facultado para acceder a los equipos de cómputo institucionales para:

- Realizar revisiones con base en el cumplimiento de las medidas de seguridad informática como antivirus y actualizaciones.
- Ejecutar las tareas del procedimiento de mantenimiento preventivo y correctivo.
- Realizar modificaciones al Sistema Operativo.
- Realizar una revisión de seguridad informática y descartar uso indebido (daños intencionales a la información o hardware) del equipo de cómputo.

Artículo 21. Toda persona titular de unidad responsable, área, coordinación o departamento, es responsable de autorizar el acceso al equipo de cómputo que tiene bajo su resguardo, para que el personal a su cargo realice sus funciones.

Artículo 22. Ninguna persona debe ver, copiar, alterar o destruir la información que reside en los equipos de cómputo y servidores sin el consentimiento explícito del responsable del equipo o del dueño de la información, excepto en casos que se especifican en el artículo 19 del presente documento.

Artículo 23. Las personas usuarias de los servicios informáticos deberán autentificarse con cuentas que permitan identificar a la persona usuaria y deberán estar protegidas con contraseñas seguras. El desarrollo, implementación y vigilancia del acceso seguro en los sistemas institucionales será responsabilidad del DDS.

Artículo 24. Todas las cuentas de usuario y su respectiva contraseña de acceso a los sistemas y servicios de información, son personales, permitiéndose el uso bajo su responsabilidad, única y exclusivamente durante la vigencia de los derechos de la persona usuaria. La vigencia de las cuentas de usuarios serán habilitadas, suspendidas o canceladas por el área en consideración a las solicitudes, necesidades y conductas de los mismos.

Artículo 25. Toda utilización de herramientas tales como analizadores, escaneo y monitoreo de red, son permitidas únicamente para las funciones de administración de las tecnologías de información y actividades académicas bajo supervisión del personal del DDS.

Artículo 26. El equipo de cómputo institucional que deberá conectar a la red (computadoras de escritorio y portátiles), será configurado solamente por personal del DDS. Toda persona usuaria se abstendrá de realizar cambios en configuraciones de esta naturaleza, en caso de falla o error de acceso a internet por esta causa, será el único responsable.

Artículo 27. A toda persona que deje de laborar o tener relación con la institución, le será cancelado su acceso de manera definitiva a los recursos informáticos institucionales. El Departamento de Recursos Humanos comunicará al DDS, toda alta, baja o cambio del personal para que se tomen las medidas correspondientes de privilegios de acceso a los servicios de red y comunicación.

Artículo 28. Todo hardware y software de uso académico, que sea considerado de riesgo para la seguridad de los servicios y sistemas informáticos institucionales, deberá ser utilizado en ambiente aislado. Por ejemplo, analizadores de tráfico de red, herramientas de análisis y diagnóstico de equipos de cómputo, equipos de laboratorio de redes, entre otros.

CAPITULO VIII.
Uso de cuentas de usuario.

Artículo 29. Toda persona que requiera acceder a servicios informáticos, tales como sistemas de información o correo electrónico institucional, será a través de una cuenta institucional compuesto por nombre de usuario y contraseña. Estos datos serán asignados por el responsable del servicio.

Artículo 30. Toda solicitud de alta, baja o cambio de privilegios de cuentas de personal administrativo o docente, para acceder a los servicios informáticos debe ser solicitado por el jefe inmediato o jefe de área, debidamente justificado.

Artículo 31. Toda persona usuaria debe actualizar la contraseña de su cuenta de acceso a los servicios informáticos por lo menos dos veces al año o cuando sospeche que pueda estar comprometida. En caso de no realizar la modificación

Artículo 32. Cuando se requiera acceder a información de un equipo de cómputo y/o cuenta de correo institucional de una persona ausente, ya sea por cuestiones de salud, por estar comisionado a actividades fuera de su área de trabajo u otro motivo no especificado, el responsable del área correspondiente deberá solicitar por escrito y con firma del solicitante o en su caso por correo electrónico que se brinde el acceso al equipo y/o servicio o sistema informático para poder dar continuidad a algún proceso institucional. El personal del DDS únicamente proporcionará acceso al responsable del área correspondiente que lo haya solicitado a efecto de que sustraiga la información necesaria. Si una persona deja de laborar en la Universidad o cambia de puesto, la persona titular inmediata podrá solicitar el acceso al equipo institucional que éste tenía asignado, para sustraer la información pertinente.

CAPITULO IX.
Monitoreo del uso de los servicios informáticos.

Artículo 33. El personal del DDS realizará periódicamente revisiones de hardware y software del activo informático institucional, para dar atención a problemas de actualizaciones y revisiones de licenciamiento. Además, se monitorean los servicios informáticos de red para administrar el uso del recurso de internet y solucionar cualquier problema detectado.

CAPITULO X.
Uso de Internet.

Artículo 34. El servicio de Internet a través de las redes institucionales se considera como herramienta de trabajo, por lo que todo usuario deberá utilizarlo exclusivamente para apoyo a las actividades relacionadas con las funciones que desempeña ya sean académicas y/o administrativas.

Artículo 35. Todo titular de unidad responsable o área puede solicitar la restricción total o parcial de acceso a páginas web del personal a su cargo, considerando para ello las funciones laborales que éstos realizan.

Artículo 36. Toda persona usuaria que descargue información y archivos de Internet mediante el navegador web u otro medio como FTP y mensajería instantánea, deberá omitir descargar archivos de dudosa procedencia. Los archivos descargados de Internet pueden contener virus o software malicioso que pongan en riesgo la información del equipo de cómputo de la persona, e incluso de la Institución.

CAPITULO XI.
Uso del correo electrónico institucional.

Artículo 37. El correo electrónico institucional es para uso exclusivo del activo administrativo y/o académico y del alumnado. Éste deberá ser utilizado sólo para realizar actividades relacionadas con sus funciones.

Artículo 38. El Departamento de Recursos Humanos deberá solicitar la creación de cuentas de correo electrónico institucional para el personal de nuevo ingreso o en su caso notificar la baja del mismo.

Artículo 39. La Universidad no es garante de los contenidos expresados en texto, sonido o video, redactados, enviados y recibidos mediante el correo electrónico institucional. Ante algún correo de naturaleza sospechosa, abstenerse de abrirlo y eliminarlo de inmediato, para evitar descargar algún tipo de amenaza para el equipo de cómputo asignado y para la red institucional.

Artículo 40. A toda persona que termine la relación laboral con la institución, una vez recibida la notificación de baja por parte del Departamento de Recursos Humanos, se inhabilitará el servicio de correo electrónico Institucional. Transcurridos 30 días hábiles, el contenido de la cuenta de correo inhabilitada será eliminado definitivamente.

Artículo 41. Toda solicitud de alta, baja o cambio de un grupo de correo institucional, debe ser solicitado por el responsable del área.

Artículo 42. El uso del correo electrónico institucional es exclusivamente para la realización de actividades académicas y de funciones de las determinadas áreas de la universidad como es el caso de los servidores públicos y personal docente, el correo institucional y su contenido pueden ser utilizados como instrumentos públicos por lo que no deberá ser usado con distintos fines a los establecidos.

Artículo 43. Es responsabilidad de toda persona usuaria del correo electrónico institucional notificar al personal del DDS la sospecha del uso no autorizado de su cuenta y hacer uso del servicio de cambio de contraseña con prontitud.

Artículo 44. Es responsabilidad de la persona usuaria respaldar aquellos correos electrónicos institucionales que por su contenido considere relevantes. Asimismo, el usuario deberá depurar constantemente los mensajes y borrar aquellos que no le sean de utilidad, para liberar el espacio asignado a su cuenta de correo y evitar problemas de saturación.

Artículo 45. Toda persona usuaria del correo electrónico institucional acepta que comprende y acuerda expresamente que la UPB no es responsable directo e indirecto y sin limitación alguna, por pérdida de datos o de cualquier otra pérdida intangible en el servicio de correo electrónico.

CAPITULO XII.
Uso del software.

Artículo 46. En todos los equipos de cómputo de la UPB, solo se permite la instalación de software con licenciamiento vigente, ya sea de uso libre o comercial. El área de soporte técnico del DDS es la única facultada para realizar o asesorar la instalación del software.

Artículo 47. Se prohíbe a las personas usuarias de un activo informático o equipo móvil instalar software sin licenciamiento vigente o malicioso en equipos de cómputo bajo su resguardo, en caso de que sea detectado el uso de los mismos por la universidad o por los propietarios de la licencia se hace único responsable de las consecuencias económicas y jurídicas que esto conlleve.

Artículo 48. Las licencias de uso de software propiedad de la Universidad otorgan a éste el derecho de emplearlas exclusivamente en los equipos asignados, propiedad de la institución.

Artículo 49. Se considera una falta grave el que las personas usuarias instalen cualquier tipo de programa (software o aplicación) en sus equipos de cómputo o estaciones de trabajo, servidores, o cualquier equipo conectado a la red, que no esté autorizado.

TRANSITORIO

ÚNICO. Las políticas y lineamientos surtirán efecto a partir de su publicación en la página institucional de la Universidad.

Cualquier asunto no contemplado en el presente documento, será analizado y resuelto en su oportunidad por el Departamento de Desarrollo de Sistemas de la UPB.

DRA. INGRID CITLALLI SUÁREZ MC LIBERTY
RECTORA